6. Some Diophantine Equations

6.1 Introduction

This chapter can be considered as the culmination of the tools that we have introduced in this course. We have already solved a number of Diophantine problems, but here we are going to solve many more. Although we have already mentioned that each Diophantine equation poses a new problem, there do exist a large number of general techniques, and in this introduction we will briefly describe these techniques and give a simple example of each (where "simple" is relative to the technique: for instance FLT is the "simplest" example of the use of Ribet's level lowering theorem!).

Whatever method is used, a general principle is that it is usually easier to show that a Diophantine equation has no solutions at all, than it is to show that it has only a specific nonempty set of solutions. A case in point is FLT since it unfortunately has the solution $1^p + (-1)^p = 0$, which in a certain sense is nontrivial.

6.1.1 The Use of Finite Fields

We can use finite fields in two opposite ways. The first is when we want to prove that an equation does *not* have a solution. In that case the finite field which is used is $\mathbb{F}_p$ for a suitable prime p. We have seen in Chapter 1 the toy example $x^2+y^2 = 3z^2$ which is seen to have no nonzero solutions by working in $\mathbb{F}_3$.

The second way is on the contrary to prove that an equation does have a solution in a finite field. If both the equation and the finite field are given, this is at least in theory very easy since we simply make the variables of the equation range over the finite number of elements of our field. The situation changes completely when we are either studying a fixed equation, but over all finite fields at once, or a family of equations over a finite field, or both. In that case we must use general theorems such as those given in Chapter 2, and in particular the very powerful Weil bounds (Corollary 2.5.27), either due to Weil himself in the case of curves, or from Deligne's proof of the Weil conjectures in the general case.

As an example we prove the following proposition.

Proposition 6.1.1. *Let $\ell \geqslant 3$ be prime and let C be the affine equation $y^2 = x^\ell + t$ for some fixed $t \in \mathbb{Z}$. This equation has a solution in $\mathbb{Z}_p$ for all p if and only if it has one for primes p of the form $p = 2k\ell + 1$ with $1 \leqslant k \leqslant (\ell - 3)/2$.*

Proof. Consider first the corresponding projective curve over $\mathbb{F}_p$. Even though the equation is singular at infinity when $\ell \geqslant 5$, if $t \neq 0$ in $\mathbb{F}_p$ and the characteristic of $\mathbb{F}_p$ is different from 2 and ℓ the Weil bounds apply, and since it is a hyperelliptic curve its genus is equal to $(\ell - 1)/2$, so we have

$$-(\ell - 1)p^{1/2} \leqslant |C(\mathbb{F}_p)| - (p + 1) \leqslant (\ell - 1)p^{1/2} .$$

In fact it is easy to compute directly $|C(\mathbb{F}_p)|$ in the cases $t = 0$ or characteristic 2 or ℓ and to see that these bounds are still valid, see Exercise 3.

In particular $|C(\mathbb{F}_p)| \geqslant p + 1 - (\ell - 1)p^{1/2}$, and this is strictly greater than 1 for $p > (\ell - 1)^2$, hence $|C(\mathbb{F}_p)| \geqslant 2$ for such p. In addition, if $p \not\equiv 1 \pmod{\ell}$ the map $x \mapsto x^\ell$ is a bijection from $\mathbb{F}_p$ to itself, so that for a given y, $x^\ell = y^2 - t$ has one solution, so $|C(\mathbb{F}_p)| = p + 1 \geqslant 2$ also for such p.

Since we must exclude the point at infinity, it follows in particular that there exists an affine nonsingular point in $C(\mathbb{F}_p)$ for all $p > (\ell - 1)^2$ and for $p \not\equiv 1 \pmod{\ell}$. Then a standard Hensel type argument shows that we can lift this solution to $\mathbb{Q}_p$, showing that C is locally soluble for such p. On the other hand if $p \leqslant (\ell - 1)^2$ and $p \equiv 1 \pmod{\ell}$ we can clearly write $p = 2k\ell + 1$ with $1 \leqslant k \leqslant (\ell - 3)/2$. □

Remark. The equation $y^2 = x^\ell + t$ is always locally soluble, in other words it always has a solution in every $\mathbb{Q}_p$, as opposed to $\mathbb{Z}_p$: simply choose $x = 1/p^2$, and $y = (1/p^\ell)(1 + p^{2\ell}t)^{1/2}$, which is p-adically convergent.

Corollary 6.1.2. *Let ℓ be a prime such that $3 \leqslant \ell \leqslant 31$. The equation $y^2 = x^\ell + t$ has a solution in $\mathbb{Z}_p$ for all p if and only if the following conditions are satisfied.*

(1) *For $\ell = 3$, 7, 13, 17, 19, and 31, no condition.*
(2) *For $\ell = 5$, $t \not\equiv 7 \pmod{11}$.*
(3) *For $\ell = 11$, $t \not\equiv 21$ or 22 modulo 23.*
(4) *For $\ell = 23$, $t \not\equiv 30$, 39, 40, 44 or 45 modulo 47, and $t \not\equiv 18$, 60 or 61 modulo 139.*
(5) *For $\ell = 29$, $t \not\equiv 31$, 32, 33, 38, 39, 43, 55 modulo 59.*

Proof. Since the above proposition reduces the problem to a reasonably small finite computation, this corollary is proved by a simple computer search, and can be extended at will. □

We will come back to this equation in Section 6.7.

6.1.2 Local Methods

We have of course already used local methods in the above examples, since we have performed Hensel lifts. Local methods can be used in several ways. One of the most common, as above, is to show that a Diophantine equation does not have any solutions in $\mathbb{Z}$, or at least to specify as much as possible which congruence classes can a possible solution belong to. We have seen in Chapter 5 the important example of *quadratic forms*, for which the Hasse–Minkowski theorem asserts that everywhere local solubility is a necessary and sufficient condition for global solubility, and we have also given methods to check local solubility at the finite number of places where this must be done.

As an additional isolated example taken almost at random from Chapter 14, consider the Diophantine equation to be solved in integers

$$y^2 = -2x^4 - 12x^2z^2 + 6z^4 \ .$$

We of course exclude the trivial solution $(x, y, z) = (0, 0, 0)$. Otherwise, if $d = \gcd(x, z)$ then $d^4 \mid y^2$, hence $d^2 \mid y$, so replacing (x, y, z) by $(x/d, y/d^2, z/d)$ we may assume that $\gcd(x, z) = 1$. We must have $2 \mid y$, hence setting $y = 2y_1$ we obtain $2y_1^2 = -x^4 - 6x^2z^2 + 3z^4$. Thus x and z have the same parity, and since they are coprime they are both odd. Since the square of an odd number is congruent to 1 modulo 8 it follows that $2y_1^2 \equiv -1 - 6 + 3 = -4 \pmod 8$, so $y_1^2 \equiv -2 \pmod 4$ which is clearly impossible. We have thus shown the impossibility of our Diophantine equation by working in $\mathbb{Z}_2$, and not only modulo powers of 2. More precisely, if we do not remove the GCD then modulo 2^m we always have the nonzero solution $x = y = 0$ and $z = 2^{\lceil m/4 \rceil}$, which tends 2-adically to the trivial solution. On the other hand after removal of the GCD, our proof shows that the equation does not have any solution modulo 16, but $(1, 0, 1)$ is clearly a solution modulo 8.

A legitimate question is to ask how one checks the local solubility of an equation. As we have seen above the usual way is to prove solubility in the residue field, and then apply a Hensel lift. It is sometimes necessary to work modulo higher powers of the prime before performing the lift. Generally speaking, checking local solubility for a given prime is easy, and usually to check everywhere local solubility one needs to consider only a finite number of primes.

A more sophisticated use of local methods is through p-adic analysis, for instance Strassmann's theorem, see Section 4.5.3 for examples. Here the fact that we do not only work modulo p^k for all k but in the *characteristic zero field* $\mathbb{Q}_p$ gives us new tools of analytic nature.

6.1.3 Global Methods

Given a Diophantine problem, the first thing to do is always to see whether the problem has a solution locally, using one of the methods mentioned above.

If has none, the problem is solved since we know that our equation has no solution. Evidently the only interesting problems are those for which the equations are everywhere locally soluble. The local information that we obtain may already completely solve the problem, or may give useful information on the global problem through local to global principles. However such principles are rather rare (see Chapter 5), so it is necessary to study the equation globally, possibly by working in some appropriate number field K. There are now many methods for doing this, which we mention briefly in turn, since we will come back to them in much more detail in the rest of this book.

• The first and most classical method, originating with Fermat, Euler, Gauss, and especially Kummer, applies when it is possible to *factor* the Diophantine equation in K, a typical example being FLT where one factors the equation in the cyclotomic field $K = \mathbb{Q}(\zeta_p)$. It is then essential to know explicitly the structure of the class group of K, of the unit group (i.e., a system of fundamental units), and to be able to find explicitly a generator of a principal ideal.

It is important to note that, being in the twentyfirst century, these computational problems can (for reasonable K) be solved at the click of a computer mouse button using computer algebra systems specialized in such tasks, such as `Kant/Kash`, `magma` or `Pari/GP`. We will therefore always assume that we have available the basic data concerning the number fields which occur. This method will be used at length in the present chapter, as well as in Chapter 14.

• A second global method for solving Diophantine equations is based on Diophantine approximation techniques, and on Baker type results on linear forms in logarithms of algebraic numbers, and I refer to Chapter 12 for a survey of the method. It is used in particular to solve *Thue equations*, in other words equations of the form $f(x,y) = m$, where f is a homogeneous polynomial in two variables. This is now in complete but quite technical algorithmic form. In Section 8.7 We will study in detail a variant which involves linear forms in elliptic logarithms, which paradoxically is easier to explain. This will enable us to find in reasonable cases all integral points on an elliptic curve.

• A third global method for solving certain types of Diophantine equations, mostly those that can be reduced to a cubic, is the use the Birch and Swinnerton-Dyer conjecture (BSD for short) which we will state and study in detail in Chapter 8. As mentioned in the introduction this remarkable conjecture enables us to predict the $\mathbb{Z}$-rank of the group of points of an elliptic curve over $\mathbb{Q}$ by computing a purely analytic quantity, and in particular tells us whether this group is infinite or not. The fact that this method is based on a *conjecture* is not important since either the analytic result says that the group is finite, and in that case BSD is proved, or it says that the group is infinite, and we can then search for generators of the group using other

techniques. All this will become much clearer in the numerous examples that we will give.

• The most modern and sophisticated method for solving Diophantine equations is that used by Ribet, Wiles, and Taylor–Wiles for solving completely Fermat's last theorem, using modular forms and Galois representations. The kind of Diophantine equations that it is able to solve is usually of the form $a+b+c=0$, where a, b, and c are highly divisible by certain integers (FLT being a typical example). This is linked to the famous *abc* conjecture (Conjecture 14.6.4). This method is based on a combination of a theorem of Ribet on "level lowering" of modular forms with the theorem of Wiles and Taylor–Wiles saying that the L-function attached to an elliptic curve defined over $\mathbb{Q}$ is in fact the L-function of a modular form. The proof of these theorems is very difficult, and Wiles's theorem has justly been celebrated as one of the great mathematical achievements of the end of the twentieth century. However it is not necessary to understand the proof to *use* the theorems, if one understands the underlying concepts. Thanks to S. Siksek, I have included as Chapter 15 a detailed black box explanation of the method. I advise the reader to look also at the expository paper by M. Bennett [Ben2] (see also [Ben-Ski]), which has a similar purpose.

6.2 Diophantine Equations of Degree 1

The simplest of all Diophantine equations are equations of degree 1. The two variable case is well-known: the equation $ax+by=c$ has a solution in integers x, y if and only if $\gcd(a,b)$ divides c, and in that case if (x_0,y_0) is a particular solution, the general solution is given by $x=x_0+kb/\gcd(a,b)$, $y=y_0-ka/\gcd(a,b)$ for any integer k. Furthermore a particular solution can easily be found with the extended Euclidean algorithm.

The case of more than two variables is slightly more difficult, because of the necessity of writing down explicitly the solution to the homogeneous equation (once again it is easy to find a particular solution with the extended Euclidean algorithm). For example, in the case of three variables, the equation $ax+by+cz=d$ has a solution if and only if $\gcd(a,b,c)$ divides d, and in that case if (x_0,y_0,z_0) is a particular solution, the general solution is given by $x=x_0+mb/\gcd(a,b)-\ell c/\gcd(a,c)$, $y=y_0+kc/\gcd(b,c)-ma/\gcd(a,b)$, $z=z_0+\ell a/\gcd(a,c)-kb/\gcd(b,c)$ for any integers k, ℓ and m, see Exercise 4.

To state the solution in the case of n variables, we must use the notion of *Hermite normal form* (HNF) of an integer matrix. However, it is not simpler to state it in that case than in the general case of a system of m linear Diophantine equations in n variables. The definition and result are as follows.

Definition 6.2.1. *Let $H = (h_{i,j})$ be an $m \times n$ matrix with $m \geqslant n$. We will say that H is in Hermite normal form (HNF) if there exists a strictly increasing function f from $[1,n]$ to $[1,m]$ such that for all $j \leqslant n$ we have $m_{f(j),j} \geqslant 1$, $m_{i,j} = 0$ for $i > f(j)$, and $0 \leqslant m_{f(j),k} < m_{f(j),j}$ for $k > j$.*

For instance, if $m = n$ we have necessarily $f(j) = j$, so in that very common and important case an integer matrix H is in HNF if and only if it is upper triangular with strictly positive diagonal elements, and its off-diagonal elements are nonnegative and strictly less than the diagonal element in the same row.

Proposition 6.2.2. *Let A be an $m \times n$ integer matrix, and let B be an m-component integer column vector. There exists a matrix $U \in \mathrm{GL}_n(\mathbb{Z})$ and a matrix H in HNF such that $AU = (0|H)$. If k is the number of zero columns in the right hand side, write $U = (U_1|U_2)$, where U_1 and U_2 are $n \times k$ and $n \times (n-k)$ matrices respectively. Then the Diophantine system $AX = B$ has a solution if and only if there exists an inverse image Z_2 of B by H (which can be checked immediately), and in that case the general solution is given by $U_2 Z_2 + U_1 Y$, for any k-component integer vector Y.*

Proof. Recall that $\mathrm{GL}_n(\mathbb{Z})$ denotes the group of integer matrices which are invertible, i.e., of determinant ± 1. The first statement is proved in a manner very similar to the existence of the column echelon form (proved using Gaussian elimination). Here, we must perform all operations using only integer matrices of determinant ± 1. This is done by using as elementary operations either column exchanges, or operations transforming a matrix $\left(\begin{smallmatrix} x & y \\ a & b \end{smallmatrix}\right)$ into a matrix of the form $\left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right)$ by right multiplication by $\begin{pmatrix} -b/\gcd(a,b) & u \\ a/\gcd(a,b) & v \end{pmatrix}$, where u and v are such that $au + bv = \gcd(a,b)$. We leave the (well-known) details to the reader (see [Coh0], Section 2.4.2).

Once this basic statement proved, the rest is immediate: the equation $AX = B$ is equivalent to $AUX_1 = B$ (with $X_1 = U^{-1}X$), hence to $(0|H)X_1 = B$, which is soluble if and only if $HZ_2 = B$ is soluble. This last equation is in echelon form, so its solubility can be checked immediately one component after the other. If such a vector Z_2 exists, we can choose for X_1 the vector $\begin{pmatrix} 0 \\ \hline Z_2 \end{pmatrix}$ with evident notation. We then have $X = UX_1 = (U_1|U_2)X_1 = U_2 Z_2$ as claimed. Finally, if X_1 is a general solution to $AUX_1 = B$, then $AU\left(X_1 - \begin{pmatrix} 0 \\ \hline Z_2 \end{pmatrix}\right) = 0$, hence $(0|H)\left(X_1 - \begin{pmatrix} 0 \\ \hline Z_2 \end{pmatrix}\right) = 0$. If we write $X_1 - \begin{pmatrix} 0 \\ \hline Z_2 \end{pmatrix} = \begin{pmatrix} Y_1 \\ \hline Y_2 \end{pmatrix}$, then we obtain $HY_2 = 0$, and since H is in HNF and in particular in column echelon form, the columns of H are linearly independent hence $Y_2 = 0$. Thus $X_1 = \begin{pmatrix} Y_1 \\ \hline Z_2 \end{pmatrix}$, so that $X = (U_1|U_2)X_1 = U_1 Y_1 + U_2 Z_2$, finishing the proof of the proposition. □

In the special case where $A = (a_j)$ has a single row, thus corresponding to a single linear Diophantine equation, the equation $AX = b$ has a solution if and only if the GCD of the a_j divides b, but the general solution must be written as explained in the proposition.

6.3 Diophantine Equations of Degree 2

We have already studied Diophantine equations of degree 2 in Section 5.3.2 in the context of the Hasse-Minkowski theorem. We will study them in more detail in this section.

6.3.1 The General Homogeneous Equation

Let $f(x_1, \ldots, x_n)$ be a quadratic form in n variables with integer coefficients, represented by a symmetric matrix Q with integral diagonal entries and half-integral off-diagonal entries. If $X = (x_1, \ldots, x_n)^t$ is a *column* vector, then $f(x_1, \ldots, x_n) = X^t Q X$. The discriminant D of the form f is by definition $D = (-1)^{n(n-1)/2} \det(2Q)$. We will always assume that f is *nonsingular*, in other words that $D \neq 0$ (a singular quadratic form is in fact equivalent to a quadratic form with a strictly smaller number of variables, so we do not lose any generality). Since we are looking for rational solutions, we will also always assume that f is not positive definite or negative definite, so that the condition at the place at infinity of the Hasse–Minkowski theorem is satisfied. In this case, we will simply say that f is *indefinite*.

By the Hasse–Minkowski theorem, we can determine whether a nontrivial rational solution to $f = 0$ exists by looking at the equation locally. More precisely, we have the following proposition.

Proposition 6.3.1. *The Diophantine equation $f(x_1, \ldots, x_n) = 0$ has a nontrivial rational solution if and only if it has a nontrivial solution in every $\mathbb{Q}_p$ for every p such that $p \mid 2D$.*

Proof. The necessity of the conditions is clear. Conversely, assume that they are satisfied. By the Chevalley–Warning Theorem 2.5.2, if $n \geqslant 3$ the equation has a nontrivial solution $X_0 = (x_{0,1}, \ldots, x_{0,n})^t \in \mathbb{F}_p^n$ for all p. Now if $p \nmid 2D$, the partial derivatives of f cannot all vanish modulo p at X_0. If for instance $\frac{\partial f}{\partial x_i}(X_0) \not\equiv 0 \pmod{p}$, the simple form of Hensel's lemma 4.1.37 tells us that there exists $\alpha_i \in \mathbb{Z}_p$ such that $f(x_{0,1}, \ldots, \alpha_i, \ldots, x_{0,n}) = 0$, so that there exists a local solution for all these p. We conclude by the Hasse–Minkowski theorem.

For $n = 2$ we reason differently. Write $f(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2$, so that $D = b^2 - 4ac$. For any field K of characteristic zero it is clear that $f(x_1, x_2) = 0$ has a nontrivial solution in K if and only if D is a square in K. Thus by assumption D is a square in every $\mathbb{Q}_p$ such that $p \mid 2D$. But in

particular this means that $v_p(D)$ is even for every $p \mid D$, in other words that D is a square in $\mathbb{Q}$, so that $f(x_1, x_2) = 0$ has a nontrivial rational solution. Finally for $n = 1$ the equation evidently has no nontrivial solutions.

□

To test local solubility at the "bad" primes p dividing $2D$ is done by looking modulo p^k for a suitable k for which Hensel's lemma can be used, hence is easy. The only difficult part is thus factoring the discriminant D.

Finding explicitly a nontrivial rational solution can be done using an efficient algorithm. We will see below such an algorithm in the important special case $n = 3$.

Once a solution $X_0 = (x_{1,0}, \ldots, x_{n,0})^t$ is found, we can ask for the general solution in *rational* numbers (the general solution in *integers* is a more difficult task which we will consider only in special cases). The result is as follows.

Proposition 6.3.2. *Let $X_0 = (x_{1,0}, \ldots, x_{n,0})^t$ be a nontrivial solution of the Diophantine equation $f(x_1, \ldots, x_n) = X^t Q X = 0$.*

(1) *The general solution X to the equation in rational numbers such that $X^t Q X_0 \neq 0$ is given by $X = d((R^t Q R)X_0 - 2(R^t Q X_0)R)$, where $R \in \mathbb{Q}^n$ is a vector of parameters such that $R^t Q X_0 \neq 0$, and $d \in \mathbb{Q}^*$.*

(2) *In addition, if we choose a matrix $M \in \mathrm{GL}_n(\mathbb{Q})$ whose last column M_n is equal to X_0, we may assume that R is a $\mathbb{Z}$-linear combination of the first $n-1$ columns of M, with the GCD of the coefficients equal to 1.*

(3) *In (2), the matrix R is unique up to changing R into $-R$, and the coefficient $d \in \mathbb{Q}$ is unique.*

Proof. (1). Since f is homogeneous, we consider nontrivial solutions of $f = 0$ as elements of the projective space $\mathbb{P}_n(\mathbb{Q})$. The parametric equation of a general line passing through X_0 is $X = uX_0 + vR$ with $(u, v) \in \mathbb{P}_2(\mathbb{Q})$, for some fixed $R \in \mathbb{P}_n(\mathbb{Q})$ not equal (projectively) to X_0. Let us find the values of (u, v) for which such an X is a solution of our equation. We write

$$0 = X^t Q X = u^2 X_0^t Q X_0 + 2uv R^t Q X_0 + v^2 R^t Q R = v(2uR^t Q X_0 + vR^t Q R) .$$

Solutions with $X^t Q X_0 \neq 0$ correspond to $vR^t Q X_0 \neq 0$, hence to $v \neq 0$ and $R^t Q X_0 \neq 0$, so that we can choose $(u, v) = (R^t Q R, -2R^t Q X_0) \in \mathbb{P}_2(\mathbb{Q})$. Since we have considered X as an element of the projective space, to obtain all solutions we must multiply by an arbitrary $d \in \mathbb{Q}^*$, proving (1).

(2). Since X_0 is nonzero, there exists a matrix M such that $M \in \mathrm{GL}_n(\mathbb{Q})$ whose last column M_n is equal to X_0. If we set $S = M^{-1}R = (y_1, \ldots, y_n)^t$, then $R = MS = \sum_{1 \leqslant j \leqslant n} y_j M_j = T + y_n X_0$, so that

$$\begin{aligned}(R^t Q R)X_0 - 2(R^t Q X_0)R &= (T^t Q T + 2y_n T^t Q X_0)X_0 - 2(T^t Q X_0)(T + y_n X_0) \\ &= (T^t Q T)X_0 - 2(T^t Q X_0)T ,\end{aligned}$$

proving that we can replace R by T, in other words take only a linear combination of the first $n-1$ columns of M. Furthermore, if u is the unique positive rational number such that the y_i/u for $1 \leqslant i \leqslant n-1$ are integers with global GCD equal to 1, we may replace T by T/u and d by du^2, proving (2).

(3). For simplicity, let us say that a $\mathbb{Z}$-linear combination is primitive if the GCD of the coefficients is equal to 1. If we set $M^{-1}X = (y_1, \ldots, y_n)^t$ for some $y_i \in \mathbb{Q}$, we have $X = \sum_{1 \leqslant i \leqslant n} y_i M_i$. Since $X^t Q X_0 \neq 0$, the vector R has the form $R = aX + bX_0$ for some a, b in $\mathbb{Q}$. It follows that

$$R = \sum_{1 \leqslant i \leqslant n-1} (ay_i)M_i + (ay_n + b)M_n \ ,$$

and since the columns of M are linearly independent, if R is a primitive $\mathbb{Z}$-linear combination of the first $n-1$ columns this means that $ay_n + b = 0$ and that for $1 \leqslant i \leqslant n-1$ the ay_i are integers with global GCD equal to 1. Thus, if as in (2) we denote by u the unique positive rational number such that the y_i/u for $1 \leqslant i \leqslant n-1$ are integers with global GCD equal to 1, we have necessarily $a = \pm 1/u$, hence $b = \pm y_n/u$, so that R is indeed determined up to sign, as claimed. In addition, we have

$$\begin{aligned}(R^t Q R)X_0 - 2(R^t Q X_0)R &= 2ab(X^t Q X_0)X_0 - 2a(X^t Q X_0)(aX + bX_0) \\ &= -2a^2(X^t Q X_0)X \ ,\end{aligned}$$

and this is equal to X/d with $d = -1/(2a^2 X^t Q X_0)$, so that d is also uniquely determined. □

Note that clearly the solutions of our Diophantine equation such that $X^t Q X_0 = 0$ cannot be attained by this parametrization, since $X^t Q X_0 = 0$ is equivalent to $R^t Q X_0 = 0$, which is excluded.

6.3.2 The Homogeneous Ternary Quadratic Equation

As we have seen during the proof of the Hasse–Minkowski theorem, the case $n = 3$ is the most important. In that case, the above proposition can be refined. We begin by a lemma.

Lemma 6.3.3. *Let Q be a nonsingular 3×3 real symmetric matrix, and let X_0 be a nonzero real vector such that $X_0^t Q X_0 = 0$. For $X \in \mathbb{R}^3$, $X^t Q X = X^t Q X_0 = 0$ is equivalent to $X = \lambda X_0$ for some $\lambda \in \mathbb{R}$.*

Proof. By diagonalizing Q, we may assume that Q is a diagonal matrix with real nonzero diagonal entries a, b, c. Thus $X^t Q X = X^t Q X_0 = 0$ is equivalent to $ax^2 + by^2 + cz^2 = axx_0 + byy_0 + czz_0 = 0$. Since $(x_0, y_0, z_0) \neq (0, 0, 0)$, we may assume for instance that $z_0 \neq 0$. Thus $z = -(axx_0 + byy_0)/(cz_0)$, hence

$$0 = X^tQX = (ax^2+by^2)cz_0^2 + (axx_0+byy_0)^2$$
$$= (axx_0+byy_0)^2 - (ax^2+by^2)(ax_0^2+by_0^2) = -ab(xy_0-yx_0)^2 ,$$

so that $xy_0 - yx_0 = 0$, hence

$$cz_0(zx_0 - xz_0) = -x_0(axx_0+byy_0) + x(ax_0^2+by_0^2) = by_0(xy_0-yx_0) = 0 ,$$

so that X and X_0 are proportional, as claimed. □

Proposition 6.3.4. *Let $X_0 = (x_0, y_0, z_0)$ be a nontrivial solution of the Diophantine equation $f(x,y,z) = X^tQX = 0$ and let M be a matrix in $\mathrm{GL}_3(\mathbb{Q})$ whose last column M_3 is equal to X_0. The general rational solution X to the equation is given by $X = d((R^tQR)X_0 - 2(R^tQX_0)R)$, where $R = sM_1+tM_2$, s and t are coprime integers, and $d \in \mathbb{Q}$.*

Proof. By Proposition 6.3.2, the above parametrization with $R^tQX_0 \neq 0$ gives all solutions such that $X^tQX_0 \neq 0$. Furthermore if $R = s_1M_1+s_2M_2$ for some s_1 and s_2 in $\mathbb{Q}$ not both 0, setting $u = \gcd(s_1,s_2)$, $s = s_1/u$, $t = s_2/u$, hence changing R into R/u, and finally changing d into du^2, it is clear that we may assume that s and t are coprime integers. In addition, by the above lemma, the solutions such that $X^tQX_0 = 0$ are the multiples of X_0. Now since Q is nonsingular and $X_0 \neq 0$, we have $QX_0 \neq 0$. It follows that the subspace V of $\mathbb{Q}^3$ of R such that $R^tQX_0 = 0$ is exactly 2-dimensional. I claim that there exists R equal to a linear combination of M_1 and M_2 which belongs to V and is not proportional to X_0. Indeed, since $M \in \mathrm{GL}_3(\mathbb{Q})$, any nonzero linear combination of M_1 and M_2 is not proportional to $M_3 = X_0$. Furthermore, for $R = sM_1 + tM_2$ the equation $R^tQX_0 = 0$ reads $sM_1^tQX_0 + tM_2^tQX_0 = 0$. If for instance $M_1^tQX_0 = 0$, we can choose $R = M_1$. Otherwise, we choose $s_1 = -M_2^tQX_0$, $t_1 = M_1^tQX_0$, and set $s = s_1/\gcd(s_1,t_1)$, $t = t_1/\gcd(s_1,t_1)$, proving my claim. Thus, using once again the above lemma, it follows that for this R we have $R^tQR \neq 0$, hence $X = d((R^tQR)X_0 - 2(R^tQX_0)R) = d(R^tQR)X_0$. Since $R^tQR \neq 0$, by choosing a suitable value of $d \in \mathbb{Q}$ we can thus obtain any multiple of X_0. □

Remark. The above construction is of course explicit: to obtain X_0 itself for instance, either $M_1^tQX_0 = 0$ in which case we choose $R = M_1$ and $d = 1/(M_1^tQM_1)$, which exists by the lemma, or $M_1^tQX_0 \neq 0$, and we choose s and t as explained, $R = sM_1 + tM_2$, and then $d = 1/(R^tQR)$.

Corollary 6.3.5. *Let $f(x,y,z)$ be a nonsingular rational quadratic form in three variables. There exist three polynomials P_x, P_y, P_z with integer coefficients which are homogeneous of degree 2 in 2 variables (i.e., integral binary quadratic forms) such that the general rational solutions of the Diophantine equation $f(x,y,z) = 0$ are given by the parametrization $x = dP_x(s,t)$, $y = dP_y(s,t)$ and $z = dP_z(s,t)$, where s and t are coprime integers and $d \in \mathbb{Q}$, uniquely determined (up to simultaneous change of sign of s and t) by x, y, z.*

Proof. Clear from the above proposition. Note that by multiplying d by a suitable rational number we may indeed assume that the polynomials P_x, P_y and P_z have integral coefficients. □

Remark. Although we have proved the above corollary in the context of quadratic forms defined over $\mathbb{Q}$, it is clear that the proofs remain valid over any field of characteristic different from 2, hence the corollary is true if we remove all mention of integrality, coprimeness or uniqueness.

Corollary 6.3.6. *Assume that $ABC \neq 0$ and let (x_0, y_0, z_0) be a particular nontrivial solution of $Ax^2 + By^2 = Cz^2$, and assume that $z_0 \neq 0$. The general solution in* rational numbers *to the equation is given by*

$$\begin{aligned} x &= d(x_0(As^2 - Bt^2) + 2y_0Bst) \\ y &= d(2x_0Ast - y_0(As^2 - Bt^2)) \\ z &= dz_0(As^2 + Bt^2) \ , \end{aligned}$$

where s and t are coprime integers *and d is any rational number. Moreover s, t and d are uniquely determined, up to a simultaneous change of sign of s and t.*

Proof. We apply the above proposition to the diagonal quadratic form with diagonal $(A, B, -C)$, and to the particular solution $(-x_0, -y_0, z_0)$ (so as to obtain a parametrization with less minus signs). Since $z_0 \neq 0$, we may choose

$$M = \begin{pmatrix} 1 & 0 & -x_0 \\ 0 & 1 & -y_0 \\ 0 & 0 & z_0 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{Q}) \ ,$$

so that $R = (s, t, 0)^t$ with s and t coprime integers, and set $E = (R^tQR)X_0 - 2(R^tQX_0)R$. We compute that

$$\begin{aligned} E &= (As^2 + Bt^2)(-x_0, -y_0, z_0)^t + 2(Asx_0 + Bty_0)(s, t, 0)^t \\ &= (x_0(As^2 - Bt^2) + 2y_0Bst, -y_0(As^2 - Bt^2) + 2x_0Ast, (As^2 + Bt^2)z_0)^t \ , \end{aligned}$$

giving the above parametrization. The uniqueness statement (up to sign) has been proved in complete generality above. □

Remark. Although evidently $(-x, y, z)$ (for instance) is also a solution if (x, y, z) is one, it is not evident on the formulas how to obtain it. We leave this as an exercise for the industrious reader, see Exercise 5.

Assume now that $f(x, y, z)$ has integral coefficients, and that we want to parametrize all *integral* solutions. Writing $d = u/v$ with $\gcd(u, v) = 1$, we see that we want $v \mid P_x(s, t)$, $v \mid P_y(s, t)$ and $v \mid P_z(s, t)$. By a well-known property of resultants, there exist polynomials U and V say with *integer* coefficients such that

$$U(S,T)P_x(S,T)+V(S,T)P_y(S,T)=R_S(P_x(S,T),P_y(S,T))\ ,$$

where R_S denotes the resultant with respect to the variable S. Clearly $R_S(P_x(S,T),P_y(S,T))=r(x,y)T^4$ for some $r(x,y)\in\mathbb{Z}$, and by homogeneity we also have $R_T(P_x(S,T),P_y(S,T))=r(x,y)S^4$ for the same constant $r(x,y)$, where R_T denotes the resultant with respect to T. By abuse of language we will call $r(x,y)$ the resultant of the polynomials P_x and P_y. It follows that $v\mid r(x,y)s^4$ and $v\mid r(x,y)t^4$, and since $\gcd(s,t)=1$ we have $v\mid r(x,y)$. We have thus proved the following.

Proposition 6.3.7. *In the parametrization of Proposition 6.3.5, if x, y and z are integers and $d=u/v$ with $\gcd(u,v)=1$ then $v\mid\gcd(r(x,y),r(x,z),r(y,z))$.*

Note that the converse is not necessarily true.

In the context of Corollary 6.3.6, assume that A, B and C are integers and that (x_0,y_0,z_0) is chosen to be an integral solution. We then have the following:

Corollary 6.3.8. *In the parametrization given by Corollary 6.3.6, if x, y and z are integers then $d=u/v$ with $v\mid 2BCz_0^2$.*

Proof. If we simply used the above proposition, we would obtain $v\mid 4ABCz_0^4$. However we can do better (also in the general case) by using *reduced resultants*. Without entering into this theory, we simply note that if we set $P_x(S,T)=x_0(AS^2-BT^2)+2y_0BST$, $P_y(S,T)=2x_0AST-y_0(AS^2-BT^2)$ and $P_z(S,T)=z_0(AS^2+BT^2)$ then

$$U(S,T)P_x(S,T)+V(S,T)P_y(S,T)=2BCz_0^2T^2\ ,$$

where

$$U(S,T)=A(y_0S-2x_0T)\quad\text{and}\quad V(S,T)=Ax_0S+2By_0T\ .$$

As above we deduce that $v\mid 2BCz_0^2$, proving the corollary. Note that if we also consider P_x and P_z or P_y and P_z, we would obtain a right hand side equal to $2BCz_0^3T^3$, hence a multiple of the above, so we would not obtain any additional information. □

6.3.3 Computing a Particular Solution

We see from the above results that the main task for finding a parametrization of a homogeneous ternary equation $X^tQX=0$ is to find a particular solution X_0. Although the proof of the Hasse–Minkowski theorem is completely effective, it would lead to a rather inefficient algorithm for finding X_0. Although this book is not mainly algorithmic in nature, we give a very elegant and efficient algorithm for doing so initially due to Gauss and Legendre, but streamlined in the present nice form by D. Simon, see [Sim1]. We begin by two lemmas of independent interest, where as usual we denote by $\mathcal{M}_n(\mathbb{Z})$ the ring of $n\times n$ matrices with integral entries.

Lemma 6.3.9. *Let $M \in \mathcal{M}_n(\mathbb{Z})$, p be a prime number, and let $d = \dim_{\mathbb{F}_p}(\mathrm{Ker}(\overline{M}))$, where $\overline{M}$ denotes the reduction of M modulo p. Then $p^d \mid \det(M)$, in other words $d \leqslant v_p(\det(M))$.*

Proof. If $\overline{U_1}, \ldots, \overline{U_d}$ is an $\mathbb{F}_p$-basis of $\mathrm{Ker}(\overline{M})$, we complete it to an $\mathbb{F}_p$-basis $\overline{U_1}, \ldots, \overline{U_n}$ of $\mathbb{F}_p^n$, we let $\overline{U} \in \mathrm{GL}_n(\mathbb{F}_p)$ be the matrix whose columns are the $\overline{U_j}$, and finally let U be any lift of $\overline{U}$ to $\mathcal{M}_n(\mathbb{Z})$. By assumption the first d columns of the matrix MU are divisible by p, hence $p^d \mid \det(MU) = \det(M)\det(U)$. On the other hand $p \nmid \det(U)$ since $\overline{U} \in \mathrm{GL}_n(\mathbb{F}_p)$, so $p^d \mid \det(M)$ as claimed. □

Lemma 6.3.10. *For any $\overline{M} \in \mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$ there exists a lift M such that $M \in \mathrm{SL}_n(\mathbb{Z})$, in other words the natural reduction map from $\mathrm{SL}_n(\mathbb{Z})$ to $\mathrm{SL}_n(\mathbb{Z}/p\mathbb{Z})$ is surjective (here p is not necessarily a prime number).*

Proof. The following proof is taken from [Shi]. We prove this by induction on the size n of the matrix, the result being trivial for $n = 1$. Assume $n > 1$ and the result true for $n - 1$, and let N be any lift to $\mathcal{M}_n(\mathbb{Z})$ of the matrix $\overline{M}$. By the elementary divisor theorem (i.e., the Smith Normal Form in algorithmic terms) we can find two matrices U and V in $\mathrm{SL}_n(\mathbb{Z})$ such that $UNV = D = \mathrm{diag}(d_1, \ldots, d_n)$ is a diagonal matrix with diagonal elements d_i such that $d_n \mid d_{n-1} \mid \cdots \mid d_1$, and we have $\det(D) = d_1 \cdots d_n \equiv 1 \pmod{p}$. If we can find a matrix $E \in \mathrm{SL}_n(\mathbb{Z})$ such that $E \equiv D \pmod{p}$ then $U^{-1}EV^{-1} \in \mathrm{SL}_n(\mathbb{Z})$ will be such that $U^{-1}EV^{-1} \equiv N \equiv \overline{M} \pmod{p}$. Thus we may assume that $N = D$ and forget the matrices U and V. Set $b = d_2 \cdots d_n$, $a = \det(D) = d_1 b$ and define

$$W = \begin{pmatrix} 1 & -1 \\ 1-b & b \end{pmatrix}, \quad \text{and} \quad X = \begin{pmatrix} 1 & d_2 \\ 0 & 1 \end{pmatrix},$$

both of determinant 1. We check that

$$W \begin{pmatrix} 1 & 0 \\ 1-d_1 & d_1 d_2 \end{pmatrix} X = \begin{pmatrix} d_1 & 0 \\ 1-a & d_2 \end{pmatrix} \equiv \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix} \pmod{p}$$

since $a \equiv 1 \pmod{p}$ by assumption.

By our induction hypothesis there exists a matrix $C \in \mathrm{SL}_{n-1}(\mathbb{Z})$ such that $C \equiv \mathrm{diag}(d_1 d_2, d_3, \ldots, d_n) \pmod{p}$. It follows that if we let W_1, X_1 in $\mathrm{SL}_n(\mathbb{Z})$ be defined as block matrices by

$$W_1 = \begin{pmatrix} W & 0 \\ 0 & I_{n-2} \end{pmatrix}, \; X_1 = \begin{pmatrix} X & 0 \\ 0 & I_{n-2} \end{pmatrix}$$

where as usual I_{n-2} is the identity matrix of order $n - 2$, and if we set

$$C_1 = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 1-d_1 & & & \\ 0 & & & \\ \vdots & & C & \\ 0 & & & \end{pmatrix}$$

which is also clearly in $\mathrm{SL}_n(\mathbb{Z})$, then $W_1C_1X_1 \equiv D \pmod{p}$ and $W_1C_1X_1 \in \mathrm{SL}_n(\mathbb{Z})$, proving the lemma by induction. □

The algorithm for finding a particular solution to a homogeneous ternary quadratic equation is based on the following theorem.

Theorem 6.3.11. *Let $Q \in \mathcal{M}_3(\mathbb{Z})$ be the (symmetric) matrix of a nondegenerate ternary quadratic form which has a nontrivial solution in $\mathbb{Q}_p$ for every $p \mid \det(Q)$. There exists a matrix $V \in \mathcal{M}_3(\mathbb{Z})$ such that*

$$\det(V) = |\det(Q)| \quad \textit{and} \quad Q_1 = \frac{1}{\det(Q)} V^t Q V \in \mathcal{M}_3(\mathbb{Z}) ,$$

and in particular $\det(Q_1) = 1$.

Furthermore if the prime factorization of $\det(Q)$ is known V can be found by a polynomial-time algorithm, and the entries of V are bounded by a polynomial in $\det(Q)$.

Proof. We prove the theorem by induction on $|\det(Q)| \geqslant 1$. If $\det(Q) = \pm 1$ there is nothing to prove. Thus let p be a prime number dividing $\det(Q)$, so that in particular $\mathrm{Ker}(\overline{Q})$ is non trivial, and let $d = \dim_{\mathbb{F}_p}(\mathrm{Ker}(\overline{Q})) \geqslant 1$, so that $p^d \mid \det(Q)$ by the above lemma. We consider three cases.

Case 1: $v_p(\det(Q)) = 1$**.** By Lemma 6.3.9 we must have $d = \dim_{\mathbb{F}_p}(\mathrm{Ker}(\overline{Q})) = 1$, and as in the proof of that lemma let $\overline{U} \in \mathrm{GL}_3(\mathbb{F}_p)$ such that the first column of $\overline{U}$ forms a basis of $\mathrm{Ker}(\overline{Q})$. Multiplying a column of $\overline{U}$ by a suitable element of $\mathbb{F}_p^*$ we may assume that $\overline{U} \in \mathrm{SL}_3(\mathbb{F}_p)$. From Lemma 6.3.10 it follows that we can lift $\overline{U}$ to a matrix $U \in \mathrm{SL}_3(\mathbb{Z})$, whose columns we denote by U_i. By assumption we know that $p \mid QU_1$, hence $p \mid U_i^t Q U_1$ for all i. Thus if we set $R = U^t Q U = (r_{i,j})$, the first column (hence the first row) of R is divisible by p. Clearly $p^2 \nmid r_{1,1}$, otherwise $p^2 \mid \det(R) = \det(Q)$, contrary to our assumption, as can be seen by dividing by p the first row then the first column. By assumption we know that $X^t R X = 0$ has a nontrivial p-adic solution $X = (a_1, a_2, a_3)^t$, where after suitable rescaling we may assume that the a_i are p-integral with one of them a p-adic unit. I claim that either a_2 or a_3 is a p-adic unit. Indeed, otherwise we would have $v_p(a_2) \geqslant 1$, $v_p(a_3) \geqslant 1$ hence $v_p(a_1) = 0$, so setting $Y = (0, a_2, a_3)^t$ and $e_1 = (1, 0, 0)^t$ we would have

$$0 = X^t R X = a_1^2 e_1^t R e_1 + 2 a_1 Y^t R e_1 + Y^t R Y ,$$

and we would have

$$v_p(a_1^2 e_1^t R e_1) = 2v_p(a_1) + v_p(r_{1,1}) = 1 \ ,$$

$v_p(2a_1 Y^t R e_1) \geqslant 2$ (since $p \mid Y$ and $p \mid Re_1$ which is the first column of R), and $v_p(Y^t R Y) \geqslant 2$ since $p \mid Y$, leading to a contradiction and proving my claim.

Exchanging the indices 2 and 3 if necessary we may assume that $v_p(a_2) = 0$, and let $x \in \mathbb{Z}$ be such that $x \equiv a_3 a_2^{-1} \pmod{p}$. Set

$$N = \begin{pmatrix} 1 & 0 & 0 \\ 0 & p & x \\ 0 & 0 & 1 \end{pmatrix}$$

and $V = UN$. It is clear that $V \in \mathcal{M}_3(\mathbb{Z})$ with $\det(V) = p$. Furthermore the above computation of $X^t R X$ shows that $Y^t R Y \equiv 0 \pmod{p}$, hence $N_3^t R N_3 \equiv 0 \pmod{p}$, where as usual N_j denotes the jth column of N. Since $p \mid N_2$ and $N_1 = e_1$, it immediately follows that the matrix $N^t R N = V^t Q V$ is divisible by p. Thus we can replace Q by $V^t Q V / p$ whose determinant is equal to $\det(Q)/p$ hence strictly smaller than that of Q in absolute value.

Algorithmic Remarks.

(1) When $p \mid r_{2,2}$ it is not necessary to use this construction since it is immediate that $N^t R N$ is divisible by p for

$$N = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & p \end{pmatrix} \ .$$

(2) Although we have used p-adic solubility we do not need an explicit p-adic solution. We only want $N_3^t R N_3 \equiv 0 \pmod{p}$ with $N_3 = (0, x, 1)^t$, in other words a solution to the quadratic equation

$$r_{2,2} x^2 + 2 r_{2,3} x + r_{3,3} \equiv 0 \pmod{p} \ .$$

Thus we take $x \in \mathbb{Z}$ such that

$$x \equiv (-r_{2,3} + \sqrt{r_{2,3}^2 - r_{2,2} r_{3,3}}) r_{2,2}^{-1} \pmod{p} \ ,$$

and the existence of V is equivalent to the existence of the square root.

(3) We have $p \nmid (r_{2,3}^2 - r_{2,2} r_{3,3})$, otherwise $p^2 \mid \det(Q)$. Thus for $p = 2$ the square root always exists so we do not need to assume local solubility at 2 in this case.

Case 2: $v_p(\det(Q)) \geqslant 2$ **and** $d = \dim_{\mathbb{F}_p}(\mathrm{Ker}(\overline{Q})) = 1$**.** Let $U \in \mathrm{SL}_3(\mathbb{Z})$ be defined as in Case 1 and set $R = U^t Q U = (r_{i,j})$. We know that the first row and column of R are divisible by p, so expanding $\det(R)$ this implies that

$$\det(Q) = \det(R) \equiv r_{1,1} \det(S) \pmod{p^2}, \quad \text{where} \quad S = \begin{pmatrix} r_{2,2} & r_{2,3} \\ r_{3,2} & r_{3,3} \end{pmatrix} \ .$$

Since $p \mid r_{1,j}$ we cannot have $p \mid \det(S)$ otherwise the last two columns of R would be linearly dependent over $\mathbb{F}_p$ so that $d \geqslant 2$, contrary to our assumption. Thus $p \nmid \det(S)$ and since $p^2 \mid \det(Q)$ we deduce that $p^2 \mid r_{1,1}$. If we set $V = UN$ with

$$N = \begin{pmatrix} 1 & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & p \end{pmatrix}$$

it is clear that $\det(V) = p^2$ and $V^t QV$ is divisible by p^2. We thus replace Q by $V^t QV/p^2$ whose determinant is equal to $\det(Q)/p^2$ hence strictly smaller than that of Q in absolute value.

Case 3: $v_p(\det(Q)) \geqslant 2$ **and** $d = \dim_{\mathbb{F}_p}(\mathrm{Ker}(\overline{Q})) \geqslant 2$**.** Here we take for U a matrix in $\mathrm{SL}_3(\mathbb{Z})$ whose first two columns reduced modulo p are linearly independent elements of $\mathrm{Ker}(\overline{Q})$ and we set $R = U^t QU$. The first two rows and columns of R are divisible by p, hence it is clear that if we set $V = UN$ with

$$N = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & p \end{pmatrix}$$

we have $\det(V) = p$ and $V^t QV$ is divisible by p. We thus replace Q by $V^t QV/p$ whose determinant is equal to $\det(Q)/p$ hence strictly smaller than that of Q in absolute value.

Since in all three cases we have obtained a new symmetric matrix with strictly smaller determinant in absolute value, the first statement of the theorem is proved by induction. The other statements immediately follow from the proof. □

Thanks to Theorem 6.3.11 the the search for a particular solution to $X^t QX = 0$ can be algorithmically reduced to the search for a particular solution to such an equation where $\det(Q) = \pm 1$. The second result which enables us to find such a solution is based on a natural modification of the LLL algorithm (Algorithm 2.3.18) due to D. Simon.

Denote by $\cdot$ the bilinear form associated with the quadratic form Q. Since Q is indefinite, this is never a scalar product, but the notation is useful nonetheless. We will write $(x)^2$ instead of $Q(x) = x \cdot x$, since for the same reason we cannot write $Q(x) = \|x\|^2$. Thus $(x)^2$ may be negative, hence we will have to include absolute values in all the necessary inequalities.

Now let $(\mathbf{b}_j)_{1 \leqslant j \leqslant n}$ be a $\mathbb{Z}$-basis of the lattice $\Lambda = \mathbb{Z}^n$ (which is more than what we ask in the usual LLL algorithm where the $\mathbf{b}_j$ are only required to be linearly independent) and let $(\mathbf{b}_i^*)$ be the corresponding Gram–Schmidt vectors obtained using the standard formulas of Proposition 2.3.5. First note that the induction used to define these vectors may *fail* since some vector $\mathbf{b}_j^*$ may be such that $\mathbf{b}_j^* \cdot \mathbf{b}_j^* = 0$. If this happens either here or in the rest of the algorithm we are in fact happy since we have a nonzero vector $\mathbf{b}_j^*$

such that $Q(\mathbf{b}_j^*) = 0$, and since $\mathbf{b}_j^* \in \mathbb{Q}^n$ throughout the algorithm it is not necessary to search any further because this is a particular solution. We will thus implicitly assume that this never happens, so that we indeed have a Gram–Schmidt basis.

Let $\gamma > 4/3$ be fixed. We define the notion of γ-LLL reduced basis in the same way as in Definition 2.3.14, except that we must add absolute value signs to the norms: in other words we must have $|\mu_{i,j}| \leqslant 1/2$ for all $j < i$ and

$$\left|(\mathbf{b}_i^* + \mu_{i,i-1}\mathbf{b}_{i-1}^*)^2\right| \geqslant \left(\frac{1}{\gamma} + \frac{1}{4}\right)\left|(\mathbf{b}_{i-1}^*)^2\right| \ ,$$

the absolute value signs being necessary since the form Q is indefinite (we will see that in our special case we must take $4/3 < \gamma < 2$). Note that contrary to the positive definite case this is not equivalent to $|(\mathbf{b}_i^*)^2| \geqslant (1/\gamma + 1/4 - \mu_{i,i-1}^2)|(\mathbf{b}_{i-1}^*)^2|$, see Exercise 8.

Given any $\mathbb{Z}$-basis $(\mathbf{b}_j)$ of $\mathbb{Z}^n$ we apply a straightforward modification of the LLL algorithm to obtain a γ-LLL-reduced basis of $\mathbb{Z}^n$ by adding suitable absolute values in Step 3 of Algorithm 2.3.18.

The proof used in the positive definite case shows that the algorithm terminates in polynomial time and that the final basis that we obtain is in particular such that

$$1 \leqslant \left|(\mathbf{b}_1)^2\right| \leqslant \gamma^{(n-1)/2}|\det(Q)|^{1/n} \ .$$

An easy modification of the proof shows that if Q is indefinite the above inequality can be slightly improved (see [Sim1]), but this is not important although useful in practice.

The second result, although very easy, is the key to finding a particular solution.

Proposition 6.3.12. *Assume that $n \leqslant 5$, that Q is a quadratic form with integral entries such that $\det(Q) = \pm 1$, and choose γ such that $4/3 < \gamma < 2^{2/(n-1)}$. Then either we find a $\mathbf{b}_j^*$ such that $Q(\mathbf{b}_j^*) = 0$ during the algorithm (hence a particular solution), or the Gram matrix of Q on the final LLL-reduced basis is diagonal with diagonal entries equal to ± 1.*

Proof. It follows from the inequality for $|(\mathbf{b}_1)^2|$ that $1 \leqslant |(\mathbf{b}_1)^2| < 2$, hence $(\mathbf{b}_1)^2 = \pm 1$ since it is an integer. Since $\mathbf{b}_1^* = \mathbf{b}_1$, for $1 < i \leqslant n$ we have

$$\mu_{i,1} = \frac{\mathbf{b}_i \cdot \mathbf{b}_1}{(\mathbf{b}_1)^2} = \pm \mathbf{b}_i \cdot \mathbf{b}_1 \ ,$$

and since the Gram matrix has integral entries and $|\mu_{i,1}| \leqslant 1/2$ we have $\mu_{i,1} = \mathbf{b}_i \cdot \mathbf{b}_1 = 0$. It follows that $\mathbf{b}_2^* = \mathbf{b}_2$ hence we can continue the same reasoning by induction. Note that the double inequality for γ is possible only if $n \leqslant 5$, whence the restriction. □

In our case we have $n = 3$ and the inequality for γ is $4/3 < \gamma < 2$. Summarizing, to find a particular solution of X^tQX for an indefinite ternary quadratic form Q which is p-adically soluble for all $p \mid \det(Q)$ we proceed as follows. After factoring $\det(Q)$ (which is theoretically the longest part of the algorithm) we apply the algorithm implicit in the proof of Theorem 6.3.11 to find a matrix $V \in \mathcal{M}_3(\mathbb{Z})$ such that $Q_1 = V^tQV/\det(Q) \in \mathcal{M}_3(\mathbb{Z})$ and such that $\det(Q_1) = 1$. We then use the modified LLL algorithm explained above applied to Q_1 and the canonical basis of $\mathbb{Z}^3$. Then either we directly find a vector $X_1 = \mathbf{b}_j^*$ such that $Q_1(\mathbf{b}_j^*) = 0$, in which case $X = VX_1$ is a particular nontrivial solution to $X^tQX = 0$, or we find a matrix $W \in \mathrm{GL}_3(\mathbb{Z})$ such that $Q_2 = W^tQ_1W$ is a diagonal matrix with diagonal entries equal to ± 1. Since Q_2 is indefinite the signs of two diagonal entries must be opposite, hence we can trivially find a solution X_2 to $X_2^tQ_2X_2 = 0$ of the form $(1, 1, 0)^t$ up to permutation. It follows that $X = VWX_2$ is a particular nontrivial solution to $X^tQX = 0$.

6.3.4 Examples of Homogeneous Ternary Equations

We now apply the above results to a number of important special cases.

Corollary 6.3.13. *Up to exchange of x and y the general* integral *solution to the Pythagorean equation $x^2+y^2 = z^2$ is given by $x = d(s^2-t^2)$, $y = 2dst$, $z = d(s^2+t^2)$, where s, t are coprime integers of opposite parity and $d \in \mathbb{Z}$. In addition, we have $|d| = \gcd(x, y) = \gcd(x, z) = \gcd(y, z)$. The general solution with x and y coprime is (up to exchange of x and y) $x = s^2 - t^2$, $y = 2st$, $z = \pm(s^2 + t^2)$.*

This is the well-known parametrization of Pythagorean triples which we will use several times.

Proof. Using Corollary 6.3.6 with the particular solution $(1, 0, 1)$, we obtain the formulas of the corollary. If $s \equiv t \pmod 2$, we set $s_1 = (s+t)/2$ and $t_1 = (s-t)/2$, so that $s = s_1+t_1$, $t = s_1-t_1$. Then $x = 4dst$, $y = 2d(s_1^2-t_1^2)$, $z = 2d(s_1^2+t_1^2)$, which is the same parametrization with x and y exchanged and d replaced by $2d$. Since $\gcd(s, t) = 1$, s and t are odd, hence s_1 and t_1 have opposite parity, showing that we can always reduce to this case. Finally, if this is the case then $\gcd(s^2-t^2, 2st) = 1$, hence x and y are in $\mathbb{Z}$ if and only if $d \in \mathbb{Z}$ (and then $|d| = \gcd(x, y)$ and the other statement follows). Finally, if we want $\gcd(x, y) = 1$, we must have $d = \pm 1$, but two of the signs in the formulas can be absorbed by exchanging s and t, and by changing s into $-s$, proving the corollary. □

Corollary 6.3.14. (1) *Let $p = \pm 2$. The general integral solution of $x^2 + py^2 = z^2$ with x and y coprime is given by $x = \pm(s^2 - pt^2)$, $y = 2st$, $z = \pm(s^2 + pt^2)$, where s and t are coprime integers with s odd and the $\pm$ signs are independent.*

(2) *The general integral solution of* $x^2 - 2y^2 = -z^2$ *(in other words of* $x^2 + z^2 = 2y^2$*) with* x *and* y *coprime is given by* $x = \pm(s^2 - 2st - t^2)$, $y = \pm(s^2 + t^2)$, $z = \pm(s^2 + 2st - t^2)$, *where* s *and* t *are coprime integers of opposite parity and the* $\pm$ *signs are independent.*

Proof. Using Corollary 6.3.6 with the particular solution $(1, 0, 1)$ we obtain the formulas $x = d(s^2 - pt^2)$, $y = 2dst$, $z = d(s^2 + pt^2)$ where s and t are coprime integers and $d \in \mathbb{Q}$. We consider two cases.

If $2 \nmid s$, then $\gcd(s^2 - pt^2, 2st) = 1$, hence for x and y to be coprime integers we must have $d = \pm 1$, giving the first parametrization.

If $2 \mid s$ then t is odd, hence $\gcd(s^2 - pt^2, 2st) = 2$. Thus for x and y to be coprime integers we must have $d = \pm 1/2$, and this leads to another parametrization which is the same as the first with s and t exchanged and some signs changed, proving (1).

In a similar manner for (2), using the particular solution $(1, 1, 1)$ we find the parametrization $x = \pm(s^2 - 4st + 2t^2)$, $y = \pm(s^2 - 2st + 2t^2)$, $z = \pm(s^2 - 2t^2)$ with s and t coprime and s odd, and (2) follows by replacing s with $s + t$, giving the more symmetrical parametrization of the corollary. □

Corollary 6.3.15. *Let* p *be a positive or negative prime number with* $p \neq 2$. *The general integral solution of* $x^2 + py^2 = z^2$ *with* x *and* y *coprime is given by one of the following two disjoint parametrizations.*

(1) $x = \pm(s^2 - pt^2)$, $y = 2st$, $z = \pm(s^2 + pt^2)$, *where* s *and* t *are coprime integers of opposite parity such that* $p \nmid s$.

(2) $x = \pm(((p-1)/2)(s^2+t^2)+(p+1)st)$, $y = s^2 - t^2$, $z = \pm(((p+1)/2)(s^2 + t^2)+(p-1)st)$, *where* s *and* t *are coprime integers of opposite parity such that* $s \not\equiv t \pmod{p}$.

In the above, the $\pm$ *signs are independent.*

Proof. Using Corollary 6.3.6 with the particular solution $(1, 0, 1)$ we again obtain the formulas $x = d(s^2 - pt^2)$, $y = 2dst$, $z = d(s^2 + pt^2)$ where s and t are coprime integers and $d \in \mathbb{Q}$. We consider two cases.

If $p \nmid s$, we easily check that $\gcd(s^2 - pt^2, 2st) = \gcd(s^2 - pt^2, 2)$, and since p is odd, this is equal to 1 if s and t have opposite parity, and to 2 otherwise. If it is equal to 1, for x and y to be coprime integers we must have $d = \pm 1$, giving the first parametrization. If it is equal to 2, then s and t have the same parity, hence are both odd. We set $s_1 = (s + t)/2$, $t_1 = (t - s)/2$ which are coprime of opposite parity such that $p \nmid (s_1 - t_1)$, and we obtain $x = -d((p - 1)(s_1^2 + t_1^2) + 2(p + 1)s_1t_1)$, $y = 2d(s_1^2 - t_1^2)$, $z = d((p + 1)(s_1^2 + t_1)^2 + 2(p - 1)s_1t_1)$. For x and y to be coprime integers we must have $d = \pm 1/2$, giving the second parametrization.

If $p \mid s$, then $p \nmid t$, so if we exchange s/p and t and change d into d/p we reduce to the preceding case, up to the sign of x which plays no role, hence we do not obtain any extra parametrizations. □

6.3.5 The Pell–Fermat Equation $x^2 - Dy^2 = N$

Introduction and Reductions.

A degree 2 equation of another kind which deserves special mention is the Pell–Fermat equation, often simply called the Pell equation. [1] This equation is $x^2 - Dy^2 = N$ for given integers D and N, to be solved in integers x and y. It is evidently closely linked to the arithmetic properties of $\mathbb{Q}(\sqrt{D})$. Its nature is very different from that of the degree two equations that we have studied above for two reasons. First, it is not a homogeneous equation. But most importantly, we want the solutions in *integers*, and not in rational numbers. Indeed, finding for instance the *rational* solutions to $x^2 - Dy^2 = 1$ is very easy, see Exercise 10.

We make a number of reductions.

• We may assume that $D \geqslant 0$, otherwise there are only a finite number of pairs (x, y) to be checked. This can be done either in a naïve manner, or more intelligently by working in the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ and using a computer algebra system (CAS) to check whether or not N is the norm of an element.

• We may assume that D is not a square, otherwise if $D = d^2$ the equation can be written $(x - dy)(x + dy) = N$, hence it is only a matter of listing all (positive or negative) divisors g of N such that $g + N/g$ is even and $d \mid (N/g - g)$.

• Hence we are reduced to working in the real quadratic field $\mathbb{Q}(\sqrt{D})$, where D is not necessarily the discriminant of the field. As in the case $D < 0$, the *existence* of a solution can be proved intelligently by using a CAS to check whether N is the norm of an element in the real quadratic *order* $\mathbb{Z}[\sqrt{D}]$. If a solution does exist, multiplicativity of the norm (equivalent to the simple identity $(x^2 - Dy^2)(z^2 - Dt^2) = (xz + Dyt)^2 - D(xt + yz)^2$) implies that the general solution is obtained by multiplying the corresponding element $x + y\sqrt{D}$ of the quadratic field by a *unit* of norm 1, i.e., a solution to $x^2 - Dy^2 = 1$.

Once these reductions are made, it is natural to consider the following three special cases.

(1) $x^2 - Dy^2 = 1$.
(2) $x^2 - Dy^2 = \pm 1$, where ± 1 means that we accept both signs as solutions.
(3) $x^2 - Dy^2 = \pm 4$, when $D \equiv 0$ or 1 modulo 4.

We note that each equation is a special case of the next one. Indeed, if (x, y) is a solution of (1), it is also a solution of (2). But conversely, we will see that the set of solutions of (2) has the form $x + y\sqrt{D} = \pm(x_0 + y_0\sqrt{D})^k$ for any $k \in \mathbb{Z}$, and then either (x_0, y_0) is already a solution of (1), in which

[1] Since there are so many theorems and equations named after Fermat, history has attached the name of the British mathematician Pell to this equation, although apparently his only merit was to have corresponded with Fermat on the subject.

case all solutions of (2) are also solutions of (1), or it is not, in which case it is immediately seen that the solutions of (1) are the solutions of (2) with k *even*. In both cases the solutions of (1) are also given by $x+y\sqrt{D} = \pm(x_0+y_0\sqrt{D})^k$ for any $k \in \mathbb{Z}$ for suitable (possibly different) (x_0, y_0).

Finally, if (x, y) is a solution of (2), then (X, y) is a solution of (3) with $X = 2x$ and D replaced by $4D$. Conversely, any solution to $X^2 - DY^2 = \pm 4$ with $X \equiv 0 \pmod 2$ gives a solution to $x^2 - (D/4)y^2 = \pm 1$ with $x = X/2$. This is automatic if $D \equiv 0 \pmod 4$. If $D \equiv 1 \pmod 4$ and X (hence Y) is odd, then we obtain a solution to $x^2 - Dy^2 = \pm 1$ by setting $x = X(X^2 + 3DY^2)/8$ and $y = Y(3X^2+DY^2)/8$, which are easily seen to be integral, and correspond to the identity $x + y\sqrt{D} = ((X + Y\sqrt{D})/2)^3$.

To summarize, what we will call *the* Pell equation is an equation of the form $x^2 - Dy^2 = \pm 4$ with $D > 0$ nonsquare and congruent to 0 or 1 modulo 4. There are two main results concerning this equation. One deals with the structure of the set of solutions, the other with the algorithmic construction of that set.

The Structure Theorem.

Proposition 6.3.16. *If $D > 0$ is not a square and is congruent to 0 or 1 modulo 4 the Pell equation $x^2 - Dy^2 = \pm 4$ has an infinity of solutions given in the following way. If (x_0, y_0) is a solution with the least strictly positive y_0 (and $x_0 > 0$, say), the general solution is given by*

$$\frac{x + y\sqrt{D}}{2} = \pm \left(\frac{x_0 + y_0\sqrt{D}}{2} \right)^k$$

for any $k \in \mathbb{Z}$.

Proof. The equation can be written $\mathcal{N}(\varepsilon) = \pm 1$, with $\varepsilon = (x + y\sqrt{D})/2$, and since x and y are integers and $x \equiv Dy \pmod 2$, ε is an algebraic integer of norm equal to ± 1, hence a unit. Since the set of elements of the form $(x+y\sqrt{D})/2$ with $x \equiv yD \pmod 2$ is the quadratic order of discriminant D, we must thus find the structure of the group of units of this order.

Let D_0 be the discriminant of the quadratic field $\mathbb{Q}(\sqrt{D})$, so that $D = D_0 f^2$ for some positive integer f. We prove the result by induction on the number of prime factors of f. If $f = 1$, by an easy special case of Dirichlet's unit theorem we know that $\varepsilon = \pm\varepsilon_0^k$ for some sign $\pm$ (having nothing to do with the sign of the equation), and $k \in \mathbb{Z}$, where ε_0 is the fundamental unit of $\mathbb{Q}(\sqrt{D_0})$, i.e., the solution of the equation with the smallest strictly positive y.

Assume now that f is arbitrary, and by induction that the result has been proved for all $g \mid f$ having a strictly smaller number of prime factors. We can thus write $D = D_1 p^2$, where p is a prime, and by induction we may assume that the result has already been proved for D_1. Thus, our Pell equation can

be written $x^2 - D_1(py)^2 = \pm 4$, so that by induction the equation is equivalent to

$$\frac{x + py\sqrt{D_1}}{2} = \pm \left(\frac{x_1 + y_1\sqrt{D_1}}{2}\right)^k ,$$

where $\varepsilon_1 = (x_1 + y_1\sqrt{D_1})/2$ is the fundamental unit of the order of discriminant D_1. We have

$$\pm py = \frac{((x_1 + y_1\sqrt{D_1})/2)^k - ((x_1 - y_1\sqrt{D_1})/2)^k}{\sqrt{D_1}} ..$$

It will thus be sufficient to prove the following lemma.

Lemma 6.3.17. *The set of $k \in \mathbb{Z}$ such that $(\varepsilon_1^k - \overline{\varepsilon_1}^k)/\sqrt{D_1} \in p\mathbb{Z}$ has the form $k_0\mathbb{Z}$ where $k_0 \mid p - \left(\frac{D_1}{p}\right)$.*

Proof. We may clearly assume that $p \nmid y_1$ otherwise we can choose $k_0 = 1$. Assume first that $p \neq 2$. If $p \mid D_1$, expanding the right hand side gives $\pm 2^{k-1} py \equiv k x_1^{k-1} y_1 \pmod{p}$, so that the set of suitable k is $p\mathbb{Z}$ if $p \nmid x_1 y_1$, and $\mathbb{Z}$ otherwise, so that $k_0 = p$ or 1 respectively. Otherwise, ε_1, $\overline{\varepsilon_1}$ can be considered as *distinct* elements e_1 and $\overline{e_1}$ of $\mathbb{F}_{p^2}$ (since $(e_1 - \overline{e_1})^2 = y_1^2 D_1 \neq 0$ since $p \nmid y_1$), so our equation is equivalent to $(\overline{e_1}/e_1)^k = 1$. The first claim of the lemma is thus proved, with k_0 being equal to the order of $(\overline{e_1}/e_1)$ in $\mathbb{F}_{p^2}$. For the second, we note that if $\left(\frac{D_1}{p}\right) = 1$ then in fact $e_1 \in \mathbb{F}_p$ hence $k_0 \mid (p-1)$. On the other hand if $\left(\frac{D_1}{p}\right) = -1$ then by the theory of finite fields we have $\overline{e_1} = e_1^p$ (the action of the Frobenius automorphism). This can also be seen directly by applying the Frobenius automorphism to the equation $e_1^2 - x_1 e_1 \pm 1 = 0$. Thus the order of $\overline{e_1}/e_1 = e_1^{p-1}$ divides $(p^2-1)/(p-1) = p+1$, proving the lemma, hence the proposition. □

The Algorithmic Method.

Now that we know the structure of the solution set of $x^2 - Dy^2 = \pm 4$, it remains to find in an efficient manner the fundamental solution (x_0, y_0) or, equivalently, the fundamental unit of the quadratic order of discriminant D. There are essentially four methods for doing this, which differ by their complexity. The first is the naïve method, consisting in trying $y = 1$, 2 etc..., until $Dy^2 \mp 4$ is a square. This method is absolutely correct but highly inefficient, since one can prove that the number of *binary digits* of y_0 may be often larger than $\sqrt{D}$. Thus, the running time can be of order $O(\exp(D^{1/2}))$. In fact, since the result we are computing is so large, the fundamental unit must be *represented* in a nontrivial manner (the so-called *compact representation*, see [Coh0]), which we will not discuss here. We will always assume that this representation is used.

The second method uses *continued fractions*, and will be described more precisely in a moment. Its running time has order $O(D^{1/2})$.

The third method is a remarkable improvement of the continued fraction method due to D. Shanks, using a combination of two of his most important algorithmic ideas: the *baby-step giant-step* method and the *infrastructure* of the continued fraction cycle. We refer the reader to [Coh0], Chapter 5 for a detailed description of these ideas and algorithms. The running time of this method has order $O(D^{1/4})$.

The fourth method is a combination of the third method with a method coming from the theory of factoring, the use of *factor bases*, introduced in this context by J. Buchmann. Its heuristic running time, well supported by practical evidence, is *subexponential*, of order $O(\exp(c\sqrt{\log(D)\log(\log(D))}))$ for a small strictly positive constant c. Using this record-breaking method, it is possible to compute the fundamental unit in a reasonable amount of time for discriminants up to 10^{80}, say.

The continued fraction method is based on the following result, which is not difficult but which we will not prove.

Proposition 6.3.18. *Let $D > 0$ be a nonsquare integer congruent to 0 or 1 modulo 4. Denote by r the largest integer such that $r^2 < D$ and $r \equiv D \pmod 2$. The continued fraction expansion of the quadratic number $\alpha = (r + \sqrt{D})/2$ is purely periodic. Furthermore, if $(a_0, a_1, \ldots, a_{n-1})$ is the period of that expansion, then the rational number p_{n-1}/q_{n-1} whose continued fraction expansion is given by that period is such that $\varepsilon = p_{n-1} - q_{n-1}(r - \sqrt{D})/2$ is a fundamental unit of the quadratic order of discriminant D.*

To apply this proposition we simply note that to compute the continued fraction expansion of a quadratic number we must *not* compute any decimal or other approximation to the number, but work formally directly only on quadratic numbers. We leave the (easy) details to the reader, or refer once again to [Coh0].

6.4 Diophantine Equations of Degree 3

6.4.1 Introduction

In the case of a Diophantine equation of degree 3 or higher (or of several equations of degree 2), a new and very annoying phenomenon occurs: the failure of the Hasse principle. In other words our equations may be everywhere locally soluble without having a global solution. We have already seen examples of this in the preceding chapter, and we will see more here. Note that it is usually very easy to check for local solubility everywhere. On the other hand to prove that a Diophantine equation has no global solutions is often very difficult, and often gives rise to unsolved problems. Even in the

simplest case of homogeneous equations of degree 3 in 3 variables, no algorithm is known, and it would be a remarkable advance in number theory to find one.

We thus consider Diophantine equations of the form $f(x_1, \ldots, x_n) = 0$, where f is a homogeneous polynomial of degree 3 with integral coefficients. We will always assume that f is nonsingular (in other words that the partial derivatives of f do not simultaneously vanish except at the origin), otherwise the problem is much easier and essentially reduced to Diophantine equations of degree 1 or 2. When $n = 2$ there is nothing much to say since by dehomogenizing the equation the problem boils down to the determination of rational roots of a polynomial in one variable, which can easily be done (see Exercise 11). When $n = 3$ then *if we know a nontrivial solution* we are by definition dealing with an elliptic curve, and we will see in Section 7.2.4 how to transform our equation into an equivalent one in *Weierstrass form* $y^2z = x^3 + axz^2 + bz^3$ for suitable a and b. We will devote the whole of Chapter 8 to the study of the global solubility of such equations. In particular we will prove the Mordell–Weil theorem which states that the set of rational points on the corresponding projective curve is a finitely generated abelian group.

When $n \geqslant 4$, contrary to the case of quadratic forms, there is no really simple reduction to a canonical form. For $n = 4$ we are dealing with a *cubic surface* S. If P and Q are distinct rational points on S, the line through P and Q either intersects S in a single third point which must be rational, or is entirely contained in S, so that we obtain new points by this secant process. Starting from a single point P we can consider the tangent plane of S at P. It will intersect S along a singular cubic curve, and any tangent at P with rational slope will intersect this curve, hence S, at a third point, which will also be rational, or again be entirely contained in S. This will be called a tangent process. We will see that for elliptic curves this does lead to the whole set of rational points starting from a finite number (the Mordell–Weil theorem). There is a conjecture of Yu. Manin which states that the same should be true here:

Conjecture 6.4.1 (Manin). *Let S be a cubic surface defined by a projective equation $f(x_1, x_2, x_3, x_4) = 0$ where f has integer coefficients and is nonsingular. There exist a* finite *number of rational points $P_1, \ldots, P_r$ on S such that any rational point of S can be obtained from them by a succession of secant and tangent processes.*

In view of all the above, in this section we will consider *diagonal equations*, in other words equations of the form $\sum_{1 \leqslant i \leqslant n} a_i x_i^3 = 0$, or inhomogeneous versions.

6.4.2 General Equations $ax^3 + by^3 + cz^3 = 0$

These equations were widely studied in the 19th century, and important results on them were obtained later by Selmer and Cassels. We begin by local solubility.

First note that, even if a, b, or c are initially in $\mathbb{Q}$, after multiplying by a suitable denominator we may assume that they are integers such that $\gcd(a,b,c) = 1$. Furthermore we may also assume that a, b and c are cubefree (in other words not divisible by the cube of a prime), since if for instance $p^3 \mid a$, we can rewrite our equation as $(a/p^3)(px)^3 + by^3 + cz^3 = 0$ (see Exercise 13 however). We will always implicitly or explicitly make these two reductions in the sequel.

The question of local solubility is answered by the following proposition.

Proposition 6.4.2. *Let a, b and c be nonzero cubefree integers such that* $\gcd(a,b,c) = 1$.

(1) *The equation $ax^3 + by^3 + cz^3 = 0$ has a nontrivial solution in $\mathbb{R}$ and in every $\mathbb{Q}_p$ for which $p \nmid 3abc$.*

(2) *Let $p \mid abc$, $p \neq 3$, reorder a, b, c so that $v_p(a) \leqslant v_p(b) \leqslant v_p(c)$, and let $\mathbf{v} = (v_p(a), v_p(b), v_p(c))$.*
   a) If $\mathbf{v} = (0,1,2)$ the equation has no nontrivial solutions in $\mathbb{Q}_p$.
   b) If $\mathbf{v} = (0,1,1)$ or $\mathbf{v} = (0,2,2)$, set $\alpha = c/b$, while if $\mathbf{v} = (0,0,1)$ or $\mathbf{v} = (0,0,2)$ set $\alpha = a/b$. The equation has a nontrivial solution in $\mathbb{Q}_p$ if and only if α is a cube in $\mathbb{F}_p^*$.

(3) *Let $p = 3$, reorder a, b, c and define $\mathbf{v}$ as above.*
   a) If $\mathbf{v} = (0,1,2)$ the equation has no nontrivial solutions in $\mathbb{Q}_3$.
   b) If $\mathbf{v} = (0,0,1)$ or $\mathbf{v} = (0,2,2)$ the equation has nontrivial solutions in $\mathbb{Q}_3$.
   c) If $\mathbf{v} = (0,0,0)$ the equation has a nontrivial solution in $\mathbb{Q}_3$ if and only if either $a \pm b \equiv 0 \pmod 9$, $a \pm c \equiv 0 \pmod 9$, or $b \pm c \equiv 0 \pmod 9$.
   d) If $\mathbf{v} = (0,0,2)$ the equation has a nontrivial solution in $\mathbb{Q}_3$ if and only if $a \pm b \equiv 0 \pmod 9$ for a suitable sign $\pm$.
   e) If $\mathbf{v} = (0,1,1)$ the equation has a nontrivial solution in $\mathbb{Q}_3$ if and only if $b/3 \pm c/3 \equiv 0 \pmod 9$ for a suitable sign $\pm$.

Proof. It is clear that our equation has a nontrivial solution in $\mathbb{R}$. Since it represents a nonsingular projective cubic curve, it has genus 1. Thus, if $N(\mathbb{F}_p)$ denotes the number of projective points on this curve with coordinates in $\mathbb{F}_p$, the general bounds (see Corollary 2.5.27) or here more simply Hasse's theorem imply that when $p \nmid 3abc$ we have $(p^{1/2}-1)^2 < N(\mathbb{F}_p) < (p^{1/2}+1)^2$, and in particular $N(\mathbb{F}_p) > (2^{1/2}-1)^2$ is nonzero.

(1). Assume first that $p \nmid 3abc$. Let (x_0, y_0, z_0) be a solution modulo p with $p \nmid x_0$, say. We fix y_0 and z_0 and consider $f(X) = aX^3 + (by_0^3 + cz_0^3)$. We know that $f(x_0) \equiv 0 \pmod p$ and $p \nmid x_0$, hence $v_p(f'(x_0)) = 0$ since $p \nmid 3a$. It

follows that we may apply Hensel's Lemma 4.1.37, which tells us that there exists $x \in \mathbb{Q}_p$ such that $f(x) = 0$.

(2). Assume now that $p \mid abc$ with $p \neq 3$, reorder a, b, c as in the proposition, and let (x, y, z) be a nontrivial solution in $\mathbb{Q}_p$. Multiplying by a suitable element of $\mathbb{Q}_p$ we may assume that x, y, and z are in $\mathbb{Z}_p$ and that one of them at least is a p-adic unit, and hence at most one is *not* a p-adic unit. With a slight abuse of notation we will write $p \mid x$ to mean that $x \in p\mathbb{Z}_p$.

It is clear that if $\mathbf{v} = (0, 1, 2)$ then $ax^3 + by^3 \equiv 0 \pmod{p^2}$, hence $p \mid x$, hence $by^3 \equiv 0 \pmod{p^2}$ hence $p \mid y$ since $v_p(b) = 1$, which is absurd since x or y is a p-adic unit, so the equation is not soluble in $\mathbb{Q}_p$ in this case. If $\mathbf{v} = (0, 0, 1)$ or $\mathbf{v} = (0, 0, 2)$ then a necessary condition for solubility in $\mathbb{Q}_p$ is that $ax^3 + by^3 \equiv 0 \pmod{p}$ be nontrivially soluble, in other words that a/b be a cube in $\mathbb{F}_p$. But conversely if this is the case, we can choose $z = 0$ and Hensel's lemma tells us that a/b is a cube in $\mathbb{Z}_p$ since $p \neq 3$. If $\mathbf{v} = (0, k, k)$ with $k = 1$ or 2 then necessarily $p \mid x$, so our equation is equivalent to $(ap^{3-k})(x/p)^3 + (b/p^k)y^3 + (c/p^k)z^3 = 0$, which has the form that we have just studied, hence is soluble in $\mathbb{Q}_p$ if and only if b/c is a cube in $\mathbb{F}_p$.

(3). This case is similar, but we must be more careful in the application of Hensel's lemma. As above it is clear that if $\mathbf{v} = (0, 1, 2)$ the equation is not soluble in $\mathbb{Q}_3$. A necessary condition for solubility in $\mathbb{Q}_3$ is solubility modulo 9. Since a cube is congruent to 0 or ± 1 modulo 9, and since at most one of x, y, and z is in $3\mathbb{Z}_3$, we must have either $a \pm b$, $a \pm c$, $b \pm c$ or $a \pm b \pm c$ congruent to 0 modulo 9. Assume first that $v_3(a) = v_3(b) = 0$, so that $a \equiv \varepsilon b \pmod{3}$ for a suitable $\varepsilon = \pm 1$. If $a \equiv \varepsilon b \pmod{9}$ we choose $z = 0$, $y = -\varepsilon$, and $x = (1 - (a - \varepsilon b)/a)^{1/3}$, which exists in $\mathbb{Q}_3$ since $|(a - \varepsilon b)/a|_3 = 1/9$. If in addition $v_3(c) = 0$, we obtain the same results by symmetry if $a \pm c$ or $b \pm c$ is divisible by 9. If $a \equiv \varepsilon_1 b + \varepsilon_2 c$ with $\varepsilon_i = \pm 1$, we choose $y = -\varepsilon_1$, $z = -\varepsilon_2$, and $x = (1 - (a - \varepsilon_1 b - \varepsilon_2 c)/a)^{1/3}$. Now it is an easy exercise to show that if $\mathbf{v} = (0, 0, 0)$ then $b \pm c$ is congruent to $\pm b$ or to $\pm c$ modulo 9, implying c), and that if $\mathbf{v} = (0, 0, 1)$ then the six numbers $\pm b$ and $\pm b \pm c$ modulo 9 are not congruent modulo 9 and not divisible by 3, so that a is necessarily congruent to one of them, proving the first part of b). Finally, as in case (2), if $v_3(b) = v_3(c) = k$ with $k = 1$ or 2 the equation is equivalent to $(a3^{3-k})(x/3)^3 + (b/3^k)y^3 + (c/3^k)z^3 = 0$ which is one that we have already studied, and we simply translate the conditions that we have found, proving the proposition. □

Lemma 6.4.3. *Let a, b, c be cubefree integers. If the equation $ax^3 + by^3 + cz^3 = 0$ has a nontrivial solution with x, y, z in $\mathbb{Q}$, it has a nontrivial solution with x, y, z in $\mathbb{Z}$ pairwise coprime. Furthermore, if in addition a, b and c are pairwise coprime, then ax^3, by^3 and cz^3 are pairwise coprime.*

Proof. Clearly by multiplying x, y and z by a common denominator we may assume that they are in $\mathbb{Z}$. Then, dividing all three by $\gcd(x, y, z)$, we may assume that $\gcd(x, y, z) = 1$. Assume by contradiction that p is a prime

such that $p \mid \gcd(x,y)$. It follows that $p^3 \mid ax^3 + by^3 = -cz^3$, and since c is cubefree, we have $p \mid z$, a contradiction. Thus x, y and z are pairwise coprime. If in addition a, b and c are pairwise coprime, assume by contradiction that there exists a prime p dividing ax^3 and by^3, so that p also divides cz^3. Clearly either $p \mid x$ or $p \mid a$. If $p \mid x$, then $p \nmid yz$, hence $p \mid \gcd(b,c)$, absurd. If $p \mid a$, then $p \nmid b$ and $p \nmid c$, hence $p \mid \gcd(y,z)$, also absurd, proving the lemma. □

6.4.3 The Equations $x^3 + y^3 + cz^3 = 0$

This equation has the evident solution $(x,y,z) = (1,-1,0)$ hence is everywhere locally soluble, so we are now going to study whether it has global rational solutions with $xyz \neq 0$. Note that proving that the equation has no such solutions for $c = 1$ is Fermat's "last theorem" for exponent 3, which was probably already solved by Fermat using the method of infinite descent, together with a touch of algebraic number theory, although a proof was only given later by Euler. Also for $c = 1$, a (slightly) more complicated proof which generalizes to the more general Fermat equation $x^p + y^p + z^p = 0$ for so-called *regular* prime exponents will be given in Proposition 6.9.14 below.

Note that the solubility of the equation $x^3 + y^3 + cz^3 = 0$ with $z \neq 0$ is equivalent to the representability of c as a sum of two rational cubes. This question will be considered in more detail (but without proofs) in Section 6.4.5.

We begin by the following proposition, which is typical of the type of reasoning which one uses to solve Diophantine equations by factoring and algebraic number theory. We will see many other such examples in this chapter and in Chapter 14.

Proposition 6.4.4. *The equation $x^2 - 3xy + 3y^2 = z^3$ with x and y coprime integers has the three disjoint parametrizations*

$$(x,y,z) = (s^3 + 3s^2t - 6st^2 + t^3, 3st(s-t), s^2 - st + t^2)\ ,$$
$$(x,y,z) = (s^3 + 3s^2t - 6st^2 + t^3, s^3 - 3st^2 + t^3, s^2 - st + t^2)\ ,$$
$$(x,y,z) = ((s+t)(s-2t)(2s-t), s^3 - 3st^2 + t^3, s^2 - st + t^2)\ ,$$

where in all three s and t are coprime integers such that $3 \nmid s + t$, and the parametrizations correspond to solutions where $6 \mid y$, $6 \mid x - y$, and $6 \mid x - 2y$ respectively.

Proof. Let $j = (-1 + \sqrt{-3})/2$ be a primitive cube root of unity. In the principal ideal domain $\mathbb{Z}[j]$ our equation factors as $(x - (1-j)y)(x - (1-j^2)y) = z^3$. If $\mathfrak{p}$ is a prime ideal of $\mathbb{Z}[j]$ which divides the two factors on the left then $\mathfrak{p}$ divides their difference and $(1-j)$ times the second minus $(1-j^2)$ times the first, hence $\mathfrak{p}$ divides $(1-j)\gcd(x,y)$, hence $\mathfrak{p} \mid (1-j)$ since x and y are coprime, so that $3 \mid z$. However this would imply $3 \mid x$, hence $9 \mid 3y^2$, hence $3 \mid y$, contradicting $\gcd(x,y) = 1$. Thus $3 \nmid z$ and the

two factors on the left are coprime. It follows that there exist $\alpha \in \mathbb{Z}[j]$ and an integer k with $0 \leqslant k \leqslant 2$ such that $x-(1-j)y = j^k\alpha^3$, hence $z = \alpha\overline{\alpha}$. Writing $\alpha = s+tj$, the condition $3 \nmid z$ translates into $3 \nmid s+t$, and choosing successively $k = 0$, 1, and 2 gives the three parametrizations, where in the second we have exchanged s and t. The divisibilities by 6 are trivially checked, and show that the parametrizations are disjoint. □

Thanks to this proposition we can now prove that many of our equations $x^3+y^3+cz^3 = 0$ do not have any global solutions with $xyz \neq 0$:

Theorem 6.4.5. (1) *Let p be a prime number such that $p \equiv 2 \pmod 3$. The equation $x^3+y^3+cz^3 = 0$ has no solutions in nonzero integers x, y and z when $c = 1$, 3, p or p^2 with $p \equiv 2$ or 5 modulo 9, except for $c = 2$ where it has the unique solution $(x,y,z) = (1,1,-1)$ (up to multiplication by a constant).*

(2) *If p is a prime number such that $p \equiv 8 \pmod 9$, the equation $x^3+y^3+cz^3 = 0$ has no nontrivial solutions with $3 \mid z$ when $c = p$ or p^2.*

(3) *If p and q are prime numbers such that $p \equiv 2 \pmod 9$ and $q \equiv 5 \pmod 9$, the equation $x^3+y^3+cz^3 = 0$ has no nontrivial solutions with $3 \mid z$ when $c = pq$.*

Proof. We may clearly assume that x, y, and z are pairwise coprime integers. We prove all the results simultaneously, and consider two cases.
Case 1: $3 \mid cz$. Then $3 \mid x+y$, hence $3 \mid (x^2-xy+y^2) = ((x+y)^2-3xy)$, so that $9 \mid cz^3 = -(x^3+y^3)$. Since $9 \nmid c$ it follows that $3 \mid z$, so we set $y_1 = (x+y)/3$, $z_1 = -z/3$ and our equation is $y_1(x^2-3xy_1+3y_1^2) = 3cz_1^3$. Since y_1 and x are coprime the two factors on the left are coprime. Since $3 \mid z$ we have $3 \nmid x$ hence $3 \mid y_1$. Furthermore if a prime number ℓ divides $x^2-3xy_1+3y_1^2$ then $\ell \nmid y_1$, and we check that $(2x/y_1)-3$ is a square root of -3 modulo ℓ, hence $\ell \equiv 1 \pmod 3$. Since in all cases considered in the theorem c has no such prime divisors, it follows that $x^2-3xy_1+3y_1^2$ is coprime to $3c$. Therefore our equation implies that there exist coprime integers a and b such that $y_1 = 3ca^3$ and $x^2-3xy_1+3y_1^2 = b^3$. By Proposition 6.4.4 this last equation has three disjoint parametrizations, but we keep only the first since we know that $3 \mid y_1$. Thus there exist coprime integers s and t with $3 \nmid s+t$ such that in particular $y_1 = 3st(s-t)$, hence $ca^3 = st(s-t)$. To symmetrize we write $u = -s$, $v = t$, $w = s-t$, which are pairwise coprime and satisfy $u+v+w = 0$ and $uvw = c(-a)^3$.

In statements (1) and (2) of the theorem, c is a power of a prime, and since s and t are coprime it follows that c divides one and only one of u, v, or w, and without loss of generality we may assume that $c \mid w$. Then c is coprime to u and v, so that $u = e^3$, $v = f^3$, $w = cg^3$, and hence $e^3+f^3+cg^3 = 0$, so we have found a new solution to our initial equation. Clearly $efg \neq 0$, and it is easily checked that $|efg| < |xyz|$, so that the magic of Fermat's descent method applies: if we had started with a nontrivial solution with minimal

$|xyz|$, we would thus obtain a smaller one, a contradiction which proves the impossibility of the initial equation.

In (3), we have $c = pq$. Then up to permutation of u, v, and w, either $pq \mid w$, or $p \mid v$ and $q \mid w$. But in this last case, we would have $u = e^3$, $v = pf^3$, $w = qg^3$, hence $e^3 + pf^3 + qg^3 = 0$. Since a cube is congruent to 0 or ± 1 modulo 9 and $p \equiv 2 \pmod 9$ and $q \equiv 5 \pmod 9$, it is easily checked that the congruence $e^3 + pf^3 + qg^3 \equiv 0 \pmod 9$ implies that e, f, and g are all divisible by 3, which is absurd since u, v, and w are pairwise coprime. Thus this case is impossible, so that $pq = c \mid w$ and we can descend as above.

Case 2: $3 \nmid cz$. Thus here $c = 1$, p or p^2 where $p \equiv 2$ or 5 modulo 9. In the special case $c = 1$ our equation is completely symmetrical in x, y, and z, so we may assume $3 \nmid xyz$, and we deduce an immediate contradiction modulo 9 since we have x^3, y^3 and z^3 all congruent to ± 1 modulo 9. Thus we assume $c = p$ or p^2.

We set here $y_1 = x + y$, so our equation is $y_1(y_1^2 - 3xy_1 + 3x^2) = -cz^3$, and since $3 \nmid z$, we have $3 \nmid y_1$ hence the factors on the left are coprime. As above a prime $p \equiv 2 \pmod 3$ cannot divide $y_1^2 - 3xy_1 + 3x^2$ when x and y_1 are coprime, so that there exist integers a and b such that $y_1 = ca^3$, $y_1^2 - 3xy_1 + 3x^2 = b^3$. By Proposition 6.4.4 once again this last equation has three disjoint parametrizations. However we note that $3 \nmid x$ and $3 \nmid y$, otherwise $x^3 + y^3 \equiv \pm 1 \pmod 9$, hence $c \equiv \pm 1 \pmod 9$, which is impossible when $c \equiv 2$ or 5 modulo 9 (this is where we must exclude 8 modulo 9, for which the theorem would be false). Thus we can keep only the third parametrization, for which $x \equiv y \pmod 3$, and we deduce that there exist coprime s and t with $3 \nmid s+t$ such that in particular $y_1 = (s+t)(s-2t)(2s-t)$. To symmetrize we set $u = s + t$, $v = s - 2t$, $w = t - 2s$ which are pairwise coprime since $3 \nmid s + t$, and satisfy $u + v + w = 0$ and $uvw = c(-a)^3$. Exactly the same reasoning as in the first case allows us to conclude that the descent method works, with one exception: if $c = 2$ and $x = y = -z = 1$, we obtain the *same* solution. Thus the descent also works in this case and shows that $(x, y, z) = (1, 1, -1)$ is the only solution. □

Remarks.

(1) As already mentioned, this theorem includes in particular Fermat's last theorem for exponent 3.

(2) It is clear that the theorem is still valid for $c = p^k$ for all k if $p \equiv 2$ or 5 modulo 9, since it is then a special case of $x^3 + y^3 + p^m z^3 = 0$ with $m = 0$, 1 or 2.

(3) When $c = p \equiv 8 \pmod 9$, not only solutions may exist, but we will see below that as a consequence of the BSD conjecture solutions should exist for every p. For instance we have $18^3 + (-1)^3 + 17(-7)^3 = 0$.

(4) When $c = 3^2$ there is the trivial solution $(x, y, z) = (1, 2, -1)$, and it is immediate to check using the methods of Chapter 8 that this gives a point of infinite order on the corresponding elliptic curve, so that there exist

an infinity of distinct coprime solutions. On the other hand for $c = 2$ the above descent method shows that $(x, y, z) = (1, 1, -1)$ is the only coprime solution (up to sign), and this means that the point is a *torsion point* on the corresponding elliptic curve.

(5) When $c = pq$ with p and q primes such that $p \equiv 2 \pmod 9$ and $q \equiv 5 \pmod 9$, there are in fact no solutions also when $3 \nmid z$, see Exercise 15.

6.4.4 The Equations $x^3 + by^3 + cz^3 = 0$

We first note that over an integral domain of characteristic zero the equation $ax^3 + by^3 + cz^3 = 0$ is equivalent to the equation $X^3 + BY^3 + Cz^3 = 0$ with for instance $B = a^2b$, $C = a^2c$, and $(X, Y, Z) = (ax, y, z)$. It is thus sufficient to study such equations with $a = 1$.

We will study these equations in great detail, and apply to them a number of different methods. In the present chapter, we will use tools of algebraic number theory (class numbers, units, etc...) to give sufficient conditions which imply that these equations are everywhere locally soluble, but are not soluble in $\mathbb{Q}$. Note that, contrary to the Fermat equations of the preceding section, there are no "evident" solutions. In Chapter 8 we will find further results on this equation in two ways. First, an elementary computation of the torsion subgroup of the associated elliptic curve will give an additional sufficient condition for nonglobal solubility (Corollary 8.1.15). Then using 3-descent we will give in Section 8.4.5 a complete theoretical solution to the existence of a global solution, which unfortunately relies on the explicit computation of the Mordell–Weil group of the associated elliptic curve, which is feasible in practice for small cases, but which is one of the major unsolved algorithmic problems on elliptic curves.

We begin by a few lemmas.

Lemma 6.4.6. *Let c be a cubefree integer different from ± 1, set $\theta = c^{1/3}$, let $K = \mathbb{Q}(\theta)$, let $f = [\mathbb{Z}_K : \mathbb{Z}[\theta]]$ be the index of $\mathbb{Z}[\theta]$ in $\mathbb{Z}_K$, let m be a nonzero integer, and let u_0, u_1, and u_2 be integers.*

(1) *If $m \mid (u_0 + u_1\theta)\mathbb{Z}_K$ then $m \mid \gcd(u_0, u_1)$.*
(2) *If $m \mid (u_0 + u_1\theta + u_2\theta^2)\mathbb{Z}_K$ then $m \mid f \gcd(u_0, u_1, u_2)$.*

Proof. (1). Set $\alpha = (u_0 + u_1\theta)/m$, so that $(m\alpha - u_0)^3 - cu_1^3 = 0$. The characteristic polynomial of α is thus $X^3 - (3u_0/m)X^2 + (3u_0^2/m^2)X - (u_0^3 + cu_1^3)/m^3$. Since α is an algebraic integer the coefficients of this polynomial are in $\mathbb{Z}$, and in particular $m^2 \mid 3u_0^2$, hence $m \mid u_0$, so that $m^3 \mid cu_1^3$, and since c is cubefree $m \mid u_1$ as claimed.

(2). Set $\alpha = (u_0 + u_1\theta + u + 2\theta^2)/m$. Since by assumption $\alpha \in \mathbb{Z}_K$, by definition of f we have $f\alpha \in \mathbb{Z}[\theta]$, in other words $m \mid fu_i$ for all i, so that $m \mid f \gcd(u_0, u_1, u_2)$. □

Remark. Using the precise description of an integral basis of $\mathbb{Z}_K$, one can show that if $c \neq \pm 1$ is cubefree, then $m \mid (u_0+u_1\theta+u_2\theta^2)\mathbb{Z}_K$ if and only if $m \mid \gcd(u_0, u_1, c_2u_2)$ when $c \not\equiv \pm 1 \pmod 9$, or $m \mid \gcd(u_0 - c_2^2u_2, u_1 - cu_2, 3c_2u_2)$ when $c \equiv \pm 1 \pmod 9$, where $c = c_1c_2^2$ with c_1, c_2 squarefree and coprime (with $f = c_2$ or $f = 3c_2$, respectively), see Exercises 17 and 18.

Lemma 6.4.7. *Let K be a number field, and let $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}_1$, and $\mathfrak{c}_2$ be integral ideals of K. Assume the following.*

(1) *We have an ideal equality $\mathfrak{c}_1\mathfrak{c}_2 = \mathfrak{b}\mathfrak{a}^3$.*
(2) *We have $\gcd(\mathfrak{c}_1, \mathfrak{c}_2, \mathfrak{a}) = 1$.*

Then there exist integral ideals $\mathfrak{a}_i$ and $\mathfrak{b}_i$ such that $\mathfrak{c}_i = \mathfrak{b}_i\mathfrak{a}_i^3$ for $i = 1, 2$, $\mathfrak{b}_1\mathfrak{b}_2 = \mathfrak{b}$, $\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{a}$, $\gcd(\mathfrak{a}_1, \mathfrak{a}_2) = 1$, and $\gcd(\mathfrak{c}_1, \mathfrak{c}_2) = \gcd(\mathfrak{b}_1, \mathfrak{b}_2)$.

Proof. If we set $\mathfrak{d} = \gcd(\mathfrak{c}_1, \mathfrak{c}_2)$ then by assumption $\mathfrak{d}$ and $\mathfrak{a}$ are coprime hence $\mathfrak{d}^2 \mid \mathfrak{b}$, so that

$$(\mathfrak{c}_1\mathfrak{d}^{-1})(\mathfrak{c}_2\mathfrak{d}^{-1}) = (\mathfrak{b}\mathfrak{d}^{-2})\mathfrak{a}^3 .$$

Since by definition of $\mathfrak{d}$ the two factors on the left are coprime, for any ideal I we have

$$\gcd((\mathfrak{c}_1\mathfrak{d}^{-1})(\mathfrak{c}_2\mathfrak{d}^{-1}), I) = \gcd(\mathfrak{c}_1\mathfrak{d}^{-1}, I)\gcd(\mathfrak{c}_2\mathfrak{d}^{-1}, I) ,$$

hence if we set $\mathfrak{d}_i = \gcd(\mathfrak{c}_i\mathfrak{d}^{-1}, \mathfrak{b}\mathfrak{d}^{-2})$ and $\mathfrak{e}_i = \mathfrak{c}_i\mathfrak{d}^{-1}\mathfrak{d}_i^{-1}$ we have $\mathfrak{d}_1\mathfrak{d}_2 = \mathfrak{b}\mathfrak{d}^{-2}$ hence $\mathfrak{e}_1\mathfrak{e}_2 = \mathfrak{a}^3$. Now since $\mathfrak{c}_1\mathfrak{d}^{-1}$ and $\mathfrak{c}_2\mathfrak{d}^{-1}$ are coprime, a fortiori so are $\mathfrak{e}_1$ and $\mathfrak{e}_2$, hence there exist coprime integral ideals $\mathfrak{a}_i$ such that $\mathfrak{e}_i = \mathfrak{a}_i^3$ and $\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{a}$. Thus if we set $\mathfrak{b}_i = \mathfrak{d}\mathfrak{d}_i$ we have $\mathfrak{c}_i = \mathfrak{b}_i\mathfrak{a}_i^3$ and $\mathfrak{b}_1\mathfrak{b}_2 = \mathfrak{d}^2\mathfrak{d}_1\mathfrak{d}_2 = \mathfrak{b}$. By construction we have $\mathfrak{d} = \gcd(\mathfrak{c}_1, \mathfrak{c}_2) \mid \gcd(\mathfrak{b}_1, \mathfrak{b}_2)$, and conversely it is clear that $\gcd(\mathfrak{b}_1, \mathfrak{b}_2) \mid \gcd(\mathfrak{c}_1, \mathfrak{c}_2)$, proving the lemma. □

Recall that an integral ideal $\mathfrak{a}$ is said to be *primitive* if $m = 1$ is the only $m \in \mathbb{Z}_{>0}$ such that $\mathfrak{a}/m$ is an integral ideal. For simplicity we introduce the following temporary definition.

Definition 6.4.8. *Let θ be an algebraic integer, $K = \mathbb{Q}(\theta)$, and $f = [\mathbb{Z}_K : \mathbb{Z}[\theta]]$. We say that an integral ideal $\mathfrak{b}$ of K dividing $b\mathbb{Z}_K$ is a* suitable *divisor of b (relative to θ) if it satisfies the following three conditions.*

(1) *$\mathfrak{b}$ is primitive and $b/\mathcal{N}(\mathfrak{b})$ is the cube of a rational number.*
(2) *If $m \in \mathbb{Z}$ divides $b\mathbb{Z}_K/\mathfrak{b}$ then $m \mid \gcd(b, f)$.*
(3) *Every prime ideal dividing $\mathfrak{b}$ and not dividing $f\mathbb{Z}_K$ has degree 1.*

For instance if b and f are coprime then this means that $\mathfrak{b}$ and $b\mathbb{Z}_K/\mathfrak{b}$ are primitive, that $b/\mathcal{N}(\mathfrak{b})$ is the cube of a rational number, and that all prime ideals dividing $\mathfrak{b}$ have degree 1. The following lemma is the key to the theorems that we are going to prove.

Lemma 6.4.9. *Let c be an integer not equal to a perfect cube and such that $c \not\equiv \pm 1 \pmod 9$, set $\theta = c^{1/3}$ and let $K = \mathbb{Q}(\theta)$. Let b be a nonzero integer, let x, y, and z be pairwise coprime integers such that $x^3 + by^3 + cz^3 = 0$, and set $L = x + z\theta$ and $Q = x^2 - xz\theta + z^2\theta^2$.*

(1) *There exist integral ideals $\mathfrak{a}_i$ and $\mathfrak{b}_i$ of K such that $L\mathbb{Z}_K = \mathfrak{b}_1\mathfrak{a}_1^3$, $Q\mathbb{Z}_K = \mathfrak{b}_2\mathfrak{a}_2^3$, $\mathfrak{b}_1\mathfrak{b}_2 = b\mathbb{Z}_K$, $\mathfrak{a}_1\mathfrak{a}_2 = y\mathbb{Z}_K$, and the $\mathfrak{a}_i$ are coprime to $3\mathbb{Z}_K$.*
(2) *If c is cubefree the ideal $\mathfrak{b}_1$ is a suitable divisor of b.*
(3) *If $b = p^k$ with p a prime different from 3 and $k = 1$ or 2, then either $\mathfrak{b}_1$ and $\mathfrak{b}_2$ are coprime, or $p\mathbb{Z}_K = \mathfrak{p}^3$ is totally ramified and $\gcd(\mathfrak{b}_1, \mathfrak{b}_2) = \mathfrak{p}^j$ for some $j \geqslant 1$.*

Proof. (1). We note first that $3 \nmid y$: indeed if $3 \mid y$ then $3 \nmid xz$ by coprimality, so $c \equiv (-x/z)^3 \equiv \pm 1 \pmod 9$, contrary to our assumption. Now with the notation of the lemma, in the field K our equation can be written $LQ = -by^3$. Let $\mathfrak{p}$, if it exists, be a prime ideal of K dividing both L and Q. Then $\mathfrak{p}$ divides $3x^2 = Q + 3xL - L^2$, hence either $\mathfrak{p} \mid 3\mathbb{Z}_K$ or $\mathfrak{p} \mid x$, and since y is coprime to x and is not divisible by 3 it follows that $\mathfrak{p} \nmid y\mathbb{Z}_K$, so $\gcd(L\mathbb{Z}_K, Q\mathbb{Z}_K)$ is coprime to $y\mathbb{Z}_K$. By Lemma 6.4.7 it follows that there exist integral ideals $\mathfrak{a}_i$ and $\mathfrak{b}_i$ such that $L\mathbb{Z}_K = \mathfrak{b}_1\mathfrak{a}_1^3$, $Q\mathbb{Z}_K = \mathfrak{b}_2\mathfrak{a}_2^3$, $\mathfrak{b}_1\mathfrak{b}_2 = b\mathbb{Z}_K$, and $\mathfrak{a}_1\mathfrak{a}_2 = y\mathbb{Z}_K$, proving (1).

(2). If $m \in \mathbb{Z}_{>0}$ divides $\mathfrak{b}_1$ then $m \mid (x + z\theta)\mathbb{Z}_K$, hence by Lemma 6.4.6 $m \mid \gcd(x, z) = 1$, so $\mathfrak{b}_1$ is primitive. By the same lemma if $m \in \mathbb{Z}_{>0}$ divides $b\mathbb{Z}_K/\mathfrak{b}_1 = \mathfrak{b}_2$ then $m \mid (x^2 - xz\theta + z^2\theta^2)\mathbb{Z}_K$, hence $m \mid f \gcd(x^2, xz, z^2) = f$ since $\gcd(x, z) = 1$, and since $\mathfrak{b}_2 \mid b\mathbb{Z}_K$ we also have $m \mid b$ so $m \mid \gcd(b, f)$. Since $L\mathbb{Z}_K = \mathfrak{b}_1\mathfrak{a}_1^3$ and $\mathcal{N}(L) = x^3 + cz^3 = -by^3$ it follows that $\mathcal{N}(\mathfrak{b}_1)\mathcal{N}(\mathfrak{a}_1)^3 = |by^3|$ so that $b/\mathcal{N}(\mathfrak{b}_1) = (\pm\mathcal{N}(\mathfrak{a}_1)/y)^3$ is the cube of a rational number. Finally, let $\mathfrak{p}$ be a prime ideal divisor of $\mathfrak{b}_1$ and p the prime number below $\mathfrak{p}$. Since by assumption $\mathfrak{p} \nmid f\mathbb{Z}_K$ we have $p \nmid f$, and since x and z are coprime, by Lemma 3.3.20 we deduce that $\mathfrak{p}$ has degree 1, proving that $\mathfrak{b}_1$ is a suitable ideal divisor of b.

(3). Let again $\mathfrak{p}$ be a prime ideal dividing L and Q, if it exists. As we have seen we have $\mathfrak{p} \mid 3x^2$, and also $\mathfrak{p} \mid 3z^2\theta^2 = Q - 3xL + 2L^2$. Since by Lemma 6.4.7 we have $\mathfrak{p} \mid \gcd(\mathfrak{b}_1, \mathfrak{b}_2)$, it follows that $\mathfrak{p}^2 \mid b\mathbb{Z}_K$. In particular, since b is coprime to 3, $\mathfrak{p} \nmid 3\mathbb{Z}_K$, hence $\mathfrak{p} \mid x$ and $\mathfrak{p} \mid z\theta$, and since x and z are coprime it follows that $\mathfrak{p} \mid x$ and $\mathfrak{p} \mid \theta$, so $\mathfrak{p} \mid L\mathbb{Z}_K$, $\mathfrak{p}^2 \mid Q\mathbb{Z}_K$, hence $\mathfrak{p}^3 \mid b\mathbb{Z}_K = p^k\mathbb{Z}_K$. Since $1 \leqslant k \leqslant 2$ this implies that $\mathfrak{p}^2 \mid p\mathbb{Z}_K$, so that $\mathfrak{p}$ is a ramified prime ideal above p, necessarily unique, proving that $\gcd(\mathfrak{b}_1, \mathfrak{b}_2) = \mathfrak{p}^j$ for some $j \geqslant 0$. If $j \geqslant 1$, then $p \mid x$ and $p \nmid yz$, hence $v_p(by^3) = v_p(b) = k < 3 \leqslant v_p(x^3)$ so that

$$v_p(c) = v_p(cz^3) = v_p(x^3 + by^3) = v_p(b) = k \ ,$$

hence $v_{\mathfrak{p}}(c\mathbb{Z}_K) = ke(\mathfrak{p}/p)$. On the other hand since $c = \theta^3$ we have $v_{\mathfrak{p}}(c\mathbb{Z}_K) = 3v_{\mathfrak{p}}(\theta\mathbb{Z}_K) \equiv 0 \pmod 3$, hence $3 \mid ke(\mathfrak{p}/p)$, and since k is coprime to 3 it follows that $3 \mid e(\mathfrak{p}/p)$ so that p is totally ramified, as claimed. □

Thanks to the above lemma we can easily give some sufficient conditions for the insolubility of the equation $x^3 + by^3 + cz^3 = 0$. We give two results, corresponding to the cases where the exponent of the class group of $K = \mathbb{Q}(c^{1/3})$ is divisible by 3 or equal to 1 or 2.

Theorem 6.4.10. *Let b and c be cubefree integers not equal to ± 1, set $\theta = c^{1/3}$, and let $K = \mathbb{Q}(\theta)$. Assume that the following conditions are satisfied.*

(1) $c \not\equiv \pm 1 \pmod 9$.
(2) *The class number h of K is divisible by 3.*
(3) *If $\mathfrak{b}$ is a suitable divisor of b then $\mathfrak{b}^{e/3}$ is not a principal ideal, where $e \mid h(K)$ is the exponent of the class group of K.*

Then the equation $x^3 + by^3 + cz^3 = 0$ has no nontrivial rational solutions.

Proof. By Lemma 6.4.3 it is sufficient to prove that the equation has no solution with x, y, z in $\mathbb{Z}$ pairwise coprime. By Lemma 6.4.9 (1) and (2) there exist integral ideals $\mathfrak{a}_i$ and $\mathfrak{b}_i$ of K such that $L\mathbb{Z}_K = \mathfrak{b}_1\mathfrak{a}_1^3$, $Q\mathbb{Z}_K = \mathfrak{b}_2\mathfrak{a}_2^3$, $\mathfrak{b}_1\mathfrak{b}_2 = b\mathbb{Z}_K$, $\mathfrak{a}_1\mathfrak{a}_2 = y\mathbb{Z}_K$, and since c is cubefree $\mathfrak{b}_1$ is a suitable divisor of b. Since $L^{e/3}\mathbb{Z}_K = \mathfrak{b}_1^{e/3}\mathfrak{a}_1^e$ and by definition of the exponent the ideal $\mathfrak{a}_1^e$ is principal, it follows that $\mathfrak{b}_1^{e/3}$ is also principal, in contradiction with the assumption. □

An important variant of the above theorem is the following.

Proposition 6.4.11. *The conclusion of the theorem is valid if we replace condition (3) by the assumptions that $b = p^k$ with p a prime not dividing the index $f = [\mathbb{Z}_K : \mathbb{Z}[\theta]]$, $k = 1$ or 2 is coprime to e, and for each prime ideal $\mathfrak{p}$ of degree 1 above p then $\mathfrak{p}^{e/3}$ is not principal.*

Proof. If $b = p$, it is easily checked by inspecting the 5 splitting possibilities for p that for any suitable divisor $\mathfrak{b}$ of b then either $\mathfrak{b}$ or $b\mathbb{Z}_K/\mathfrak{b}$ is a prime ideal $\mathfrak{p}$ above p of degree 1, hence $\mathfrak{p}^{e/3}$ is not principal, so in both cases $\mathfrak{b}^{e/3}$ is not principal so assumption (3) of the theorem is satisfied. Thus assume that $b = p^2$, so that the class number of K is odd. As before we have $p^2\mathbb{Z}_K = \mathfrak{b}_1\mathfrak{b}_2$ where $\mathfrak{b}_1$ is a suitable divisor of p^2 such that the $\mathfrak{b}_i^{e/3}$ are principal ideals. We consider three cases.

Case 1: $p \neq 3$ **and** $\gcd(\mathfrak{b}_1, \mathfrak{b}_2) = \mathbb{Z}_K$. It is easily seen by inspection that we always have $\mathfrak{b}_1 = \mathfrak{q}^2$ or $\mathfrak{b}_2 = \mathfrak{q}^2$ for some prime ideal $\mathfrak{q}$ above p of degree one. Since the class number of K is odd it follows that $\mathfrak{q}^{e/3}$ is a principal ideal of degree one, contrary to our assumption.

Case 2: $p \neq 3$ **and** $\gcd(\mathfrak{b}_1, \mathfrak{b}_2) \neq \mathbb{Z}_K$. By Lemma 6.4.9 (3) we know that $\gcd(\mathfrak{b}_1, \mathfrak{b}_2) = \mathfrak{p}^j$ for $j \geqslant 1$, where $\mathfrak{p}$ is a totally ramified prime ideal above p. But then it is clear that there are no decompositions $\mathfrak{p}^6 = \mathfrak{b}_1\mathfrak{b}_2$ with $\mathfrak{b}_1$ and $\mathfrak{b}_2$ primitive, hence this case cannot occur since $\mathfrak{b}_1$ is a suitable divisor of p^2.

Case 3: $b = 9$. Recall that the prime 3 is always ramified in the pure cubic field K. If $3\mathbb{Z}_K = \mathfrak{p}^3$ is totally ramified, as in case 2 there do not exist suitable

divisors of b. Thus assume that $3\mathbb{Z}_K = \mathfrak{p}_1^2\mathfrak{p}_2$ with $\mathfrak{p}_2 \neq \mathfrak{p}_1$. Our equation implies that $x^3 + cz^3 \equiv 0 \pmod 9$, so that $3 \nmid z$ (otherwise $3 \mid x$ and x and z would not be coprime) hence $c \equiv (-x/z)^3 \pmod 9$, so $c \equiv 0 \pmod 9$ since by assumption $c \not\equiv \pm 1 \pmod 9$. Since c is cubefree, this means that $v_3(c) = 2$. But as above this is absurd since this implies that $v_{\mathfrak{p}_1}(c) = 2v_3(c) = 4$, while $v_{\mathfrak{p}_1}(c) = 3v_{\mathfrak{p}_1}(\theta) \equiv 0 \pmod 3$, proving the proposition (another way of saying this is that if $v_3(c) = 1$ or 2 then 3 is totally ramified in $K = \mathbb{Q}(c^{1/3})$). □

Remark. Among the 84 fields $Q(c^{1/3})$ with c cubefree such that $2 \leqslant c \leqslant 100$, 50 have class number divisible by 3.

A result when $h = 1$ or 2, or more generally when the exponent of the class group is equal to 1 or 2 is the following.

Theorem 6.4.12. *Let b and c be cubefree integers, set $\theta = c^{1/3}$, and let $K = \mathbb{Q}(\theta)$. Assume that the following conditions are satisfied.*

(1) $c \not\equiv \pm 1 \pmod 9$ *and* $c \not\equiv 0 \pmod 9$.
(2) *The exponent e of the class group of K is equal to 1 or 2.*
(3) *If ε is a fundamental unit of K then $\varepsilon \equiv \pm 1 \pmod{3\mathbb{Z}_K}$.*
(4) *For every suitable divisor $\mathfrak{b}$ of b there exists a generator α of $\mathfrak{b}^e$ of the form $\alpha = x_0 + x_1\theta + x_2\theta^2$ with $x_i \in \mathbb{Q}$ and $v_3(x_2) = 0$ when $e = 1$, or $v_3(x_1^2 - 4x_0x_2) = 0$ when $e = 2$.*

Then the equation $x^3 + by^3 + cz^3 = 0$ has no nontrivial rational solutions.

Proof. As before by Lemma 6.4.3 we may assume that x, y, z are pairwise coprime integers. Writing our equation $LQ = -by^3$ as above, by Lemma 6.4.9 we know that there exist integral ideals $\mathfrak{a}_i$ and $\mathfrak{b}_i$ of K such that $L\mathbb{Z}_K = \mathfrak{b}_1\mathfrak{a}_1^3$, $Q\mathbb{Z}_K = \mathfrak{b}_2\mathfrak{a}_2^3$, $\mathfrak{b}_1\mathfrak{b}_2 = b\mathbb{Z}_K$, $\mathfrak{a}_1\mathfrak{a}_2 = y\mathbb{Z}_K$, where $\mathfrak{b}_1$ is a suitable divisor of b and the $\mathfrak{a}_i$ are coprime to $3\mathbb{Z}_K$. By assumption we have $\mathfrak{b}_1^e = \alpha\mathbb{Z}_K$ with $\alpha = x_0 + x_1\theta + x_2\theta^2$, where $x_i \in \mathbb{Q}$, so we can write

$$(x + z\theta)^e\mathbb{Z}_K = (x_0 + x_1\theta + x_2\theta^2)(u + v\theta + w\theta^2)^3\mathbb{Z}_K\,,$$

where $u + v\theta + w\theta^2$ is a generator of $\mathfrak{a}_1^e$. Thus, if ε is a fundamental unit of K there exists $m \in \mathbb{Z}$ and a sign $\pm$ such that

$$(x + z\theta)^e = \pm\varepsilon^m(x_0 + x_1\theta + x_2\theta^2)(u + v\theta + w\theta^2)^3\,.$$

Now it follows from the Dedekind criterion (see Theorem 6.1.4 of [Coh0]) that condition (1) on c is equivalent to $3 \nmid f = [\mathbb{Z}_K : \mathbb{Z}[\theta]]$. Multiplying both sides of the equation by f^{m+4} gives

$$f^{m+4-e}(fx + fz\theta)^e = \pm(f\varepsilon)^m(fx_0 + fx_1\theta + fx_2\theta^2)(fu + fv\theta + fw\theta^2)^3\,,$$

where all the coefficients are now in $\mathbb{Z}$. Note that

$$\begin{aligned}\pm\mathcal{N}(f\mathfrak{a}_1^e) &= \mathcal{N}(fu+fv\theta+fw\theta^2)\\ &= (fu)^3+(fv)^3c+(fw)^3c^2-3(fu)(fv)(fw)c\\ &\equiv (fu+fv\theta+fw\theta^2)^3 \pmod 3\ ,\end{aligned}$$

and since by assumption $f\varepsilon \equiv \pm 1 \pmod{3\mathbb{Z}[\theta]}$ it follows that

$$f^{m+4-e}(fx+fz\theta)^e \equiv \pm f^3\,\mathcal{N}(\mathfrak{a}_1)^e(fx_0+fx_1\theta+fx_2\theta^2) \pmod{3\mathbb{Z}[\theta]}\ .$$

If $e=1$ we identify the coefficients of θ^2 and deduce that $0 \equiv \pm f^4 x_2\,\mathcal{N}(\mathfrak{a}_1) \pmod 3$, and since $3 \nmid f$ and by assumption $3 \nmid x_2$, it follows that $3 \mid \mathcal{N}(\mathfrak{a}_1)$ which is absurd since $\mathfrak{a}_1$ is coprime to $3\mathbb{Z}_K$. If $e=2$ we note that the left hand side has the form $y_0+y_1\theta+y_2\theta^2$ with $y_1^2-4y_0y_2=0$, so identifying this expression on both sides (which we can do since 1, θ, θ^2 are $\mathbb{Q}$-linearly independent) we obtain $0 \equiv f^8\,\mathcal{N}(\mathfrak{a}_1)^4(x_1^2-4x_0x_2) \pmod 3$, and since $3 \nmid f$ and $3 \nmid (x_1^2-4x_0x_2)$, it follows that $3 \mid \mathcal{N}(\mathfrak{a}_1)$, again a contradiction and proving the theorem. □

Remarks.

(1) Among the 58 cubefree values of c such that $2 \leqslant c \leqslant 100$ and $c \not\equiv \pm 1 \pmod 9$ and $c \not\equiv 0 \pmod 9$, 19 are such that K has exponent of the class group equal to 1 or 2, and among those, 7 satisfy $\varepsilon \equiv \pm 1 \pmod{3\mathbb{Z}_K}$.

(2) Because of the condition on the fundamental unit, if there exists a generator α as in (4), then *all* generators satisfy the 3-adic condition.

Corollary 6.4.13. *The equations $x^3+by^3+cz^3=0$ have a nontrivial solution in every completion of $\mathbb{Q}$ but no nontrivial solutions in $\mathbb{Q}$ for $(b,c) = (3,20)$, $(3,22)$, $(4,15)$, $(5,12)$, $(6,10)$, $(6,11)$, $(6,17)$, $(10,15)$, $(10,22)$, $(11,15)$, $(11,20)$, $(12,17)$, $(15,17)$, $(15,20)$, $(15,22)$, $(17,20)$, and $(17,22)$.*

Proof. Recall that we have at our disposal a CAS which can say immediately whether the conditions of the theorems are satisfied or not. Thus a small computer program shows that the above equations are the only ones satisfying the hypotheses of the corollary with $b \leqslant c \leqslant 22$. □

We will come back to the equation $x^3+15y^3+22z^3=0$ at the end of Section 7.2.4. The reason we stopped the (easily obtained) examples at the strange limit 22 is to have this example available. Many more examples are given in the table given below.

Corollary 6.4.14 (Selmer). *The equation $3x^3+4y^3+5z^3=0$ has a nontrivial solution in every completion of $\mathbb{Q}$ but no nontrivial solutions in $\mathbb{Q}$.*

Proof. Multiplying the equation by 2 and setting $(X,Y,Z)=(2y,x,z)$, it is clear that its solubility in any field of characteristic 0 is equivalent to that of the equation $X^3+6Y^3+10Z^3=0$, and it is easy to check that the

conditions of Theorem 6.4.12 are satisfied for $c = 6$ and $b = 10$ (the pair $(6, 10)$ is among those given above). □

This equation has historical value since it was the first example of an equation of that type violating the Hasse principle.

In all of the above results we have assumed that b is coprime to $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$. When this condition is not satisfied, we can often still obtain a result, see Exercise 17.

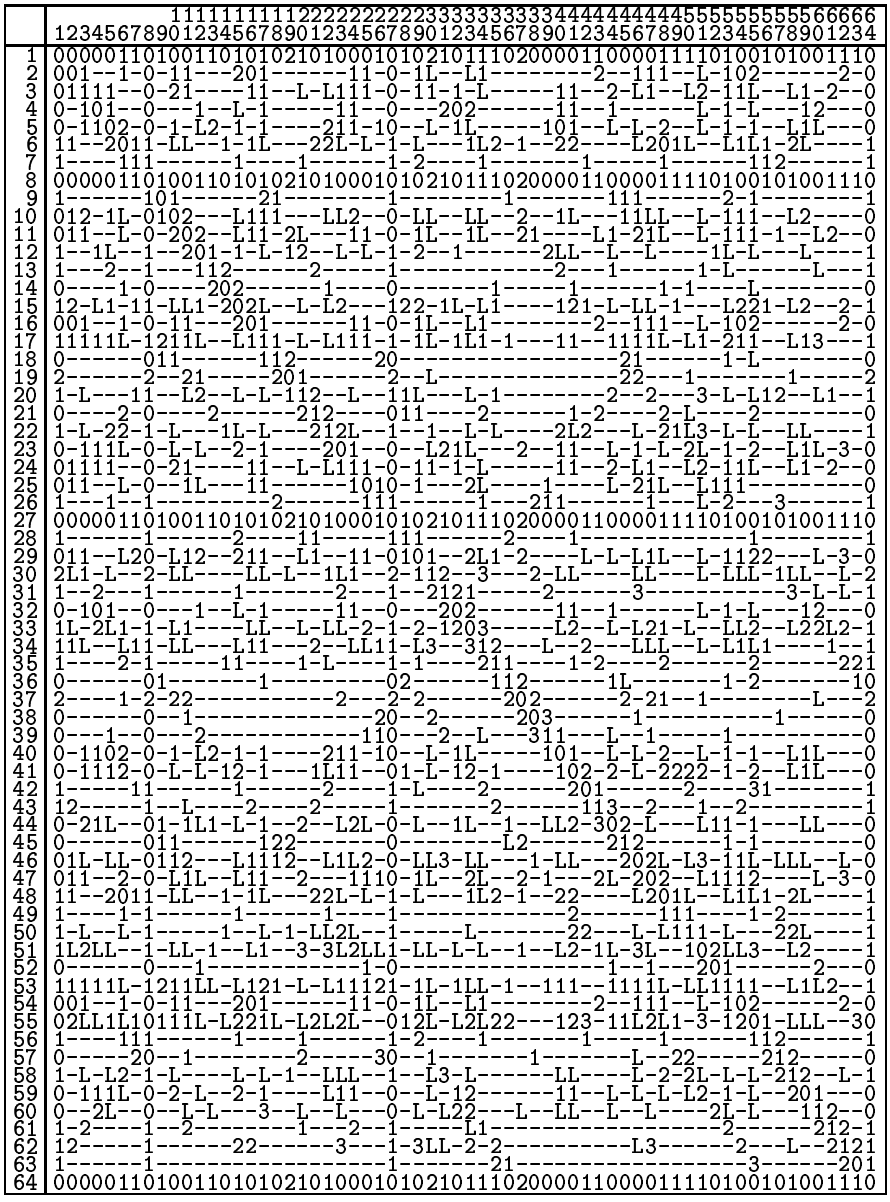
There are a number of other sufficient conditions based on algebraic number theory which imply the nonglobal solubility of our equations, in particular conditions based on cubic reciprocity, see for instance the first paper by Selmer [Sel1] on the subject. However the above conditions suffice in small cases. For instance, they allow a complete answer for $\max(|b|, |c|) \leqslant 65$, and leave only (at most) 12 indeterminate cases (out of 5050) for $\max(|b|, |c|) \leqslant 100$, which can all be treated using the general method explained in Section 8.4.5. For the convenience of the reader, in the following table we give in a very compact form detailed information on the solubility of the equation $x^3 + by^3 + cz^3 = 0$ for $1 \leqslant b, c \leqslant 64$. The entry in line b and column c of the table means the following: `-` means locally insoluble and `L` means everywhere locally soluble but not globally soluble (hence a failure of the Hasse principle). In every other case, the equation is globally soluble, hence the curve $x^3 + by^3 + cz^3 = 0$ is the projective equation of an elliptic curve, and the entry (`0`, `1`, `2`, or `3` in the limits of the table) gives the *rank* of the curve (see Chapters 7 and 8 for all these notions). In particular if the entry is equal to `0` this means that the equation has only a finite nonzero number of (projective) solutions which can all easily be found. By Corollary 8.1.15 this implies that either b, c, or b/c is a cube. The same corollary also gives the torsion subgroup.

This table has been computed as follows. Note first that without loss of generality it is enough to compute the entries where b and c are cubefree. Using Proposition 6.4.2, we determine whether the equation is everywhere locally soluble. We then make a naïve search for solutions up to a small bound (we chose x, $|y|$ up to 1000). If no solution is found, we apply Theorem 6.4.10, Proposition 6.4.11, and Theorem 6.4.12. This leaves 54 cases which are undetermined, up to exchange of b and c. Using the simple remark that the solubility of $x^3 + by^3 + cz^3 = 0$ is equivalent to that of $X^3 + BY^3 + cBz^3$, where B is such that bB is a cube, we remove 27 indeterminate cases, leaving 27. Note that here it is essential to use the *exponent* of the class group in the theorems, and not the class number itself. If we had used only the class number we would have removed only 1 indeterminate case, but the 26 missed ones would have been removed in the next stage.

In a second stage, using descent methods or Cremona's `mwrank` program (see Chapter 8), we compute the rank of the Jacobian of our curve (see Proposition 7.2.4, the warning following it, and Section 13.2). Thanks to

Corollary 8.1.15, when this rank is equal to 0 (and neither b, c, nor b/c is a cube, but this never happens at this stage), we conclude that the equation has no global solutions. This leaves only 10 undetermined cases for which the Jacobian has rank greater or equal to 1. Pushing further the search for solutions, using also 3-adic and 7-adic information, we find global solutions for all of these cases (the most difficult being $149105^3 + 17 \cdot (-140161)^3 + 41 \cdot 101988^3 = 0$ for $(b, c) = (17, 41)$ and $147267^3 + 41 \cdot (-6040)^3 + 59 \cdot (-37793)^3 = 0$ for $(b, c) = (41, 59)$).

The visual rows, columns and diagonals that can easily be seen in the table reflect the existence of simple global solutions. For instance on the diagonal $c = 64 - b$ we see that the equation is always globally soluble, and this is clear since there exist the solution $(x, y, z) = (-4, 1, 1)$.



Solubility in $\mathbb{Q}$ of $x^3 + by^3 + cz^3 = 0$ up to $\max(b, c) = 64$

6.4.5 Sums of Two or More Cubes

The problem of representing integers or rational numbers by sums of *squares* is completely understood thanks to the Hasse–Minkowski theorem and Proposition 5.4.4 (see Section 5.4.4). On the other hand the problem for cubes is

much more difficult and far from being understood. First as we have seen above in several analogous situations (Section 6.4.4) the local to global principle fails. The analogue of Proposition 5.4.4 also fails: representations as sums of cubes of rational numbers and as sums of cubes of integers are two quite different problems. For instance we will see below that every integer is the sum of three cubes of rational numbers, while it is trivial to see that the integer 4 cannot be equal to the sum of three cubes of integers. Hence in this subsection we give an assortment of results and conjectures on those subjects, including the proof of a beautiful result of Dem'janenko.

Finally note that the natural setting for the problems which we consider is $\mathbb{Q}$ or $\mathbb{Z}$, and *not* the positive rationals or the positive integers, so we do not consider the problem of representations as sums of *positive* cubes. Thus when we speak of an *integer*, we always mean an element of $\mathbb{Z}$, not necessarily of $\mathbb{Z}_{\geqslant 0}$. In addition, since the exponent 3 is odd, contrary to the quadratic case we do not need to look at signs. Note however the following result.

Proposition 6.4.15. *An integer $n \geqslant 1$ is a sum of two rational cubes if and only if it is a sum of two* nonnegative *rational cubes.*

Proof. We may evidently assume that n is not a cube, so let $n = x_0^3 + y_0^3$ be a decomposition of n as a sum of two cubes. If x_0 and y_0 are nonnegative there is nothing to prove, so we may assume without loss of generality that $y_0 > 0$ and $x_0 < 0$. It is easily checked that if $x_k^3 + y_k^3 = n$ then $x_{k+1}^3 + y_{k+1}^3 = n$ with

$$x_{k+1} = \frac{y_k^4 + 2x_k^3 y_k}{y_k^3 - x_k^3} \quad \text{and} \quad y_{k+1} = -\frac{x_k^4 + 2x_k y_k^3}{y_k^3 - x_k^3} .$$

The existence of such an identity comes from Fermat's tangent method and will be explained in detail in Chapter 7 (see also Exercise 9 of Chapter 7), but the direct verification is immediate. We thus define a sequence of points on the curve $x^3 + y^3 = n$. I claim that there exists $k \in \mathbb{Z}_{\geqslant 0}$ such that $x_k > 0$ and $y_k > 0$. Indeed, if we set $u_k = y_k/x_k$ this is equivalent to $u_k > 0$ (since $n > 0$), and u_k satisfies the recursion $u_{k+1} = f(u_k)$ with

$$f(x) = -\frac{2x^3 + 1}{x(x^3 + 2)} .$$

Furthermore, since $y_0 > 0$, $x_0 < 0$ and $x_0^3 + y_0^3 = n$ we have $u_0^3 + 1 < 0$, hence $u_0 < -1$. Now we have

$$f(x) - 8x - 7 = -\frac{(x+1)^2(8x^3 - 9x^2 + 12x + 1)}{x(x^3 + 2)} ,$$

and since for $x < -1$ we have $8x^3 - 9x^2 + 12x + 1 < -28$ it follows in particular that for $-\sqrt[3]{2} < x < -1$ we have $f(x) - 8x - 7 < 0$. Thus if $-\sqrt[3]{2} < u_k < -1$ we have $u_{k+1} + 1 < 8(u_k + 1)$. Since $u_0 + 1 < 0$ it follows that there exists $k \geqslant 0$ such that $u_k < -\sqrt[3]{2}$. But then clearly $u_{k+1} = f(u_k) > 0$, as was to be proved. □

Proposition 6.4.16. *There are infinitely many integers which are not the sum of two cubes of rational numbers.*

Proof. Indeed, Theorem 6.4.5 tells us for instance that odd primes congruent to 2 or 5 modulo 9 cannot be the sum of two cubes of rational numbers, and by Dirichlet's theorem on primes in arithmetic progression (Theorem 10.5.29) there are infinitely many such primes. □

It is reasonable to ask if, in a manner analogous to Proposition 5.4.9, we can characterize the integers which are sums of two cubes, either of integers, or of rational numbers. The answer for integers is trivial. For rational numbers there is a conjecture, and a theorem for representation of prime numbers as sums of two cubes of rational numbers which is a combination of work of N. Elkies with a theorem of F. Rodriguez-Villegas and D. Zagier [Rod-Zag].

Proposition 6.4.17. *An integer n is a sum of two cubes of (positive or negative) integers if and only if there exists a positive divisor d of n such that $(4n/d - d^2)/3$ is the square of an integer. For example a (positive) prime p is a sum of two cubes of integers if and only if $p = 2$ or p has the form $p = 3x^2 - 3x + 1$ for $x \geqslant 2$.*

Proof. Left to the reader (Exercise 20). □

The conjecture for sums of two cubes of rational numbers is the following.

Conjecture 6.4.18. (1) *Any squarefree integer congruent to 4, 6, 7, or 8 modulo 9 is a sum of two rational cubes.*

(2) *Denote by $S(X)$ the set of squarefree integers less than or equal to X which are congruent to 1, 2, 3, or 5 modulo 9 and which are the sum of two rational cubes. Then $S(X)$ has density 0, more precisely there exists a strictly positive constant c such that*

$$S(X) \sim cX^{5/6}\log(X)^{\sqrt{3}/2-1/8}\ .$$

The first conjecture immediately follows from the BSD conjecture, hence is almost certainly correct. The second conjecture has been obtained using methods coming from random matrix theory, and is more speculative although supported by numerical evidence [Kea-Sna]. Note that it is possible to state a conjecture for *cubefree* integers, which is a more natural condition, but the statement is more complicated.

To state the theorems of Elkies and Rodriguez-Villegas–Zagier we first need to define a sequence of polynomials.

Definition 6.4.19. *We define the Villegas–Zagier polynomials $V_n(t)$ by the initial conditions $V_{-1}(t) = 0$, $V_0(t) = 1$ and the recursion*

$$V_{n+1}(t) = (8t^3 - 1)V_n'(t) - (16n + 3)t^2V_n(t) - 4n(2n - 1)tV_{n-1}(t)$$

for $n \geqslant 1$.

Theorem 6.4.20. *Assume the Birch and Swinnerton-Dyer conjecture (Conjecture 8.1.7), and let p be a prime number. Then p is the sum of two cubes of rational numbers if and only if one of the following conditions is satisfied.*

(1) $p = 2$
(2) $p \equiv 4$, 7, *or* 8 *modulo* 9.
(3) $p \equiv 1 \pmod 9$ *and* $p \mid V_{(p-1)/3}(0)$.

The proof of this theorem uses the classical theory of modular forms, complex multiplication, and central values of L-series. For example, it implies that the only $p \leqslant 100$ such that $p \equiv 1 \pmod 9$ and which are sums of two cubes of rational numbers are $p = 19$ and $p = 37$.

Note that in Theorem 6.4.5 we have proved by descent arguments that if $p = 3$ or $p \geqslant 5$ and $p \equiv 2$ or 5 modulo 9 then p is not a sum of two cubes. When $p \equiv 4$ or 7 modulo 9, N. Elkies has shown that p is a sum of two cubes of rational numbers without assuming BSD. The result for $p \equiv 1 \pmod 9$ is also independent of the correctness of BSD. The only case where the BSD conjecture is needed is for $p \equiv 8 \pmod 9$.

It is possible that this theorem can be extended to a complete characterization of all integers which are sums of two cubes of rational numbers. Note, however, that if we are willing to reason in a heuristic manner and in particular to believe the BSD conjecture, it is easy to determine whether or not a *given* integer (or rational number) c is a sum of two cubes. Without loss of generality assume that c is a cubefree integer and that $c > 2$. It follows from Proposition 7.2.3 and the remarks following it, combined with Corollary 8.1.15 and BSD, that c is a sum of two cubes if and only if the elliptic curve E_c with affine equation $y^2 = x^3 + 16c^2$ has rank at least equal to 1. To check this, we first compute the root number (in the case of squarefree c it will be equal to -1 for $c \equiv 4$, 6, 7, or 8 modulo 9, and to 1 otherwise, explaining Conjecture 6.4.18 (1)). If it is equal to -1, then by BSD c is a sum of two cubes (and BSD is not necessary if the rank is equal to 1, which can be checked by computing $L'(E_c, 1)$ using Corollary 8.5.10). If the root number is equal to 1, we compute $L(E_c, 1)$ using Corollary 8.5.7, which gives a rapidly convergent series for $L(E_c, 1)$. If the result is different from 0 (which can always be proved if true), then by the proven results on the BSD conjecture we know that the rank of E_c is equal to 0, hence that c is not a sum of two cubes. On the other hand if the result seems to be very close to 0, then it is highly plausible (but not proved, even assuming BSD) that c is a sum of two cubes since the rank of E_c will probably be at least equal to 2.

In this manner, it is easy to construct the following table, whose validity does not depend on BSD since in the range of the table we only have curves of analytic rank 0 or 1, or curves with proven rank 2 or 3. The entry in row numbered R and column C (with R going from 0 to 1953 and C going from 1 to 63) gives the rank of the curve E_c with $c = R + C$, except when the rank is 0 and the curve has nontrivial torsion (which occurs if and only if c is equal

to a cube or twice a cube), in which case the letter `T` occurs, corresponding to the trivial solutions $0^3+1^3=1$ and $1^3+1^3=2$, and their multiples.

	111111111122222222223333333333444444444455555555556666 123456789012345678901234567890123456789012345678901234567890123
0	TT00011T1001101T1021010001T10210111020000110000111101T010100111
63	T20111111001001100001121011210101110000111110020001101001001 2T2
126	2T0102110100111110000000122001101111210100111100011111022001101
189	000101011002120110122111111T22200111000110101001010210110211 1T10
252	020001100001101010212110111102111110100001120000101011012100110
315	1001011111000011010211010 12T1210210100011111000100110020110 0010
378	21010111110211111120210110102110101100010211011011111T202201101
441	001121111012100111102111112200001002000101110010100111122101111
504	0200011T2001101211211100010100111111000101101101121010210100110
567	100111101012021100001121011010101111110101111022001100001001211
630	21012011200011111001200110320110101001012111010011111 00T0201100
693	001101111000100111122111111200010 12T201101111010100110101111111
756	000001101001101010110100110102111110220001100001101012012100111
819	100112111200101101001001011110020132100111110021001101211101210
882	212100111100101111202021100001101211210102011002111111200201101
945	20111101101210111010210111020100110100110121002012011 2T20111112
1008	00000112000 3121T0021010011110211111100000010002211101121 0100110
1071	120011110000001110001101010202100110100111110000103101001121211
1134	010102111100111210002101101001101011210110110100101110020001101
1197	000121012012000110200111112100201100001101030010101101102111111
1260	200021300201100011010100110102111111000101121001101110012100111
1323	1101113T2000001300020101011012102111102111111020001011221101011
1386	210100112100101110020101101001101010011302111100111111002011100
1449	10012121T2101221111001011010200031000011210110121011100201111 11
1512	202001101001001010212100110100111110012003100001101011202100010
1575	120111111001201100021101011212102112100111110220211101000101010
1638	010102111101111110200001112001101211110102001120111111010101111
1701	02110101101010011010211011T2000001210211212100100021121201011 10
1764	000001102011101010012100111102111310200201101001102011010101010
1827	100111111002001101001111032002100111102111110001201100001101111
1890	230120111000111111000001101002101021010100110000111111022000111
1953	021121010010122110100011112202101120001121210 0T2102111120111130

Sums of Two Rational Cubes up to 2016

To find explicitly the decomposition of a cubefree integer $c \leqslant 2016$ as a sum of two cubes the reader should proceed as follows. If the table above indicates `0` there are no solutions. If it indicates `T`, there is only one solution, either $c = x^3$ if c is a cube, or $c = x^3 + x^3$ if c is twice a cube. If it indicates `2` or `3`, then for all $c \leqslant 2016$ the `mwrank` program or the 2-descent methods of Chapter 8 will succeed in finding a nontrivial point on the elliptic curve $y^2 = x^3 + 16c^2$, which can then be transformed into a solution of $x^3 + y^3 = c$ thanks to Proposition 7.2.3 and the remarks following it. Finally, if it indicates `1` then either `mwrank` or 2-descent will find a nontrivial rational point, or we apply the Heegner point method described in Section 8.6.

We now consider the case of three cubes. The main conjecture, now widely believed to be true, is the following.

Conjecture 6.4.21. *An integer* n *is a sum of three cubes of integers if and only if* $n \not\equiv \pm 4 \pmod 9$.

Note that since the cube of an integer is congruent to 0 or ± 1 modulo 9, an integer $n \equiv \pm 4 \pmod 9$ cannot be the sum of three cubes. The conjecture claims that this is the only restriction.

It is also conjectured that any integer not congruent to ± 4 modulo 9 is a sum of three cubes of integers in an infinite number of ways. However, to

the author's knowledge the only known representations of the integer 3 are $3 = 1^3 + 1^3 + 1^3 = 4^3 + 4^3 + (-5)^3$ (and permutations of the latter).

A large amount of computer work has been done on these conjectures. For a long time the smallest positive integer $n \not\equiv \pm 4 \pmod 9$ not known to be a sum of three cubes was $n = 30$, until the discovery by M. Beck, E. Pine, W. Tarrant and K. Yarbrough of the decomposition

$$30 = (-283059965)^3 + (-2218888517)^3 + (2220422932)^3 .$$

As of 2005 the only integers n such that $0 \leqslant n \leqslant 100$ and $n \not\equiv \pm 4 \pmod 9$ which are not known to be a sum of three cubes are $n = 33$, 42, 52, and 74. The size of the solutions found suggest that they are at least exponential in n.

Note that, contrary to similar results for squares, we must not assume that n is cubefree. To take a simple example, 5 is evidently not a sum of three cubes, but $135 = 3^3 \cdot 5 = 2^3 + (-6)^3 + 7^3$ is one.

Indeed, as for two cubes the situation changes dramatically for the representation with *rational* numbers:

Proposition 6.4.22. *Every integer (and in fact every rational number) is the sum of three cubes of rational numbers. For instance we have $n = x^3 + y^3 + z^3$, with*

$$x = m - 1,\ y = \frac{3(m^2+m)}{m^2+m+1},\ z = \frac{-m^3+3m+1}{m^2+m+1} ,$$

where we have set $m = n/9$.

Proof. Just check. Of course this does not explain how to obtain such identities or why they exist. □

We now consider the case of four or more cubes. Because of the above proposition we no longer need to consider representations as sums of cubes of rational numbers. For integers there is a conjecture (a weak version and a strong version), and two results.

Conjecture 6.4.23. (1) (*Weak version.*) *Every integer is a sum of four cubes of integers.*

(2) (*Strong version.*) *Every integer has the form $2x^3 + y^3 + z^3$, hence is a sum of four cubes of integers of which two at least are equal.*

The two known results on this subject are as follows. The first is very easy, and the second is due to Dem'janenko [Dem1].

Proposition 6.4.24. *Every integer is a sum of five cubes of integers, where we can in fact assume that at least two are equal. In other words every integer has the form $2x^3 + y^3 + z^3 + t^3$.*

Proof. The identity $6x = (x-1)^3 + (-x)^3 + (-x)^3 + (x+1)^3$ shows that every multiple of 6 is a sum of four cubes of which two are equal. If n is an integer, $n - n^3$ is divisible by 6 hence is a sum of four cubes, so $n = (n - n^3) + n^3$ is a sum of five cubes of which two are equal. □

Theorem 6.4.25 (Dem'janenko). *Every integer n such that $n \not\equiv \pm 4 \pmod 9$ is a sum of four cubes of integers.*

Note that this theorem was certainly conjectured as far back as the end of the nineteenth century, but was only proved by Dem'janenko in 1966, see [Dem1].

Proof. First the polynomial identities

$$\begin{aligned} 6x &= (x-1)^3 + (-x)^3 + (-x)^3 + (x+1)^3 \text{ and} \\ 6x+3 &= x^3 + (-x+4)^3 + (2x-5)^3 + (-2x+4)^3 \end{aligned}$$

show that every multiple of 3 is a sum of four cubes. Next the identities

$$\begin{aligned} 18x+1 &= (2x+14)^3 + (-2x-23)^3 + (-3x-26)^3 + (3x+30)^3\,, \\ 18x+7 &= (x+2)^3 + (6x-1)^3 + (8x-2)^3 + (-9x+2)^3\,, \\ 18x+8 &= (x-5)^3 + (-x+14)^3 + (-3x+29)^3 + (3x-30)^3\,, \end{aligned}$$

together with the complementary identities obtained by changing x into $-x$ and multiplying by -1 show that every $n \equiv \pm 1, \pm 7$ or ± 8 modulo 18 is a sum of four cubes. The only remaining congruence classes are $n \equiv \pm 2 \pmod{18}$. Finally the polynomial identities

$$\begin{aligned} 54x+2 &= (29484x^2 + 2211x + 43)^3 + (-29484x^2 - 2157x - 41)^3 \\ &\quad + (9828x^2 + 485x + 4)^3 + (-9828x^2 - 971x - 22)^3 \\ 54x+20 &= (3x-11)^3 + (-3x+10)^3 + (x+2)^3 + (-x+7)^3 \\ 216x-16 &= (-27x+13)^3 + (24x-12)^3 + (18x-8)^3 + (3x-3)^2 \text{ and} \\ 216x+92 &= (3x-164)^3 + (-3x+160)^3 + (x-35)^3 + (-x+71)^3 \end{aligned}$$

together with their complementary identities only leave the congruence classes $n \equiv \pm 38 \pmod{108}$, hence let $n \in \mathbb{Z}$ be of this form. Changing if necessary n into $-n$ we may assume that $n \equiv 38 \pmod{108}$.

In the sequel, denote by p the prime number $p = 83$. Assume first that $p \mid n$. Then $n/p \equiv 38p^{-1} \equiv 46 \pmod{108}$, and the identity

$$\begin{aligned} 83(108x+46) &= (29484x^2 + 25143x + 5371)^3 + (-29484x^2 - 25089x - 5348)^3 \\ &\quad + (9828x^2 + 8129x + 1682)^3 + (-9828x^2 - 8615x - 1889)^3 \end{aligned}$$

shows that n is a sum of four cubes. We may thus assume that $n \equiv 38 \pmod{108}$ with $p \nmid n$.

Let a, b, m be integers and set

$$w = -(24m - 25a + 2937b),\ x = 27m - 19a + 2746b,$$
$$y = -(19m + 9a + 602b),\ z = 10m + 27a - 928b\ .$$

We check that $w^3 + x^3 + y^3 + z^3 = 18p(a^2 - 3420b^2)m + P(a,b)$, with

$$P(a,b) = (25a - 2937b)^3 + (-19a + 2746b)^3 + (-9a - 602b)^3 + (27a - 928b)^3\ .$$

Thus, if a and b are chosen as solutions of the Pell equation $a^2 - 3420b^2 = 1$ we have $w^3 + x^3 + y^3 + z^3 = 18pm + P(a,b)$ hence, given such a pair (a,b), the equation $w^3 + x^3 + y^3 + z^3 = n$ is solvable in m if and only if $P(a,b) \equiv n$ is solvable modulo 2, 9, and p. Since $n \equiv 2 \pmod{18}$, the condition modulo 2 is $2 \mid b$, and the condition modulo 9 is easily seen to be $a \equiv 1 \pmod 3$ and $b \equiv 2 \mod 3$. Thus the condition modulo 18 is $a \equiv 1 \pmod 3$ and $b \equiv 2 \pmod 6$. There remains the condition modulo p.

The fundamental unit of the order $\mathbb{Z}[\sqrt{3420}]$ is easily computed to be $\varepsilon = 3041 + 52\sqrt{3420}$, which has norm 1. Thus $a + b\sqrt{3420} = s\varepsilon^k$ for any $k \in \mathbb{Z}$ and $s = \pm 1$, in other words

$$a = s\frac{\varepsilon^k + \overline{\varepsilon}^k}{2} \quad \text{and} \quad b = s\frac{\varepsilon^k - \overline{\varepsilon}^k}{2\sqrt{3420}}\ .$$

Since a and b satisfy a second order linear recurrence, it is immediately seen that the congruence conditions modulo 3 and 6 on a and b are equivalent to $a + b\sqrt{3420} = (-\varepsilon)^k$ with $k \equiv 1 \pmod 3$. Thus if we set $\eta = -\varepsilon^3$ and $j = (k-1)/3$ we have

$$a = \frac{(-\varepsilon)\eta^j + \overline{(-\varepsilon)}\,\overline{\eta}^j}{2} \quad \text{and} \quad b = \frac{(-\varepsilon)\eta^j - \overline{(-\varepsilon)}\,\overline{\eta}^j}{2\sqrt{3420}}\ .$$

We note that $3420 \equiv 10^2 \pmod p$, hence that $\varepsilon \equiv 75 \pmod p$, $\overline{\varepsilon} \equiv 31 \pmod p$, $\eta \equiv 14 \pmod p$, and $\overline{\eta} \equiv 6 \pmod p$, so that

$$a \equiv \frac{8 \cdot 14^j - 31 \cdot 6^j}{2} \pmod p \quad \text{and} \quad b \equiv \frac{8 \cdot 14^j + 31 \cdot 6^j}{2 \cdot 10} \pmod p\ ,$$

and replacing gives finally

$$P(a,b) \equiv 71 \cdot 50^j \pmod p\ .$$

Now it is immediately checked that 50 is a primitive root modulo p. Since $\gcd(71, p) = 1$ it follows that for any n such that $p \nmid n$ there exists $j \in \mathbb{Z}$ with $71 \cdot 50^j \equiv n \pmod p$, hence there exists a and b such that $P(a,b) \equiv n \pmod p$, proving that the condition modulo p can be satisfied and finishing the proof of the theorem. □

Remarks.

(1) The above proof is translated essentially verbatim from Dem'janenko's paper, but with a few minor improvements. First it is not at all clear from this proof how one obtains the second degree polynomial identities and why we define w, x, y, and z as above (for instance why use the identity $(-24)^3+27^3+(-19)^3+10^3=0$ among so many similar ones?). This has been explained by M. Watkins in an unpublished manuscript. Furthermore, Dem'janenko chooses the prime $p=3323$, but Watkins shows that one can use the smaller prime $p=83$, so that I have used this p instead. Finally, the identity for $216x-16$ was sent to me by D. Alpern, and replaces a more complicated identity involving quadratic polynomials analogous to the one for $54x+2$ found by Dem'janenko. It can be found very simply from the identity for $18x+7$ by a linear change of variable.

(2) I would like to emphasize that the above proof gives a covering set of 82 identities involving linear polynomials for all integers $n \equiv 38 \pmod{108}$. For instance, the choice $a+b\sqrt{3420}=-\varepsilon$ and a linear change of variable leads to the identity

$$1494x-178=(-24x-213614285)^3+(27x+240317344)^3 \\ +(-19x-169113356)^3+(10x+89004059)^3\,.$$

(3) The use of polynomial identities is essential in the above proof. It is natural to ask whether it is possible to use such identities also for integers congruent to ± 4 modulo 9 (with a left hand side which is *linear* in x). It has been proved by Schinzel, Mordell and successors that such an identity does not exist with polynomials of degree less than or equal to 7. It is reasonable to conjecture that no such identity exists.

To conclude this section, we note the following related result.

Proposition 6.4.26. *Up to permutation of the variables the equation* $w^3+x^3+y^3+z^3=0$ *in* $\mathbb{Q}$ *has the trivial parametrization* $x=-w$, $z=-y$, *and the parametrization*

$$\begin{aligned} w &= -d((s-3t)(s^2+3t^2)+1) \\ x &= d((s+3t)(s^2+3t^2)+1) \\ y &= -d((s^2+3t^2)^2+(s+3t)) \\ z &= d((s^2+3t^2)^2+(s-3t)) \end{aligned}$$

with d, s, *and* t *in* $\mathbb{Q}$.

Proof. If we set $W=(w+x)/2$, $X=(x-w)/2$, $Y=(y+z)/2$, and $Z=(z-y)/2$ the equation is equivalent to $W(W^2+3X^2)=-Y(Y^2+3Z^2)$. Excluding the trivial parametrization we have $W\neq 0$ and $Y\neq 0$, so that if

we define s and t by $(Y + Z\sqrt{-3})/(W + X\sqrt{-3}) = s + t\sqrt{-3}$, we have by definition $sW - 3tX = Y$ and $sX + tW = Z$, and the equation is equivalent to $W = -Y(s^2 + 3t^2)$. Thus $-3tX = Y(1 + s(s^2 + 3t^2))$ or, equivalently, $X = d(1 + s(s^2 + 3t^2))$ and $Y = -3dt$, hence $W = 3dt(s^2 + 3t^2)$ and $Z = d(s + (s^2 + 3t^2)^2)$, so we obtain the given parametrization. □

When s, t and d are integers the solution is trivially integral, but the converse is not true (choose for instance $d = -361/42$, $s = -10/19$, $t = -7/19$, which gives one of the smallest nontrivial integral solution $(w, x, y, z) = (12, 1, -10, -9)$). No complete parametrization of the equation in integers is known, but nontrivial partial ones are easy to find, see Exercise 22. Note that Elkies gives the following homogeneous rational parametrization:

$$\begin{aligned} w &= d(-(r+s)t^2 + (s^2+2r^2)t - s^3 + rs^2 - 2r^2s - r^3) \\ x &= d(t^3 - (r+s)t^2 + (s^2+2r^2)t + rs^2 - 2r^2s + r^3) \\ y &= d(-t^3 + (r+s)t^2 - (s^2+2r^2)t + 2rs^2 - r^2s + 2r^3) \\ z &= d((s-2r)t^2 + (r^2-s^2)t + s^3 - rs^2 + 2r^2s - 2r^3)\ . \end{aligned}$$

Here $d = 1/7$, $r = 1$, $s = -4$, and $t = -2$ give the solution $(9, -1, 10, -12)$.

6.5 Skolem's Equation $x^3 + dy^3 = 1$

6.5.1 The Basic Theorem

The aim of this section is to prove the following theorem.

Theorem 6.5.1 (Skolem). *If $d \in \mathbb{Z}$ is given with $d \neq 0$, there exists at most one pair $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ with $y \neq 0$ such that $x^3 + dy^3 = 1$.*

Proof. If $d = c^3$ with $c \in \mathbb{Z}$, then $(x + cy) \mid (x^3 + dy^3) = 1$, hence $x + cy = \pm 1$. Replacing in the equation gives $\pm 1 - 3cy \pm 3c^2y^2 = 1$, hence looking modulo 3 we have $\pm = +$, hence $cy(cy - 1) = 0$. Thus since we assume $d \neq 0$ and $y \neq 0$, we obtain $y = 1/c$ as the only possible solution (if $d = \pm 1$), otherwise none. Thus, assume that d is not a perfect cube, and let $K = \mathbb{Q}(\theta)$ with $\theta = d^{1/3}$ be the corresponding pure cubic field. In particular its signature is $(1, 1)$, hence by Dirichlet's unit theorem there exists a fundamental unit ε such that any unit has the form $\pm\varepsilon^k$ for $k \in \mathbb{Z}$. Changing if necessary ε into $-\varepsilon$ we may assume that ε has norm $+1$.

Assume now that there exist two solutions (x_1, y_1) and (x_2, y_2) to our equation with $y_1 \neq 0$ and $y_2 \neq 0$, and set $\varepsilon_i = x_i + y_i\theta$ for $i = 1$ and 2. Our equation is equivalent to $\mathcal{N}_{K/\mathbb{Q}}(\varepsilon_i) = 1$, hence since the ε_i are algebraic integers, they are units in K of norm 1, so that $\varepsilon_i = \varepsilon^{p_i}$ for some $p_i \in \mathbb{Z}$. Writing $p_1/p_2 = n_1/n_2$ with $\gcd(n_1, n_2) = 1$, we thus have $(x_1 + y_1\theta)^{n_2} =$

$(x_2+y_2\theta)^{n_1}$, and if necessary exchanging (x_1,y_1) and (x_2,y_2) we may assume that $3 \nmid n_1$. Thus $N = n_2/n_1$ can be considered as an element of $\mathbb{Z}_3$. To simplify, write $x = x_1$ and $y = y_1$. By definition of θ, we have

$$(x+y\theta)^3 = x^3 + 3x^2y\theta + 3xy^2\theta^2 + dy^3 = 1 + 3xyG \quad \text{with} \quad G = x\theta + y\theta^2 \ .$$

We will work in $\mathbb{Q}_3(\theta)$, which by Proposition 4.4.41 is isomorphic to the direct sum of the completions of $\mathbb{Q}(\theta)$ for the absolute values corresponding to the prime ideals of $\mathbb{Z}_K$ dividing 3. Write $N = 3M + r$ with $0 \leqslant r \leqslant 2$. Since $N \in \mathbb{Z}_3$, by Corollary 4.2.13 we can thus write $x_2 + y_2\theta = (1+3xyG)^M(x+y\theta)^r$, where $(1+3xyG)^M$ is *defined* by a convergent binomial series. Thus, using Corollary 4.2.15 (which was proved for a $\mathfrak{p}$-adic field but is clearly still true for a product of such), we have

$$x_2+y_2\theta = (1+3xyG)^M(x+y\theta)^r = (1+3Mxy(x\theta+y\theta^2)+9Mx^2y^2B)(x+y\theta)^r$$

for some $B \in \mathbb{Z}_3[\theta]$. Note that even though $\mathbb{Q}_3(\theta)$ is not in general a field, 1, θ, and θ^2 are still $\mathbb{Q}_3$-linearly independent, hence we may identify the coefficients of powers of θ in the above formula. In particular, if we write $B = B_0 + B_1\theta + B_2\theta^2$ with $B_i \in \mathbb{Z}_3$ and identify the coefficients of θ^2 we obtain

$$0 = \begin{cases} 3Mxy^2(1+3xB_2) & \text{for } r = 0 \\ 3Mx^2y^2(2+3(yB_1+xB_2)) & \text{for } r = 1 \\ y^2(1+9Mx^2(x+B_2x^2+2B_1xy+B_0y^2)) & \text{for } r = 2 \ . \end{cases}$$

Since x and y are nonzero, and N is not equal to 0 or 1, we can divide respectively by $3Mxy^2$, $3Mx^2y^2$ and y^2, and we immediately obtain a contradiction modulo 3. □

6.5.2 Special Cases

Since we can replace y^3 by c^3y^3 for any $c \in \mathbb{Z}$, in Skolem's theorem we may assume that d is a positive cubefree integer.

Corollary 6.5.2. *For $d = 1, 2, 7, 9, 17, 19, 20, 26, 28, 37, 43, 63, 65$ and 91 the equation $x^3 + dy^3 = 1$ has a (necessarily unique) integral solution with $y \neq 0$, given respectively by $(x,y) = (0,1), (-1,1), (2,-1), (-2,1), (18,-7), (-8,3), (-19,7), (3,-1), (-3,1), (10,-3), (-7,2), (4,-1), (-4,1)$ and $(9,-2)$.*

Proof. Clear by direct check, the uniqueness coming from Skolem's theorem. □

Corollary 6.5.3. *The only* integral *solutions to the equation $y^2 = x^3 + 1$ are $(x,y) = (-1,0), (0,\pm1)$ and $(2,\pm3)$.*

Proof. We rewrite the equation as $(y-1)(y+1) = x^3$. If y is even, $y-1$ and $y+1$ are coprime, hence are both cubes, and since the only two cubes which differ by 2 are -1 and 1 we deduce that $(x,y) = (-1,0)$. Otherwise y is odd, hence x is even. Changing if necessary y into $-y$ we may assume that $y \equiv 1 \pmod 4$. Thus $((y-1)/4)((y+1)/2) = (x/2)^3$, hence there exist integers a and b such that $y-1 = 4a^3$ and $y+1 = 2b^3$, so that $b^3 - 2a^3 = 1$. By Skolem's theorem above, the only solutions to this equation are $(a,b) = (0,1)$ and $(-1,-1)$, giving the solutions $(x,y) = (0,\pm 1)$ and $(2,\pm 3)$. □

The following result can be shown using only slightly more complicated methods.

Theorem 6.5.4 (Delone). *Let d be a positive cubefree integer. The equation $x^3 + dy^3 = 1$ has a nontrivial integral solution if and only if the fundamental unit ε of the* ring $\mathbb{Z}[d^{1/3}]$ *(which is not necessarily equal to the full ring of integers of $\mathbb{Q}(d^{1/3})$) such that $0 < \varepsilon < 1$ has the form $x + yd^{1/3}$ with x and y in $\mathbb{Z}$.*

Using this theorem, it is immediate to check that the values of d given in Corollary 6.5.2 are the *only* positive cubefree values of d less than or equal to 100 for which Skolem's equation has a solution with $y \neq 0$. The only additional such values for $d \leqslant 1000$ are $d = 124$, 126, 182, 215, 217, 254, 342, 422, 511, 614, 635, 651, 730 and 813. Let us show how we can prove that there are no nontrivial solutions in the particular case $d = 11$.

Proposition 6.5.5. *The only integral solution to $x^3 + 11y^3 = 1$ is the trivial solution $(x,y) = (1,0)$.*

Proof. We work in the number field $\mathbb{Q}(\theta)$ with $\theta = 11^{1/3}$. A fundamental unit is $\varepsilon = 1 + 4\theta - 2\theta^2$, with $\mathcal{N}_{K/\mathbb{Q}}(\varepsilon) = 1$. Since our Diophantine equation is equivalent to $\mathcal{N}_{K/\mathbb{Q}}(x + y\theta) = 1$, Dirichlet's unit theorem tells us that $x + y\theta = \varepsilon^n$ for some $n \in \mathbb{Z}$.

The smallest prime p in which $X^3 - 11$ splits completely is $p = 19$, hence we work in $\mathbb{Q}_{19}$, in which the three roots are $c_1 \equiv -3 + 5 \cdot 19 \pmod{19^2}$, $c_2 \equiv -2 + 8 \cdot 19 \pmod{19^2}$ and $c_3 \equiv 5 + 6 \cdot 19 \pmod{19^2}$. The corresponding values of the embeddings of ε are $e_1 \equiv 9 + 2 \cdot 19 \pmod{19^2}$, $e_2 \equiv 4 \pmod{19^2}$, $e_3 \equiv 9 + 16 \cdot 19 \pmod{19^2}$, and for $j = 1$, 2 and 3 we have $x + yc_j = e_j^n$. Since $\mathrm{Tr}_{K/\mathbb{Q}}(\theta) = \mathrm{Tr}_{K/\mathbb{Q}}(\theta^2) = 0$, we have $\sum_j c_j = \sum_j c_j^2 = 0$, hence $c_1 e_1^n + c_2 e_2^n + c_3 e_3^n = 0$. On the other hand, since $\mathcal{N}_{K/\mathbb{Q}}(\varepsilon) = 1$ we have $e_1 e_2 e_3 = 1$, hence replacing e_1 by $(e_2 e_3)^{-1}$ and multiplying by $(e_2 e_3)^n$ we obtain

$$c_1 + c_2 e_2^{2n} e_3^n + c_3 e_2^n e_3^{2n} = 0 \, .$$

We first consider this equation modulo 19. We obtain $16 + 17 \cdot 11^n + 5 \equiv 0 \pmod{19}$, in other words $11^n \equiv 1 \pmod{19}$ or, equivalently since the order of 11 modulo 19 is equal to 3, $n \equiv 0 \pmod 3$. Thus, we must have $n = 3m$ for some $m \in \mathbb{Z}$. But then we have $(e_2^2 e_3)^3 \equiv 1 + 7 \cdot 19 \pmod{19^2}$ and $(e_2 e_3^2)^3 \equiv$

$1 + 11 \cdot 19 \pmod{19^2}$. Thus, with the notation of Corollary 4.2.16, we have $(e_2^2 e_3)^n = \phi_a(m)$ and $(e_2 e_3^2)^n = \phi_b(m)$ for $a = e_2^2 e_3 - 1$ and $b = e_2 e_3^2 - 1$. We immediately see that $\phi_a(X) = 1+7\cdot 19\,X \pmod{19^2}$ and $\phi_b(X) = 1+11\cdot 19\,X \pmod{19^2}$, and since $c_1 + c_2 + c_3 = 0$, our equation has the form $\phi(m) = 0$ with $\phi(X) \equiv 3 \cdot 19\,X \pmod{19^2}$. In the notation of Strassmann's theorem we thus have $N = 1$, hence there is only one solution $m = 0$ corresponding to $(x, y) = (1, 0)$, as claimed. □

6.5.3 The Equations $y^2 = x^3 \pm 1$ in Rational Numbers

In Corollary 6.5.3 we have found all *integral* solutions to the equation $y^2 = x^3+1$. It is instructive to see how to find all *rational* solutions to this equation. The method that we use is not related to Skolem's, but is an example of a *descent* method which we will explore in more detail in Section 8.2. This proof is essentially due to L. Euler. I would like to thank B. de Weger and R. Schoof for showing me their version, and the one below is a (slight) blend of the two. We slightly simplify Euler's argument by using the following lemma.

Lemma 6.5.6. *Let $K = \mathbb{Q}(\sqrt{-3})$ and $\alpha \in \mathbb{Z}_K$. Then $\alpha\overline{\alpha}$ is a square in $\mathbb{Z}$ if and only if there exist $n \in \mathbb{Z}$ and $\beta \in \mathbb{Z}_K$ such that $\alpha = n\beta^2$.*

Proof. Since $\mathbb{Z}_K$ is a principal ideal domain, simply decompose α into a product of a root of unity by a product of powers of prime elements of $\mathbb{Z}_K$. The details are left to the reader (Exercise 24). □

The key descent result of Euler is the following.

Proposition 6.5.7. *Let $\varepsilon = \pm 1$. The only nonzero integral solutions to the Diophantine equations $Y^2 = XZ(X^2 - 3\varepsilon XZ + 3Z^2)$ with $\gcd(X, Z) = 1$ are for $\varepsilon = 1$, with $(X, Z) = \pm(1, 1)$ (hence $Y = \pm 1$) or $\pm(3, 1)$ (hence $Y = \pm 3$).*

Proof. Since the discriminant of $X^2 - 3\varepsilon X + 3$ is negative it follows that $XZ > 0$, in other words X and Z have the same sign. Thus if necessary changing (X, Z) into $(-X, -Z)$ we may assume they are both positive.

Assume first that $3 \nmid X$, and consider a solution to our equation where $|Y| > 1$ is *minimal*. As always in descent arguments we are going to construct another solution with a strictly smaller value of $|Y|$, hence giving a contradiction. Thus X, Z and $X^2 - 3\varepsilon XZ + 3Z^2$ are pairwise coprime, and since they are all positive they are all three squares, so we write $X = x^2$, $Z = z^2$ and $X^2 - 3\varepsilon XZ + 3Z^2 = a^2$, say. If we set $\alpha = X + Z(-3\varepsilon + \sqrt{-3})/2 \in \mathbb{Z}_K$, we see that $\alpha\overline{\alpha} = a^2$, so that by the above lemma we have $\alpha = n\beta^2$ with $n \in \mathbb{Z}$ and $\beta \in \mathbb{Z}_K$. Since $(1, (-3\varepsilon + \sqrt{-3})/2)$ is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$, we write $\beta = u+v(-3\varepsilon+\sqrt{-3})/2$, and equating coefficients we obtain $X = n(u^2-3v^2)$, $Z = n(2uv - 3\varepsilon v^2)$. Since X and Z are coprime, it follows that $n = \pm 1$, that u and v are coprime and $3 \nmid u$. Since X is a square and $3 \nmid u$ we

have $X \equiv nu^2 \equiv n \pmod 3$, hence $n \equiv 1 \pmod 3$ so in fact $n = 1$. We thus obtain the system of equations $u^2 = x^2 + 3v^2$, $z^2 = v(2u - 3\varepsilon v)$. If $\alpha_1 = x + v\sqrt{-3}$ we have $\alpha_1\overline{\alpha_1} = u^2$, so again by the above lemma there exists $\beta_1 = (s + t\sqrt{-3})/2 \in \mathbb{Z}_K$, hence with $s \equiv t \pmod 2$, and $n_1 \in \mathbb{Z}$ such that $\alpha_1 = n_1\beta_1^2$, which gives by equating coefficients $x = n_1(s^2 - 3t^2)/4$, $v = n_1st/2$, hence $u = n_1(s^2 + 3t^2)/4$. Replacing in the formula for z^2, we obtain $z^2 = (n_1/2)^2st(s^2 - 3\varepsilon st + 3t^2)$. It follows that $Y_1 = z/(n_1/2)$ is an integer such that $Y_1^2 = st(s^2 - 3\varepsilon st + 3t^2)$, so we have obtained a new solution to our Diophantine equation. Evidently s and t are nonzero (otherwise v, hence Z is zero). If $g = \gcd(s,t)$ (equal in fact to 1 or 2), replacing (s,t,Y_1) by $(s/g, t/g, Y_1/g^2)$ we may assume that s and t are coprime. Let us show that $|Y_1| < |Y|$. Indeed, we have

$$\frac{Y^2}{Y_1^2} = \frac{XZ(X^2 - 3\varepsilon XZ + 3Z^2)}{4z^2/n_1^2} \geqslant \frac{X(X^2 - 3\varepsilon XZ + 3Z^2)}{4}\ .$$

Now $X^2 - 3\varepsilon XZ + 3Z^2 \geqslant 7$ for $\varepsilon = -1$. For $\varepsilon = 1$, since $Z = z^2$ we have $X^2 - 3XZ + 3Z^2 = (X - 3Z/2)^2 + 3Z^2/4 \geqslant 3z^4/4 > 1$ for $|z| \geqslant 2$. For $\varepsilon = Z = 1$, since $X = x^2$ we have $X(X^2 - 3\varepsilon X + 3) \geqslant x^2(x^4 - 3x^2 + 3) > 4$ for $|x| > 1$. It follows from all this that $|Y| > |Y_1|$ unless $\varepsilon = X = Z = 1$. But in that case we have $|Y| = 1$, and since we have initially assumed that $|Y| > 1$, this gives the desired contradiction showing that when $3 \nmid X$ the only possible solution has $|Y| = 1$, which is indeed possible with $\varepsilon = 1$ and $X = Z = 1$, but not possible if $\varepsilon = -1$.

If $3 \mid X$ then $3 \mid Y$, hence $(Y/3)^2 = Z(X/3)(Z^2 - 3\varepsilon Z(X/3) + 3(X/3)^2)$, and since $\gcd(X,Z) = 1$ we have $3 \nmid Z$, so by we have just proved we have $\varepsilon = 1$, $(Z, X/3) = \pm(1,1)$ hence $(X,Z) = \pm(3,1)$. □

Corollary 6.5.8. *The only* rational *solutions of the equation* $y^2 = x^3 - 1$ *is* $(x,y) = (1,0)$, *and the only rational solutions of the equation* $y^2 = x^3 + 1$ *are* $(x,y) = (-1,0)$, $(0,\pm1)$ *and* $(2,\pm3)$.

As already mentioned we will later give a similar proof of this result (Proposition 8.2.14), this time using 2-descent explicitly.

Proof. Write $x = m/n$ with $\gcd(m,n) = 1$. Multiplying the equation $y^2 = x^3 + \varepsilon$ by n^4 we see that $n(m^3 + \varepsilon n^3)$ is a square, and if we set $c = m + \varepsilon n$ this means that $nc(m^2 - \varepsilon mn + n^2) = nc(c^2 - 3\varepsilon nc + 3n^2)$ is a square. Clearly $\gcd(c,n) = \gcd(m,n) = 1$, $n \neq 0$, and $c \neq 0$ except if $m = -\varepsilon n$, i.e., $x = -\varepsilon$. Thus by the above proposition we deduce that otherwise we have $\varepsilon = 1$, and $(c,n) = \pm(1,1)$ or $\pm(3,1)$, giving $x = 0$ or $x = 2$ respectively, and proving the corollary. □

6.6 The Fermat Quartics $x^4 + y^4 = cz^4$

For a more detailed study of these Diophantine equations, in particular over number fields, I refer to [Cal].

We will denote by $\mathcal{C}_c$ the projective curve defined by the equation $x^4+y^4 = cz^4$. We may clearly assume that c is not divisible by a fourth power strictly greater than 1.

6.6.1 Local Solubility

We begin by studying local solubility over $\mathbb{Q}$, in order to give a necessary and sufficient condition for the equation to be everywhere locally soluble.

Proposition 6.6.1. (1) *$\mathcal{C}_c(\mathbb{Q}_2) \neq \emptyset$ if and only if $c \equiv 1$ or 2 modulo 16.*
(2) *If p is an odd prime divisor of c, then $\mathcal{C}_c(\mathbb{Q}_p) \neq \emptyset$ if and only if $p \equiv 1 \pmod 8$.*
(3) *If $p \equiv 3 \pmod 4$ is a prime not dividing c then $\mathcal{C}_c(\mathbb{Q}_p) \neq \emptyset$.*
(4) *If $p \geqslant 37$ is a prime not dividing c then $\mathcal{C}_c(\mathbb{Q}_p) \neq \emptyset$.*
(5) *$\mathcal{C}_c(\mathbb{Q}_{17}) \neq \emptyset$.*
(6) *Let $p \in \{5, 13, 29\}$ be a prime not dividing c. Then*
  a) $\mathcal{C}_c(\mathbb{Q}_5) \neq \emptyset$ if and only if $c \not\equiv 3$ or 4 modulo 5.
  b) $\mathcal{C}_c(\mathbb{Q}_{13}) \neq \emptyset$ if and only if $c \not\equiv 7$, 8 or 11 modulo 13.
  c) $\mathcal{C}_c(\mathbb{Q}_{29}) \neq \emptyset$ if and only if $c \not\equiv 4$, 5, 6, 9, 13, 22 or 28 modulo 29.

Proof. If $(x : y : z) \in \mathcal{C}_c(\mathbb{Q}_p)$, we may clearly assume that x, y and z are p-adic integers and that at least one is a p-adic unit. If $p \nmid c$, reduction modulo p gives a projective curve $\overline{\mathcal{C}_c}$ over $\mathbb{F}_p$, which is smooth (nonsingular) if $p \neq 2$.

(1). Let u be a 2-adic unit. I claim that $u \in \mathbb{Q}_2^4$ if and only if $u \equiv 1 \pmod{16\mathbb{Z}_2}$. Indeed, if v is a 2-adic unit we can write $v = 1 + 2t$ with $t \in \mathbb{Z}_2$, and

$$v^4 = 1 + 8t + 24t^2 + 32t^3 + 16t^4 \equiv 1 + 8(t(3t+1)) \equiv 1 \pmod{16}\,.$$

Conversely, if $u \equiv 1 \pmod{16\mathbb{Z}_2}$ we write $u = 1 + x$ with $v_2(x) \geqslant 4$, and it is easy to check that the binomial expansion for $(1+x)^{1/4}$ converges for $v_2(x) \geqslant 4$. Alternatively, we set $f(X) = X^4 - u$ and use Hensel's lemma (Proposition 4.1.37): if $u \equiv 1 \pmod{32}$ we have $|f'(1)|_2 = 1/4$ and $|f(1)|_2 \leqslant 1/32 < |f'(1)|_2^2$, while if $u \equiv 17 \pmod{32}$ we have $|f'(5)|_2 = 1/4$ and $|f(5)|_2 \leqslant 1/32 < |f'(5)|_2^2$, proving my claim.

Now assume that $x^4 + y^4 = cz^4$. Since $v_2(c) \leqslant 3$, either x or y is a 2-adic unit. It follows that $x^4 + y^4 \equiv 1$ or 2 modulo 16, hence z is a 2-adic unit, so that $c \equiv 1$ or 2 modulo 16 as claimed. Conversely, if $c \equiv 1 \pmod{16}$ then $c = t^4$ by my claim above, so that $(t : 0 : 1) \in \mathcal{C}_c(\mathbb{Q}_2)$, while if $c \equiv 2 \pmod{16}$, then $c - 1 = t^4$ for some t, hence $(t : 1 : 1) \in \mathcal{C}_c(\mathbb{Q}_2)$, proving (1).

(2). Assume that $p \mid c$ is odd. Since $v_p(c) \leqslant 3$, x and y are p-adic units, so that -1 is a fourth power in $\mathbb{F}_p$. If g is a generator of the cyclic group $\mathbb{F}_p^*$, then $-1 = g^{(p-1)/2}$, hence -1 is a fourth power in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 8$. If this is the case, let $x_0 \in \mathbb{Z}$ such that $x_0^4 \equiv -1 \pmod p$. By Hensel's lemma

(which is trivial here since the derivative of $X^4 + 1$ at x_0 is a p-adic unit), there exists $x \in \mathbb{Z}_p$ such that $x^4 = -1$, so that $(x : 1 : 0) \in \mathcal{C}_c(\mathbb{Q}_p)$, proving (2).

The following lemma shows that for the remaining p it is sufficient to consider the equation in $\mathbb{F}_p$.

Lemma 6.6.2. *Let $p \nmid 2c$ be a prime number. Then $\mathcal{C}_c(\mathbb{Q}_p) \neq \emptyset$ if and only if $\overline{\mathcal{C}_c}(\mathbb{F}_p) \neq \emptyset$. In particular if $p \not\equiv 1 \pmod 8$ then*

$$\mathcal{C}_c(\mathbb{Q}_p) \neq \emptyset \quad \textit{if and only if} \quad c \bmod p \in \mathbb{F}_p^4 + \mathbb{F}_p^4 \ .$$

Proof. One direction is clear. Conversely, assume that $\overline{\mathcal{C}_c}(\mathbb{F}_p) \neq \emptyset$, and let $(x_0 : y_0 : z_0)$ with x_0, y_0, and z_0 not all divisible by p such that $x_0^4 + y_0^4 \equiv cz_0^4 \pmod p$. Since $p \nmid c$, either $p \nmid x_0$ or $p \nmid y_0$. Assume for instance that $p \nmid x_0$, and set $f(X) = X^4 + y_0^4 - cz_0^4$. Clearly $|f'(x_0)|_p = 1$ and $|f(x_0)|_p < 1$, so that by Hensel's lemma there exists $t \in \mathbb{Q}_p$ such that $f(t) = 0$, hence $(t : y_0 : z_0) \in \mathcal{C}_c(\mathbb{Q}_p)$, proving the converse.

Finally, assume that $p \not\equiv 1 \pmod 8$. If $x^4 + y^4 \equiv cz^4 \pmod p$ with x or y not divisible by p, we cannot have $p \mid z$ otherwise $x^4 \equiv -y^4 \pmod p$ so that -1 is a fourth power modulo p, a contradiction. Thus $p \nmid z$, hence $(xz^{-1})^4 + (yz^{-1})^4 \equiv c \pmod p$, finishing the proof of the lemma. □

(3). Let $p \nmid c$, $p \equiv 3 \pmod 4$. I claim that there exist x and y in $\mathbb{Z}$ such that $x^4 + y^4 \equiv c \pmod p$. Indeed, in a finite field $\mathbb{F}$ any element is a sum of two squares (in characteristic 2 any element is a square so the result is trivial, otherwise if $q = |\mathbb{F}|$ then there are $(q+1)/2$ squares hence $(q+1)/2$ elements of the form $c - y^2$, so the two sets have a nonempty intersection, see Proposition 5.2.1). Thus there exist u and v such that $c \equiv u^2 + v^2 \pmod p$. However, when $p \equiv 3 \pmod 4$ we have $\mathbb{F}_p^{*\,2} = \mathbb{F}_p^{*\,4}$: indeed we have a trivial inclusion, and the kernel of the map $x \mapsto x^4$ from $\mathbb{F}_p^*$ into itself is ± 1, so that $|\mathbb{F}_p^{*\,4}| = (p-1)/2 = |\mathbb{F}_p^{*\,2}|$, proving the equality. Thus $c = x^4 + y^4$, as claimed, and the above lemma proves (3).

(4). If $p \nmid 2c$ we may apply Corollary 2.5.23 which tells us in particular $|\overline{\mathcal{C}_c}(\mathbb{F}_p)| \geqslant p + 1 - 6p^{1/2}$. This is strictly positive (for p prime) if and only if $p \geqslant 37$, so that (4) follows from the above lemma. Note that Corollary 2.5.23 is a special case of the Weil bounds, but in the present (diagonal) case we do not need these general bounds but only the case that we have proved.

(5) and (6). Thanks to the above cases, it remains to consider the primes p not dividing c such that $3 \leqslant p \leqslant 31$ and $p \equiv 1 \pmod 4$, in other words $p \in \{5, 13, 17, 29\}$. For such a p, -1 is a fourth power modulo p only for $p = 17$. In that case, Hensel's lemma as usual shows that there exists $t \in \mathbb{Q}_{17}^4$ such that $-1 = t^4$, proving (5) in this case. Otherwise, we compute that

$$\mathbb{F}_5^4 = \{0, 1\}, \quad \mathbb{F}_{13}^4 = \{0, 1, 3, 9\}, \quad \mathbb{F}_{29}^4 = \{0, 1, 7, 16, 20, 23, 24, 25\} \, ,$$

and we deduce the list of nonzero elements of $\mathbb{F}_p^4 + \mathbb{F}_p^4$, proving (6). □

Corollary 6.6.3. *The curve $\mathcal{C}_c$ is everywhere locally soluble (i.e., has points in every completion of $\mathbb{Q}$) if and only if $c > 0$ and the following conditions are satisfied.*

(1) $c \equiv 1$ *or* 2 *modulo* 16.
(2) $p \mid c$, $p \neq 2$ *implies* $p \equiv 1 \pmod 8$.
(3) $c \not\equiv 3$ *or* 4 *modulo* 5.
(4) $c \not\equiv 7$, 8 *or* 11 *modulo* 13.
(5) $c \not\equiv 4$, 5, 6, 9, 13, 22 *or* 28 *modulo* 29.

Proof. Clear. □

Corollary 6.6.4. *For all primes p such that $p \equiv 1 \pmod{1160}$ the curve $\mathcal{C}_{p^2}$ is everywhere locally soluble, but is not globally soluble, so is a counterexample to the Hasse principle.*

Proof. It is clear that the above conditions are satisfied modulo 16, 5, and 29, and also modulo 13 since 7, 8, and 11 are nonquadratic residues modulo 13. On the other hand we will prove below in Proposition 6.6.14 Fermat's classical result that the equation $x^4 + y^4 = Z^2$ does not have any nontrivial solutions, so this is in particular the case for our equation $x^4 + y^4 = (pz^2)^2$. □

Since by Dirichlet's theorem on primes in arithmetic progressions (Theorem 10.5.29) there exist infinitely many primes $p \equiv 1 \pmod{1160}$ this corollary gives infinitely many counterexamples to the Hasse principle.

6.6.2 Global Solubility: Factoring over Number Fields

Now that we know necessary and sufficient conditions for our equation to be everywhere locally soluble, we begin the study of *sufficient* conditions for our equation to have no global solutions, since is does not seem reasonable to hope for necessary and sufficient ones. We will give two types of conditions. The first uses classical techniques of algebraic number theory and the other uses the theory of elliptic curves. Thus, for an integer $c \geqslant 1$ we consider the equation

$$x^4 + y^4 = cz^4 \ .$$

Without loss of generality we may assume that c is not divisible by a nontrivial fourth power, hence we may also assume that x, y, and z are pairwise coprime. The cases $c = 1$ and $c = 2$ (which are in fact the easiest) are treated in Section 6.6.5 and Exercise 26, hence we will assume that $c \geqslant 3$, so that in particular $xyz \neq 0$. Finally, we assume that our equation is everywhere locally soluble (otherwise there is nothing more to be done), in other words that the conditions of Corollary 6.6.3 are satisfied.

Since x and y are coprime one of them at least is odd, so by exchanging x and y if necessary, we can assume that x is odd. If necessary by changing

the signs of x and y we may assume that $x \equiv 1 \pmod 4$, and that either y is even or $y \equiv 1 \pmod 4$. In addition since $c \equiv 1$ or 2 modulo 16 it follows that z is necessarily odd.

In this section, to study our equation we will *factor* it over the natural number field which occurs, which is here the field $K = \mathbb{Q}(\zeta)$, where $\zeta = \zeta_8$ is a primitive 8th root of unity (whose minimal polynomial is $P(X) = X^4 + 1$). Luckily the ring of integers $\mathbb{Z}_K$ of K is as simple as can be desired: we have $\mathbb{Z}_K = \mathbb{Z}[\zeta]$, $\mathbb{Z}_K$ has class number 1, in other words is a principal ideal domain, and the group of units of $\mathbb{Z}_K$ is the group of elements of the form $\zeta^j \varepsilon^k$ with $0 \leqslant j \leqslant 7$, $k \in \mathbb{Z}$, and for instance $\varepsilon = 1 + \zeta - \zeta^3$, which is equal to $1 + \sqrt{2}$ if we choose $\zeta = (1 + i)/\sqrt{2}$ as primitive 8th root of unity. The prime 2 is totally ramified in K as $2\mathbb{Z}_K = \mathfrak{p}^4$, and we have $\mathfrak{p} = (1+\zeta)\mathbb{Z}_K$. It is also clear that $G = \mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \sigma_3, \sigma_5, \sigma_7\}$, is a Klein 4-group, where σ_j sends ζ to ζ^j.

All these facts are obtained immediately by using a CAS, but are also very easy to show directly. Finally, to simplify notation we will denote by $\mathcal{N}$ the absolute norm $\mathcal{N}_{K/Q}$ from K to $\mathbb{Q}$.

Definition 6.6.5. *Let $\gamma = A+B\zeta+C\zeta^2+D\zeta^3 \in \mathbb{Z}[\zeta]$ be such that $v_\mathfrak{p}(\gamma) \leqslant 1$.*

(1) *If $v_\mathfrak{p}(\gamma) = 0$ we say that γ is* normalized *if*

$$A \equiv 1 \pmod 4,\ B \equiv 0 \pmod 2,\ C \equiv 0 \pmod 2,\ \textit{and}\ D \equiv 0 \pmod 4\ .$$

(2) *If $v_\mathfrak{p}(\gamma) = 1$ we say that γ is normalized if*

$$A \equiv 1 \pmod 4,\ B \equiv 1 \pmod 4,\ C \equiv 0 \pmod 2,\ \textit{and}\ D \equiv 0 \pmod 4\ .$$

Lemma 6.6.6. *Let γ be such that $v_\mathfrak{p}(\gamma) \leqslant 1$.*

(1) *There exists a unit u of K such that $u\gamma$ is normalized, in other words there exists an associate of γ which is normalized.*
(2) *If γ and $u\gamma$ are both normalized, with u a unit, then u is equal to ε^{4k} for some $k \in \mathbb{Z}$.*

Proof. (1). Assume first that $v_\mathfrak{p}(\gamma) = 0$. Multiplication by ζ maps the coefficients (A, B, C, D) of γ to $(-D, A, B, C)$, in other words is a circular permutation up to sign changes. Since γ is coprime to 2 we have $A + B + C + D \equiv 1 \pmod 2$, hence either a single coefficient is odd or a single one is even, so that with a suitable circular permutation we may put the single odd coefficient as the constant coefficient, or the single even coefficient as the coefficient of ζ^2. It follows that there is an associate of γ such that A is odd and C even, and then necessarily $B \equiv D \pmod 2$.

Now multiplication by the unit $\zeta\varepsilon$ is easily seen to change (A, B, C, D) into $(A+B-D, A+B+C, B+C+D, -A+C+D)$. This transformation preserves the fact that A is odd, C even, and $B \equiv D \pmod 2$, but changes the parity of B and D. Therefore we may assume that B, C, and D are all even, and

changing γ into $-\gamma$ that $A \equiv 1 \pmod 4$. These congruences being satisfied we check that multiplication by $-\zeta^2\varepsilon^2$ preserves all the congruences, and changes (A,B,C,D) into (A',B',C',D') with $(A',B',C',D') \equiv (A,B+2,C,D+2) \pmod 4$, so that we may assume that $D \equiv 0 \pmod 4$, hence the result is normalized.

Assume now that $v_{\mathfrak{p}}(\gamma) = 1$ and set $\gamma_1 = \gamma/(1+\zeta) = A_1 + B_1\zeta + C_1\zeta^2 + D_1\zeta^3 \in \mathbb{Z}_K$, so that $v_{\mathfrak{p}}(\gamma_1) = 0$. By the first part of the proof there exists an associate of γ_1 which is normalized. Since $A = A_1 - D_1$, $B = A_1 + B_1$, $C = B_1 + C_1$, and $D = C_1 + D_1$, we deduce that $A \equiv 1 \pmod 4$, $B \equiv 1 \pmod 2$, and $C \equiv D \equiv 0 \pmod 2$. Multiplication by ε^2 preserves these congruences and changes (C,D) into $(2B+3C+2D, -2A+2C+3D) \equiv (C+2, D+2) \pmod 4$, so that we may assume that $D \equiv 0 \pmod 4$. If $B \equiv 1 \pmod 4$ then γ is already normalized. Thus assume that $B \equiv 3 \pmod 4$. When $C \equiv 0 \pmod 4$, multiplication by $\zeta^2\varepsilon$ preserves existing congruences and leads to $B \equiv 1 \pmod 4$. When $C \equiv 2 \pmod 4$, the same is true with $\zeta^6\varepsilon^3$ instead of $\zeta^2\varepsilon$, thus proving the existence of a normalized associate of γ in all cases.

(2). If $v_{\mathfrak{p}}(\gamma) = 0$ and γ and $u\gamma$ are normalized, then $u \equiv 1 \pmod{2\mathbb{Z}[\zeta]}$. An immediate computation among units of the form $\zeta^j\varepsilon^k$ for $0 \leqslant j \leqslant 7$ and $0 \leqslant k \leqslant 3$ shows that the only such units up to powers of ε^{4k} are ± 1 and $\pm\varepsilon^2$, and it is immediate that the only one of these which respects the additional congruences modulo 4 is $u = 1$. Since $\varepsilon^4 \equiv 1 \pmod{4\mathbb{Z}[\zeta]}$ the result follows in this case. If $v_{\mathfrak{p}}(\gamma) = 1$ and $C \equiv 0 \pmod 4$, we must now have $u\gamma \equiv \gamma \pmod 4$ (since it is easily checked that the coefficient of ζ^3 of $u\gamma$ is congruent to C modulo 4), hence $u \equiv 1 \pmod{4/\mathfrak{p}}$, and this implies as above that u is a power of ε^4. Finally if $v_{\mathfrak{p}}(\gamma) = 1$ and $C \equiv 2 \pmod 4$, we have 8 units $u \equiv 1 \pmod{2/\mathfrak{p}}$ of the form $\zeta^j\varepsilon^k$ for $0 \leqslant j \leqslant 7$, and it is immediate that the congruences modulo 4 imply $u = 1$, proving the lemma. □

Definition 6.6.7. *Let p be a prime number such that $p \equiv 1 \pmod 8$. For each of the four values of $r \in \mathbb{F}_p$ such that $r^4 = -1$ we denote by $\phi_{p,r}$ the ring homomorphism from $\mathbb{Z}[\zeta]$ to $\mathbb{F}_p$ which sends 1 to 1 and ζ to r.*

Note that it is clear that $\phi_{p,r}$ is well defined, and since $8 \mid (p-1)$ that there exist 8 distinct 8th roots of unity in $\mathbb{F}_p$, of which 4 are such that $r^4 = -1$.

The main result that we are going to prove is the following, due in essence to Bremner and Morton [Bre-Mor].

Proposition 6.6.8. *Let $c \geqslant 3$ not divisible by a nontrivial fourth power. A* necessary *condition for the global solubility in $\mathbb{Q}$ of $x^4 + y^4 = cz^4$ is the existence of a* normalized *divisor γ of c in $\mathbb{Z}[\zeta]$ of the form $\gamma = A + B\zeta + C\zeta^2 + D\zeta^3$ satisfying the following properties.*

(1) *There exists $\alpha \in \mathbb{Z}[\zeta]$ such that $x + y\zeta = \gamma\alpha^4$.*
(2) *We have $v_{\mathfrak{p}}(\gamma) = 0$ when $c \equiv 1 \pmod{16}$ and $v_{\mathfrak{p}}(\gamma) = 1$ when $c \equiv 2 \pmod{16}$.*

(3) *When* $c \equiv 1 \pmod{16}$ *the conjugates of* γ *are pairwise coprime, and when* $c \equiv 2 \pmod{16}$ *the conjugates of* $\gamma/(1+\zeta)$ *are pairwise coprime.*
(4) *We have* $\mathcal{N}(\gamma) = c$.
(5) *The coefficients of* γ *satisfy the congruences*

$$\begin{aligned} C &\equiv D \equiv 0 \pmod 4 \\ AC &\equiv BD \pmod 8 \\ C(A+C) &\equiv D(B-D) \pmod 3 . \end{aligned}$$

(6) *For each odd prime number* p *dividing* c *(hence such that* $p \equiv 1 \pmod 8$*), there exists a unique fourth root* r *of* -1 *in* $\mathbb{F}_p$ *such that* $\phi_{p,r}(\gamma) = 0$. *Then both*

$$\frac{1-r^2}{2}\frac{\phi_{p,r}(\sigma_5(\gamma))}{\phi_{p,r}(\sigma_3(\gamma))} \quad \textit{and} \quad \frac{1+r^2}{2}\frac{\phi_{p,r}(\sigma_5(\gamma))}{\phi_{p,r}(\sigma_7(\gamma))}$$

are fourth powers in $\mathbb{F}_p^*$.

Proof. (1) and (2). Factoring our equation in $\mathbb{Z}_K$ gives

$$x^4 + y^4 = (x+\zeta y)(x+\zeta^3 y)(x+\zeta^5 y)(x+\zeta^7 y) = cz^4 .$$

Assume that π is a prime element such that $\pi \mid \gcd(x+\zeta^m y, x+\zeta^n y)$ for two distinct odd exponents m and n such that $1 \leqslant m, n \leqslant 7$. Then $\pi \mid (\zeta^m - \zeta^n)y$ and $\pi \mid \zeta^m(x+\zeta^n y) - \zeta^n(x+\zeta^m y) = (\zeta^m - \zeta^n)x$, hence $\pi \mid (\zeta^m - \zeta^n)$ since x and y are coprime. Since the norm of $\zeta^m - \zeta^n$ is a power of 2, it follows that π is a prime dividing 2, in other words (up to multiplication by a unit) $\pi = 1+\zeta$. From our factored equality and the fact that z is odd, we deduce that when $c \equiv 1 \pmod{16}$ the four factors on the left are pairwise coprime, and when $c \equiv 2 \pmod{16}$ (hence with x and y odd) the factors divided by $1+\zeta$ are (algebraic integers and) also pairwise coprime. Assume for instance that $c \equiv 1 \pmod{16}$ and set $\gamma = \gcd(x+\zeta y, c)$, defined for the moment only up to multiplication by a unit. Since $(x+\zeta y)/\gamma$ is coprime to the other three factors and to c/γ, it follows that it must be a fourth power of an ideal in $\mathbb{Z}_K$. Since $\mathbb{Z}_K$ is a principal ideal domain, this means that there exists α and γ (equal to a unit multiple of the initially chosen one) in $\mathbb{Z}_K$, coprime to 2, and such that $x+\zeta y = \gamma\alpha^4$. Since we may change simultaneously γ into γv^4 and α into α/v for any unit v, we note for future reference that if some γ is fixed, it is only necessary to consider associates of γ modulo fourth powers of units. Similarly, if $c \equiv 2 \pmod{16}$ we deduce that $x+\zeta y = \gamma\alpha^4$, where α is coprime to 2 and $v_{\mathfrak{p}}(\gamma) = 1$, proving (1) and (2).

(3) and (4). We take the norm down to $\mathbb{Q}$ of the relation obtained in (1). Setting $m = \mathcal{N}(\alpha)$ we thus obtain $cz^4 = x^4 + y^4 = \mathcal{N}(\gamma)m^4$, hence $m^4 \mid cz^4$, and since c is not divisible by a fourth power we have $m \mid z$, so that $\mathcal{N}(\gamma) = c(z/m)^4$, hence $c \mid \mathcal{N}(\gamma)$. Conversely, we have $\gamma \mid x+\zeta y$, hence for any $\sigma \in G = \mathrm{Gal}(K/\mathbb{Q})$ we have $\sigma(\gamma) \mid x+\sigma(\zeta)y$. When $c \equiv 1 \pmod{16}$ the numbers $x+\sigma(\zeta)y$ are pairwise coprime, hence the conjugates $\sigma(\gamma)$ are

pairwise coprime. Since $\sigma(\gamma) \mid \sigma(c) = c$ it follows that $\mathcal{N}(\gamma) = \prod_{\sigma \in G} \sigma(\gamma) \mid c$, and combining this with $c \mid \mathcal{N}(\gamma)$ we deduce that $c = \mathcal{N}(\gamma)$. When $c \equiv 2 \pmod{16}$ the same reasoning shows that the $\sigma(\gamma/(1+\zeta))$ are pairwise coprime hence that $\mathcal{N}(\gamma)/2 \mid c/2$ and we conclude in the same way, proving (3) and (4).

(5). Possibly after changing γ into $-\gamma$, we may multiply α by any power of ζ without changing (1). If we write $\alpha = a + b\zeta + c\zeta^2 + d\zeta^3$, the condition α coprime to 2 means that $a+b+c+d \equiv 1 \pmod 2$, in other words either one or three of the coefficients are odd, and the others are even. Since multiplication by ζ sends (a, b, c, d) to $(-d, a, b, c)$, in other words is a circular permutation up to changes of sign, it is clear that we may assume that a is odd and c even, and then $b \equiv d \pmod 2$.

Write $\alpha^4 = U + V\zeta + W\zeta^2 + X\zeta^3$. An easy calculation shows that

$$U \equiv 1 \pmod 8, \quad V \equiv X \equiv 4b \pmod 8, \quad \text{and} \quad W \equiv 0 \pmod 8 .$$

On the other hand since $\gamma = A + B\zeta + C\zeta^2 + D\zeta^3$ we have

$$\begin{aligned} x + \zeta y = \gamma\alpha^4 &= (AU - BX - CW - DV) + (AV + BU - CX - DW)\zeta \\ &\quad + (AW + BV + CU - DX)\zeta^2 + (AX + BW + CV + DU)\zeta^3 . \end{aligned}$$

It follows in particular that $AW + BV + CU - DX = 0$ and $AX + BW + CV + DU = 0$. Since V, W, and X are divisible by 4 and U is odd, we already deduce that $4 \mid C$ and $4 \mid D$. Also, since we have chosen $x \equiv 1 \pmod 4$ we have $1 \equiv x \equiv AU - BX - CW - DV \equiv A \pmod 4$. If $c \equiv 1 \pmod{16}$ we must have $B \equiv 0 \pmod 2$, hence γ is normalized. If $c \equiv 2 \pmod{16}$ then since we have chosen $y \equiv 1 \pmod 4$ we have $1 \equiv y \equiv AV + BU - CX - DW \equiv B \pmod 4$, hence γ is normalized also in this case.

Working now modulo 8, we deduce from the same two equations above that $4bB + C - 4bD \equiv 4bA + 4bC + D \equiv 0 \pmod 8$, and since $4 \mid C$ and $4 \mid D$, we have $C \equiv 4bB \pmod 8$ and $D \equiv 4bA \pmod 8$, from which we evidently obtain $AC \equiv BD \pmod 8$. For the result modulo 3, another easy calculation using the trivial relations $x^3 \equiv x \pmod 3$ and $xy(x^2 - y^2) \equiv 0 \pmod 3$ shows that $U \equiv a^2 - b^2 + c^2 - d^2 \pmod 3$, $V \equiv X \equiv ab - bc + cd + da \pmod 3$, and $W \equiv 0 \pmod 3$. The equalities obtained above thus imply that

$$(B - D)V + CU \equiv 0 \pmod 3 \quad \text{and} \quad (A + C)V + DU \equiv 0 \pmod 3 ,$$

hence that

$$(D(B - D) - C(A + C))V \equiv (D(B - D) - C(A + C))U \equiv 0 \pmod 3 .$$

Now we cannot have $U \equiv V \equiv 0 \pmod 3$. Indeed, otherwise

$$(a + b + d)^2 + (c - b + d)^2 \equiv (a - b - d)^2 + (c + b - d)^2 \equiv 0 \pmod 3$$

by the congruences obtained above, and since a sum of two squares is divisible by 3 if and only if both are, we would have $a + b + d \equiv c - b + d \equiv a - b - d \equiv$

$c+b-d \equiv 0 \pmod 3$, hence $3 \mid \gcd(a,b,c,d)$, so $3 \mid \gcd(x,y)$ in contradiction with our assumption, proving the congruence modulo 3 of the proposition.

(6). Let $r \in \mathbb{F}_p$ be such that $r^4 = -1$. The four roots of this equation are r^j for $1 \leqslant j \leqslant 7$, j odd, and it is clear that $\phi_{p,r}(\sigma_j(\gamma)) = \phi_{p,r^j}(\gamma)$. It follows that

$$\prod_{1 \leqslant j \leqslant 7,\ j \text{ odd}} \phi_{p,r^j}(\gamma) = \phi_{p,r}(\mathcal{N}(\gamma)) \ .$$

Since $\mathcal{N}(\gamma) = c$ and $p \mid c$ we have $\phi_{p,r}(\mathcal{N}(\gamma)) = 0$, hence there exists j such that $\phi_{p,r^j}(\gamma) = 0$, proving the existence of r such that $\phi_{p,r}(\gamma) = 0$.

From the equation $x + \zeta y = \gamma\alpha^4$ we deduce by application of the σ_j that $x + \zeta^j y = \sigma_j(\gamma)\sigma_j(\alpha)^4$ for j odd, hence by application of the homomorphism $\phi_{p,r}$ we deduce that there exists f_3, f_5, and f_7 such that in $\mathbb{F}_p$ we have $x + ry = 0$ and

$$x + r^3 y = \phi_{p,r}(\sigma_3(\gamma))f_3^4, \ x + r^5 y = \phi_{p,r}(\sigma_5(\gamma))f_5^4, \ x + r^7 y = \phi_{p,r}(\sigma_7(\gamma))f_7^4 \ .$$

From the first equation we deduce that $x = -ry$, so replacing and using $r^4 = -1$ we obtain

$$(r^3 - r)y = \phi_{p,r}(\sigma_3(\gamma))f_3^4, \ -2ry = \phi_{p,r}(\sigma_5(\gamma))f_5^4, \ -(r^3 + r)y = \phi_{p,r}(\sigma_7(\gamma))f_7^4 \ .$$

Since $r^3 - r \neq 0$, $2r \neq 0$, and $r^3 + r \neq 0$, this shows in particular that $\phi_{p,r}(\sigma_j(\gamma)) \neq 0$ for $j \neq 1$, since otherwise $y \equiv 0 \pmod p$, hence $x \equiv 0 \pmod p$, contradicting the assumption that x and y are coprime, proving the uniqueness of r since $\phi_{p,r}(\sigma_j(\gamma)) = \phi_{p,r^j}(\gamma)$. Finally, by dividing the second relation by the first and the third respectively we obtain the conditions given in (6). □

Remarks.

(1) A short computation shows that if $c \equiv 1 \pmod{16}$ and γ is normalized then $\mathcal{N}(\gamma) \equiv 1 + 2C^2 \pmod{16}$, and since $\mathcal{N}(\gamma) = c$ it follows that in this case the condition $C \equiv D \equiv 0 \pmod 4$ is automatic as soon as γ is normalized.

(2) Once γ is known to be normalized it is clear that the congruence modulo 8 is equivalent to $C \equiv 0 \pmod 8$ when $c \equiv 1 \pmod{16}$, and to $C \equiv D \pmod 8$ when $c \equiv 2 \pmod{16}$.

Lemma 6.6.9. *Let $c \equiv 1 \pmod{16}$ (resp., $c \equiv 2 \pmod{16}$). An element γ is normalized and satisfies conditions* (1) *to* (6) *of Proposition 6.6.8 if and only if $\sigma_5(\gamma)$ (resp., $\zeta\sigma_7(\gamma)$) does.*

Proof. Since $\sigma_5(A + B\zeta + C\zeta^2 + D\zeta^3) = A - B\zeta + C\zeta^2 - D\zeta^3$ and $\zeta\sigma_7(A + B\zeta + C\zeta^2 + D\zeta^3) = B + A\zeta - D\zeta^2 - C\zeta^3$, the lemma is clear. □

Corollary 6.6.10. *Assume that the equation $x^4 + y^4 = cz^4$ is everywhere locally soluble, in other words that c satisfies the conditions of Corollary 6.6.3. Let $\mathcal{F}$ be a set of representatives of normalized divisors γ of c coprime to their conjugates and such that $\mathcal{N}(\gamma) = c$, modulo multiplication by powers of ε^4, and modulo the action of σ_5 when $c \equiv 1 \pmod{16}$ and the action of $\zeta\sigma_7$ when $c \equiv 2 \pmod{16}$. If for every $\gamma \in \mathcal{F}$ one of the conditions (5) or (6) of Proposition 6.6.8 is not satisfied then the equation $x^4 + y^4 = cz^4$ has no nontrivial global solution. Furthermore, if c is not a square or twice a square we have $|\mathcal{F}| = 2^{2k-1}$, where k is the number of distinct prime factors of c congruent to 1 modulo 8.*

Proof. Indeed, it is clear that multiplication of γ by a power of ε^4 does not change the conditions in (6). Furthermore it is immediate to check that multiplication by ε^4 does not change $AC - BD \bmod 8$ or $C(A+C) - D(B-D) \bmod 3$, so that it is enough to consider γ up to powers of ε^4 (we have already mentioned this fact in the proof of (4)), and by the preceding lemma up to the action of σ_5 or $\zeta\sigma_7$. Finally, it is clear from the uniqueness of the normalization up to powers of ε^4 that the number of normalized γ coprime to their conjugates and such that $\mathcal{N}(\gamma) = c$ is equal to 4^k, since every prime congruent to 1 modulo 8 splits completely into 4 factors (since γ is coprime to its conjugates we cannot mix different factors above the same prime even when c is not squarefree). Now we check that if $c \equiv 1 \pmod{16}$ and $\sigma_5(\gamma) = \gamma$ then $c = \mathcal{N}(\gamma) = (A^2 + C^2)^2$, and if $c \equiv 2 \pmod{16}$ and $\zeta\sigma_7(\gamma) = \gamma$ then $c = \mathcal{N}(\gamma) = 2(A^2 - 2AC - C^2)^2$, so that when c is not a square or twice a square we have $|\mathcal{F}| = 2^{2k-1}$. □

Note that if c is a square our equation has no global solutions by Proposition 6.6.14, and if c is twice a square it has no solutions for $c > 2$ by Exercise 26.

Remark. The conditions of Proposition 6.6.8 are all useful. For instance, to exclude $c = 4801$ the condition modulo 8 is the only one which applies. To exclude $c = 5266$ the condition modulo 3 is the only one which applies. To exclude $c = 5281$ we need the condition on fourth powers for one of the values of γ. In many examples we can use only one of the two conditions on fourth powers, in others we can use both. We will give a summary of results in a table below.

6.6.3 Global Solubility: Coverings of Elliptic Curves

Although Corollary 6.6.10 is very powerful in proving that a Fermat quartic has no global solution, it is not the whole story. For instance as will be clear from the table given below, of the 107 suitable values of c such that $3 \leqslant c \leqslant 10000$, 99 can be treated using this corollary, leaving 8 indeterminate cases. Another natural (and in fact easier) approach is to use maps from the curve $\mathcal{C}_c$ with affine equation $x^4 + y^4 = c$ to two elliptic curves, and then to

use results on elliptic curves to conclude. This will enable us to solve 5 of the remaining 8 cases with $c \leqslant 10000$.

Let c be as above, and consider the two elliptic curves with affine Weierstrass equations

$$E_c : Y^2 = X^3 - cX \quad \text{and} \quad F_c : Y^2 = X^3 + c^2X \ .$$

It is immediate to check that the maps ϕ and ψ defined in affine coordinates by

$$\phi((x,y)) = (-x^2, xy^2) \quad \text{and} \quad \psi((x,y)) = (cx^2/y^2, c^2x/y^3)$$

are maps from $\mathcal{C}_c$ to E_c and F_c respectively. Since all rational points of $\mathcal{C}_c$ are affine, it is clear that if $P \in \mathcal{C}_c(\mathbb{Q})$ then $\phi(P) \in E_c(\mathbb{Q})$ and $\psi(P) \in F_c(\mathbb{Q})$. In particular, since the inverse image of a point by ϕ or ψ is finite, if *either* $E_c(\mathbb{Q})$ or $F_c(\mathbb{Q})$ is an explicit finite set, it will be immediate to determine $\mathcal{C}_c(\mathbb{Q})$. We will see in Chapter 8 that this means that $E_c(\mathbb{Q})$ or $F_c(\mathbb{Q})$ has rank 0, hence equal to its easily determined torsion subgroup. Thus in this favorable case it is very easy to determine $\mathcal{C}_c(\mathbb{Q})$:

Proposition 6.6.11. *Let $c \geqslant 3$ be an integer not divisible by a nontrivial fourth power. If either $E_c(\mathbb{Q})$ or $F_c(\mathbb{Q})$ has rank 0 then $\mathcal{C}_c(\mathbb{Q}) = \emptyset$.*

Proof. Note first that the trivial 2-torsion point $(X,Y) = (0,0)$ on E_c corresponds to $x = 0$ on $\mathcal{C}_c$, hence to $c = y^4$, which is absurd by assumption. We now use Proposition 8.1.14 that we will prove in Chapter 8. It tells us that there can be other torsion points only if c (for E_c) or $-c^2$ (for F_c) is equal to m^2 or to $-4m^4$. Consider first E_c. Since $c > 0$ (and also because it is not divisible by a fourth power) we cannot have $c = -4m^4$. On the other hand $c = m^2$ is a priori possible, and gives as affine torsion points the ones with $Y = 0$. But this implies that either x or y is equal to 0, which is impossible, proving the result for E_c. Consider now F_c. We cannot have $-c^2 = m^2$, so the only possibility is $c = 2m^2$, and the extra torsion points are clearly $(X,Y) = (2m^2, \pm 4m^3)$. The inverse images (x,y) of these points by the map ψ are easily seen to be such that $y = \pm x$ and $y^3 = \pm x$, and since $x \neq 0$ this gives $m = \pm x^2$. Thus x is an integer and $c = 2m^2 = 2x^4$, which implies that $c = 2$ since c is assumed not to be divisible by a fourth power, and this is excluded since we have assumed that $c \geqslant 3$. □

Examples. We first choose $c = 562$, for which $\mathcal{C}_c$ is locally soluble by Corollary 6.6.3. The 2-descent method that we will study in Section 8.2 or Cremona's `mwrank` program shows that $E_c(\mathbb{Q})$ has rank 1, but that $F_c(\mathbb{Q})$ has rank 0, so that $\mathcal{C}_{562}(\mathbb{Q}) = \emptyset$.

Choose now $c = 226$ or $c = 977$. The 2-descent methods and `mwrank` only tell us that the rank of $F_c(\mathbb{Q})$ is equal to 0 or 2. However, the computation of $L(F_c, 1)$ (see Section 8.5) shows that in both cases we have $L(F_c, 1) \neq 0$, hence since the BSD conjecture is a theorem in this case (in fact here due to

Coates–Wiles [Coa-Wil] since F_c has complex multiplication), this proves that the rank of $F_c(\mathbb{Q})$ is equal to 0, and once again this implies that $\mathcal{C}_c(\mathbb{Q}) = \emptyset$.

It is important to note that we have the following stronger result due to Dem'janenko (see [Dem3]). See Section 13.3.1 for an indication on the method of proof.

Theorem 6.6.12 (Dem'janenko). *If $c \geqslant 3$ is an integer not divisible by a nontrivial fourth power and if the rank of $E_c(\mathbb{Q})$ is at most equal to 1 then $\mathcal{C}_c(\mathbb{Q}) = \emptyset$.*

This theorem sometimes allows us to show that the Fermat quartic is not globally soluble, even when both $E_c(\mathbb{Q})$ and $F_c(\mathbb{Q})$ have nonzero rank. For instance if $c = 2642$, for which $\mathcal{C}_c$ is again everywhere locally soluble, it can be shown that $E_c(\mathbb{Q})$ has rank 1 and $F_c(\mathbb{Q})$ has rank 2, so that thanks to Dem'janenko's theorem we can conclude that $\mathcal{C}_c(\mathbb{Q}) = \emptyset$, which we would not have been able to do using only the rank 0 conditions.

Remarks.

(1) It is easy to compute that the *root number* (see Theorem 8.1.4) of E_c is equal to 1 when $c \equiv 1 \pmod{16}$, to -1 when $c \equiv 2 \pmod{16}$, and that of F_c is always equal to 1. Thus, it follows from a weak form of the BSD conjecture that F_c will always have even rank, and E_c will have even or odd rank according to whether c is odd or even. This shows in particular that Dem'janenko's theorem is absolutely necessary to deal with the case $c \equiv 2 \pmod{16}$.

(2) The existence of the maps ϕ and ψ, together with the map $\overline{\phi}$ from $\mathcal{C}_c$ to E_c defined by $\overline{\phi}((x,y)) = (-y^2, yx^2)$ means that the Jacobian of $\mathcal{C}_c$ is isogenous to $E_c \times E_c \times F_c$, the map $(\phi, \overline{\phi}, \psi)$ giving the embedding of $\mathcal{C}_c$ into its Jacobian (see Section 13.2 for these notions). The proof of Dem'janenko's theorem amounts to showing that if $(x,y) \in \mathcal{C}_c(\mathbb{Q})$ the two points $\phi((x,y))$ and $\overline{\phi}((x,y))$ in E_c are generically independent, so that E_c must have rank at least equal to 2.

6.6.4 Conclusion, and a Small Table

When there does exist solutions to our Fermat quartic, for instance when $c = 1$, 2, or 17, we can ask for *all* the solutions (since a Fermat quartic is a curve of genus 3, we know by Faltings's theorem that there are only finitely many). For $c = 1$, Fermat's theorem for $n = 4$ (which follows from Proposition 6.6.14 below) tells us that the points $(\pm 1, 0)$ and $(0, \pm 1)$ are the only rational points on the curve $x^4 + y^4 = 1$. By a similar method of descent, for $c = 2$ it is easy to show that the points $(\pm 1, \pm 1)$ are the only rational points on the curve $x^4 + y^4 = 2$ (Exercise 26). On the other hand it is much more difficult to prove that for $c = 17$ the only rational points on $x^4 + y^4 = 17$ are $(\pm 1, \pm 2)$ and $(\pm 2, \pm 1)$. This problem was posed by J.-P. Serre as the

simplest nontrivial case of the Fermat quartic equations, and also because it was known that the standard methods using Chabauty type techniques failed on this curve. It was only solved in 1999 by Flynn and Wetherell using covering techniques, and their proof is not easy (see also Section 13.3.4).

A table up to 10000**.** The following table gives numerical data obtained using all of the preceding results. It first lists the 109 values of $c \geqslant 1$ not divisible by a nontrivial fourth power for which the equation $x^4 + y^4 = c$ is everywhere locally soluble, together with $c = 0$. Below each such value of c is either a pair (x, y) of rational numbers such that $x^4 + y^4 = c$, or a code made with one or more letters. The letter A (for Algebraic) means that we can prove the nonexistence of global solutions using Corollary 6.6.10. The letter D means that $E_c(\mathbb{Q})$ has rank 1 so that Dem'janenko's Theorem 6.6.12 is applicable (this can occur only for c even, see above), E means that $E_c(\mathbb{Q})$ has rank 0 (this can occur only for c odd), and F means that $F_c(\mathbb{Q})$ has rank 0, so that in both of these cases Proposition 6.6.11 is applicable. Thus if at least one of these letters occur this implies that $\mathcal{C}_c(\mathbb{Q}) = \emptyset$. Finally, the letter U (for undetermined), which occurs three times, means that the results given above, together with a computer search, do not allow us to conclude. We refer to [Bre-Mor] for still other methods which can prove nonglobal solubility of our equation in other cases, in particular for the first undetermined case $c = 4481$.

0	1	2	17	82	97	146	226	257	337
(0,0)	(0,1)	(1,1)	(1,2)	(1,3)	(2,3)	ADF	AF	(1,4)	(3,4)
482	562	577	626	641	706	802	881	977	1042
ADF	ADF	A	(1,5)	(2,5)	(3,5)	ADF	(4,5)	AF	AF
1186	1201	1297	1361	1522	1777	1921	2017	2066	2161
DF	AF	(1,6)	AEF	A	A	(5,6)	AF	ADF	EF
2306	2402	2417	2482	2642	2657	2722	2801	2866	3026
ADF	(1,7)	(2,7)	(3,7)	AD	(4,7)	ADF	A	ADF	(5,7)
3041	3106	3121	3202	3217	3442	3506	3617	3697	3761
AF	AF	AE	DF	AF	ADF	ADF	AF	(6,7)	AF
3826	4097	4162	4177	4226	4241	4306	4322	4481	4657
ADF	(1,8)	ADF	(3,8)	AD	AF	ADF	ADF	U	AEF
4721	4786	4801	4946	5186	5266	5281	5297	5426	5521
(5,8)	ADF	AF	ADF	AF	ADF	AE	AF	AF	AF
5617	5906	5986	6242	6337	6497	6562	6577	6626	6722
A	$*$	AF	AF	AF	(7,8)	(1,9)	(2,9)	ADF	ADF
6817	6961	6977	7121	7186	7297	7361	7537	7666	7762
(4,9)	AF	EF	AF	(5,9)	AEF	A	U	ADF	D
7841	8161	8306	8402	8482	8546	8737	8882	8962	9026
AEF	AF	ADF	ADF	ADF	AF	AE	U	(7,9)	AF
9122	9266	9281	9346	9377	9442	9586	9697	9857	9986
ADF	A	A	ADF	AEF	ADF	A	AF	AE	ADF

Sums of Two Rational Fourth Powers up to 10000

In the above table, $*$ means $(25/17, 149/17)$. Evidently all the values of c for which any of the letters A, D, E, or F occur are counterexamples to the Hasse principle. It can be seen from this table that the purely algebraic method using the factorization of our equation is much more powerful than the method using elliptic curves, although the latter is necessary in five cases of the above table (and the curve F_c is always sufficient in these cases). If we push the computation to 10^5, there are 831 suitable values of $c \geqslant 3$ for which the equation is everywhere locally soluble, 91 for which we find a global solution, 691 can be shown to have no global solutions by the algebraic method, and of the 49 remaining ones 33 can be shown to have no global solutions using elliptic curves, leaving 16 undetermined cases.

An amusing corollary of the above table is the following result, due to Bremner and Morton [Bre-Mor]:

Corollary 6.6.13. *The integer $c = 5906$ is the smallest integer which is the sum of two fourth powers of rational numbers, and not the sum of two fourth powers of integers.*

Proof. Indeed, for all smaller values of c except $c = 4481$ we see that either the equation $x^4 + y^4 = c$ has no *rational* solutions, or it has an integral solution. It is an immediate verification that 5906 is not a sum of two fourth powers of integers, and it is the sum of the two fourth powers of rational numbers given above. There remains to prove that $x^4 + y^4 = 4481z^4$ is not globally soluble, and this is done using the more general factoring methods explained in [Bre-Mor]. □

6.6.5 The Equations $x^4 \pm y^4 = z^2$ and $x^4 \pm 2y^4 = z^2$

The equation $x^4 + y^4 = z^2$ was solved by Fermat by using the method of infinite descent, similar but simpler than the one we used in Theorem 6.4.5. The proof is also based on the parametric solution of a simpler equation, here of the Pythagorean equation $x^2 + y^2 = z^2$ which we have given in Corollary 6.3.13.

Proposition 6.6.14. *Let $\varepsilon = \pm 1$. The Diophantine equation $x^4 + \varepsilon y^4 = z^2$ has no solutions with $xyz \neq 0$.*

Proof. Once again we may assume that x, y and z are pairwise coprime. Assume first that z is even. This can happen only if $\varepsilon = -1$, otherwise we would get a contradiction modulo 8. Writing the equation as $y^4 + z^2 = x^4$ with y odd, by Corollary 6.3.13 we obtain $y^2 = s^2 - t^2$, $z = 2st$ and $x^2 = s^2 + t^2$ for some coprime s and t of opposite parity. It follows that $s^4 - t^4 = (xy)^2 = u^2$ with u odd, so we have reduced our equation to one where the right hand side is odd.

We may thus assume that z is odd. If $\varepsilon = 1$ we exchange x and y if necessary so that x is odd and y is even, while if $\varepsilon = -1$, reasoning modulo 4 we see that these conditions are automatic. By Corollary 6.3.13 there exist coprime s and t of opposite parity such that $x^2 = s^2 - \varepsilon t^2$, $y^2 = 2st$ and $z = \pm(s^2 + \varepsilon t^2)$ (the sign of x^2 for $\varepsilon = -1$ can be removed since $x^2 \geqslant 0$). Since $st \geqslant 0$, changing if necessary (s, t) into $(-s, -t)$ we may assume that $s \geqslant 0$ and $t \geqslant 0$. Exchanging if necessary s and t if $\varepsilon = -1$, we may assume that s is odd and t is even, this being automatic if $\varepsilon = 1$. Using once again Corollary 6.3.13 on the equation $x^2 = s^2 - \varepsilon t^2$, we deduce the existence of coprime u and v of opposite parity such that $x = \pm(u^2 - \varepsilon v^2)$, $s = \pm(u^2 + \varepsilon v^2)$ and $t = 2uv$, and since $t \geqslant 0$ we may assume $u \geqslant 0$ and $v \geqslant 0$. The last remaining equation to be solved is therefore $(y/2)^2 = \pm uv(u^2 + \varepsilon v^2)$, where the $\pm$ sign must be $+$ if $\varepsilon = 1$, and can be removed by exchanging u and v otherwise. Since $\gcd(u, v) = 1$ the three factors on the right are clearly pairwise coprime and are nonnegative, hence each one is a square. Thus, if $u = u_1^2$, $v = v_1^2$ and $u^2 + \varepsilon v^2 = w^2$ we have $u_1^4 + \varepsilon v_1^4 = w^2$. This is exactly our initial equation with new values of the variables. However, following through the reductions it is immediate that $|w| < |z|$ when $z \neq 0$. Thus, if we start with a solution with the smallest nonzero value of $|z|$ we obtain a strictly smaller one, a contradiction which shows that there cannot be any such solution. □

Proposition 6.6.15. *The Diophantine equations* $x^4 \pm 2y^4 = z^2$ *have no solution with* $y \neq 0$.

Proof. Set $p = \pm 2$ and let (x, y, z) be integers such that $x^4 + py^4 = z^2$, where we may assume that x, y and z are pairwise coprime. By Corollary 6.3.14 there exist coprime integers s and t with s odd such that $x^2 = \pm(s^2 - pt^2)$ and $y^2 = 2st$. It follows that $s = \pm u^2$ and $t = \pm 2v^2$, hence $x^2 = \pm(u^4 - 4pv^4)$, and u is odd and coprime to v. If the sign was $-$, we would have $x^2 + u^4 = 4pv^4$, which already implies that $p = +2$, and since u and x are odd $x^2 + u^4 \equiv 2 \pmod 8$, a contradiction. Thus the sign is $+$, so that $x^2 + 4pv^4 = u^4$, hence again by Corollary 6.3.14 there exist coprime a and b such that $2v^2 = 2ab$ and $u^2 = a^2 + pb^2$. It follows that $a = \pm c^2$, $b = \pm d^2$ so that $c^4 + pd^4 = u^2$, which is our initial Diophantine equation, and we conclude by the usual descent argument since clearly $|u| < |z|$. □

6.7 The Equation $y^2 = x^n + t$

For general results on this equation, we refer to [Cohn1] and [Cohn2], from which a large part of this section is taken.

In this section, we look for *integral* solutions to the equation $y^2 = x^n + t$, where t and n are given integers with $n \geqslant 3$ (otherwise the equation is trivial). If n is even this equation factors as $(y - x^{n/2})(y + x^{n/2}) = t$ which is trivially solved: if $t < 0$ (which will be the main case that we will consider), we may assume that $x > 0$, hence we let $d = x^{n/2} - y$, which will be a positive divisor of $|t|$ less than or equal to $|t|^{1/2}$, and the condition to be satisfied is that $(d + |t|/d)/2 = x^{n/2}$ must be an exact $n/2$th power with $n/2 \geqslant 2$. From this, a short calculation shows the following, which we give for future reference:

Proposition 6.7.1. *Let* $n \geqslant 4$ *be even and let* t *be a squarefree negative integer not congruent to* 1 *modulo* 8. *The only values of* n *and* t *with* $n \geqslant 4$ *even and* $-100 < t \leqslant -1$ *squarefree and not congruent to* 1 *modulo* 8 *for which the Diophantine equation* $y^2 = x^n + t$ *has solutions are for* $t = -1$ *with solutions* $(x, y) = (\pm 1, 0)$, *and for* $(n, t) = (4, -17)$, $(6, -53)$, $(4, -65)$, $(4, -77)$, *and* $(4, -97)$ *with respective solutions* $(x, y) = (\pm 3, \pm 8)$, $(\pm 3, \pm 26)$, $(\pm 3, \pm 4)$, $(\pm 3, \pm 2)$, *and* $(\pm 7, \pm 48)$.

If n is odd and $p \mid n$, we can write $x^n = (x^{n/p})^p$, so we can reduce to the exponent p. Thus in the sequel we will usually assume that n is an odd prime number p.

6.7.1 General Results

For reasons which will soon become clear, we make the following definitions.

Definition 6.7.2. *We will say that condition $H(p,t)$ is satisfied if p is an odd prime, t is a squarefree negative integer not congruent to 1 modulo 8, and p does not divide the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{t})$. By abuse of notation we will say that $H(t)$ is satisfied if t is a squarefree negative integer not congruent to 1 modulo 8.*

Proposition 6.7.3. *Assume $H(p,t)$, and define $A_p(t)$ to be the (possibly empty) set of nonnegative integers a such that*

$$\sum_{k=0}^{(p-1)/2} \binom{p}{2k} a^{2k} t^{(p-1)/2-k} = \pm 1 .$$

The set of solutions $(x,y) \in \mathbb{Z}^2$ to the Diophantine equation $y^2 = x^p + t$ is given by the pairs

$$(x,y) = \left(a^2 - t, \pm \sum_{k=0}^{(p-1)/2} \binom{p}{2k+1} a^{2k+1} t^{(p-1)/2-k} \right)$$

for each $a \in A_p(t)$, with in addition the so-called special pairs

$$(x,y) = (a^2 + 2\varepsilon, \pm(a^3 + 3\varepsilon a))$$

if $p = 3$ and $t = -(3a^2 + 8\varepsilon)$ for any $\varepsilon = \pm 1$ and odd a such that $a \geqslant 1$ if $\varepsilon = 1$ or $a \geqslant 3$ if $\varepsilon = -1$.

Proof. Let (x,y) be a solution to the equation $y^2 = x^p + t$. In the quadratic field $K = \mathbb{Q}(\sqrt{t})$ we can write $(y - \sqrt{t})(y + \sqrt{t}) = x^p$. I claim that the ideals generated by the two factors on the left are coprime. Indeed, assume otherwise, so let $\mathfrak{q}$ be a prime ideal of $\mathbb{Z}_K$ dividing these factors. It thus divides their sum and difference, hence if q is the prime number below $\mathfrak{q}$ we have $q \mid 2y$ and $q \mid 2t$. If x is even, then y is odd since otherwise $4 \mid t$ contradicting the squarefreeness of t, hence $t = y^2 - x^p \equiv 1 \pmod 8$, contradicting our assumption on t. Thus x is odd, hence $\mathfrak{q}$ cannot be above 2, so $q \mid \gcd(y,t)$, hence $q \mid x$ so $q^2 \mid t$, again contradicting the fact that t is squarefree and proving my claim. Since the product of the two coprime ideals $(y - \sqrt{t})\mathbb{Z}_K$ and $(y + \sqrt{t})\mathbb{Z}_K$ is a pth power, it follows that $(y + \sqrt{t})\mathbb{Z}_K = \mathfrak{a}^p$ for some ideal $\mathfrak{a}$ of $\mathbb{Z}_K$. On the other hand if h denotes the class number of K then essentially by definition the ideal $\mathfrak{a}^h$ is a principal ideal. Since by assumption p and h are coprime, there exist integers v and w such that $vp + wh = 1$, so that $\mathfrak{a} = (\mathfrak{a}^p)^v (\mathfrak{a}^h)^w$ is itself a principal ideal, say $\mathfrak{a} = \alpha\mathbb{Z}_K$ for some $\alpha \in \mathbb{Z}_K$ (this type of reasoning involving the class number is typical, and will be met again, for instance in Fermat's last theorem). We thus deduce that there exists a unit $\varepsilon \in K$ such that $y + \sqrt{t} = \varepsilon\alpha^p$. However, since K is an *imaginary* quadratic field, there are not many units, and more precisely the

group of units is $\{\pm 1\}$ except for $t = -1$ and $t = -3$ for which it has order 4 and 6 respectively. Since p is odd, it follows that apart from the special case $(p,t) = (3,-3)$ the order of the group of units is coprime to p, hence any unit is a pth power, so in these cases we are reduced to the equation $y + \sqrt{t} = \alpha^p$ with $\alpha \in \mathbb{Z}_K$. We will see in Proposition 6.7.5 below that there are no solutions for $(p,t) = (3,-3)$. Otherwise, we write $\alpha = (a + b\sqrt{t})/d$ with a and b integral, where either $d = 1$, or, only in the case $t \equiv 5 \pmod 8$, also $d = 2$ and a and b odd. Expanding the relation $y + \sqrt{t} = \alpha^p$ gives the two equations

$$d^p y = \sum_{k=0}^{(p-1)/2} \binom{p}{2k+1} a^{2k+1} b^{p-2k-1} t^{(p-1)/2-k} \text{ and}$$
$$d^p = \sum_{k=0}^{(p-1)/2} \binom{p}{2k} a^{2k} b^{p-2k} t^{(p-1)/2-k} .$$

Note that we may assume $a \geqslant 0$ since changing a into $-a$ does not change the second equation, and changes y into $-y$ in the first. From the second equation we deduce that $b \mid d^p$, and since b is coprime to d this means that $b = \pm 1$. It follows that

$$d^p = \pm \sum_{k=0}^{(p-1)/2} \binom{p}{2k} a^{2k} t^{(p-1)/2-k} .$$

If $d = 1$, we obtain the formula for y by replacing in the first equation, and we have $x = a^2 - b^2 t$. If $d = 2$, then since p is an odd prime we have

$$2 \equiv 2^p \equiv \pm t^{(p-1)/2} \equiv \pm\left(\frac{t}{p}\right) \equiv 0,\ \pm 1 \pmod p ,$$

which is possible only for $p = 3$, giving $t = -(3a^2 \mp 8)$, $y = -a^3 \pm 3a$, $x = a^2 \mp 2$, whence the additional cases of the proposition. □

Remarks.

(1) When t is not squarefree, it is easy to obtain similar but more complicated results, see for example Exercise 31.

(2) For *given* t and p, it is trivial to find all possible values of $a \in A_p(t)$. What is considerably more difficult in general is to find the sets $A_p(t)$. Thanks to a remarkable theorem of Bilu, Hanrot, and Voutier, this problem is completely solved, see below.

(3) Considering the formula modulo p, it is clear that the $\pm$ sign on the right hand side of the formula defining $A_p(t)$ is equal to $\left(\frac{t}{p}\right)$.

(4) Much more important is the fact that in the cases that we have not treated ($t \equiv 1 \pmod 8$, $t > 0$, or p not coprime to the class number of

$\mathbb{Q}(\sqrt{t})$) the problem is considerably more difficult but can be reduced to a finite number of so-called Thue equations. First if $t \equiv 1 \pmod 8$ (positive or negative, but squarefree), we see that either x is odd, hence y is even and the proof goes through as above. Or x is even hence y is odd, hence $y - \sqrt{t}$ and $y + \sqrt{t}$ are both divisible by 2 in $\mathbb{Z}_K$, and we can easily deduce that $(y + \sqrt{t})/2 = \mathfrak{p}_2^{p-2}\mathfrak{a}^p$ for some ideal $\mathfrak{a}$ and some ideal $\mathfrak{p}_2$ above 2. Thus for *any* squarefree t we can reduce our equation to either to $(y+\sqrt{t})/d = \mathfrak{a}^p$, or to $(y+\sqrt{t})/d = \mathfrak{p}_2^{p-2}\mathfrak{a}^p$ for $d = 1$ or 2. Since the number of possibilities for d and $\mathfrak{p}_2$ is finite, since the class group and the unit group modulo pth powers are also finite, an easy argument shows that our Diophantine equation reduces to a *finite* set of equations of the form $y + \sqrt{t} = \beta_i \alpha_i^p$, for a known finite set of elements $\beta_i \in K^*$, and unknowns $\alpha_i \in \mathbb{Z}_K$ (the above proof corresponds to the special case $\beta_i = 1$). When we expand this equation after writing $\alpha_i = (a + b\sqrt{t})/d$, the enormous simplification of having b as a common factor of all the coefficients of $\sqrt{t}$ (implying $b = \pm 1$) no longer occurs, and we have to solve equations of the form $P(a,b) = d^p$, where P is a homogeneous polynomial of degree p in a and b with integral coefficients depending on t. These are called Thue equations, and there are excellent methods for solving them, based on linear forms in logarithms. The problem is that the equations depends on t, so for a fixed t and p it is "easy" to solve the equation, however when we fix p, say, and let t vary it is more difficult to give a general solution.

Proposition 6.7.3 can be rephrased in a more positive way as follows.

Corollary 6.7.4. *Let $p \geqslant 3$ be a prime, let x and y be integers, and assume that $t = y^2 - x^p$ satisfies $H(t)$ (so that in particular x and y are coprime and x is odd). Assume in addition that $t + x$ is not a square, and furthermore when $p = 3$ that we do not have $(x,t) = (a^2 + 2\varepsilon, -(3a^2 + 8\varepsilon))$ for some odd a and some $\varepsilon = \pm 1$. Then the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{t})$ is divisible by p.*

Proof. Clear since $x = a^2 - t$, except in the given special case. □

6.7.2 The Case $p = 3$

To apply Proposition 6.7.3 (assuming $H(p,t)$), there remains to find the sets $A_p(t)$. As already mentioned, this is trivial if p and t are fixed. The difficulty is to give general results when only one of these two variables is fixed. We will give detailed results below, and in particular complete results for some fixed values of t. In the next subsections we give the complete results for fixed p.

Proposition 6.7.5. *Assume $H(3,t)$.*

(1) *When $t \equiv 2$ or 3 modulo 4 then if t is not of the form $t = -(3a^2 \pm 1)$ the equation $y^2 = x^3 + t$ has no integral solutions. If $t = -(3a^2 + \varepsilon)$ with $\varepsilon = \pm 1$, the integral solutions are $x = 4a^2 + \varepsilon$, $y = \pm(8a^3 + 3\varepsilon a)$.*

(2) *When* $t \equiv 5 \pmod 8$ *then if* t *is not of the form* $t = -(12a^2 - 1)$ *or* $-(3a^2 \pm 8)$, *both with* a *odd, the equation* $y^2 = x^3 + t$ *has no integral solutions. If* $t = -(12a^2 - 1)$ *with* a *odd, the integral solutions are* $x = 16a^2 - 1$, $y = \pm(64a^3 - 6a)$. *If* $t = -(3a^2 + 8\varepsilon)$ *with* $\varepsilon = \pm 1$ *and* a *odd, the integral solutions are* $x = a^2 + 2\varepsilon$, $y = \pm(a^3 + 3a\varepsilon)$.

Proof. This case is especially simple since the equations defining the sets $A_3(t)$ are *linear* in t. We find $t = -(3a^2 \pm 1)$, $x = a^2 - t$ and $y = \pm(a^3 + 3at)$, giving the solutions of the proposition, to which we must add the solutions for the special case $t = -(3a^2 \pm 8)$. Recall that we have postponed the case $t = -3$ which we now consider. In the proof of Proposition 6.7.3 we found that $y + \sqrt{t} = u\alpha^3$ for some unit u. Thus either we are led to the equations of the proposition (if $u = \pm 1$), or there exists $\varepsilon = \pm 1$ such that $y + \sqrt{t} = ((a + b\sqrt{t})/2)^3(-1 + \varepsilon\sqrt{t})/2$. Equating coefficients of $\sqrt{t}$ gives

$$16 = \varepsilon(a^3 - 9b^2a) - 3b(a^2 - b^2) \ .$$

If $a \equiv 0 \pmod 3$, the right hand side is divisible by 3, a contradiction. If $b \equiv 0 \pmod 3$, the right hand side is congruent to ± 1 modulo 9 since a cube is such, again a contradiction. Thus neither a nor b is divisible by 3, hence $a^2 \equiv b^2 \equiv 1 \pmod 3$, so the right hand side is still congruent to ± 1 modulo 9, a contradiction once again, so there are no solutions for $t = -3$. □

Note that the case $t = -2$ of the above equation was already solved by Fermat, who posed it as a challenge problem to his English contemporaries.

Although usually the problem for $t > 0$ or for $t \equiv 1 \pmod 8$ is much more difficult, in certain cases it is quite easy to find the set of integral solutions. A classical example is the following, for which the special case $t = 7$ is also due to Fermat.

Proposition 6.7.6. *Let* a *and* b *be odd integers such that* $3 \nmid b$, *and assume that* $t = 8a^3 - b^2$ *is squarefree but of any sign. Then the equation* $y^2 = x^3 + t$ *has no integral solution.*

Proof. We rewrite the equation as

$$y^2 + b^2 = (x + 2a)((x - a)^2 + 3a^2) \ .$$

Note that x must be odd otherwise $y^2 = x^3 + t \equiv t \equiv 7 \pmod 8$, which is absurd. Since a is also odd it follows that $(x - a)^2 + 3a^2 \equiv 3 \pmod 4$, and since this is a positive number (why is this needed?) this implies that there exists a prime $p \equiv 3 \pmod 4$ dividing it to an *odd* power. Thus $y^2 + b^2 \equiv 0 \pmod p$, and since $\left(\frac{-1}{p}\right) = -1$ this implies that p divides b and y. I claim that $p \nmid x + 2a$. Indeed, since

$$(x - a)^2 + 3a^2 = (x + 2a)(x - 4a) + 12a^2$$

if we had $p \mid x + 2a$ we would have $p \mid 12a^2$, hence either $p \mid a$ or $p = 3$ ($p = 2$ is impossible since $p \equiv 3 \pmod 4$). But $p \mid a$ implies $p^2 \mid t = 8a^3 - b^2$, a contradiction since t is squarefree, and $p = 3$ implies $3 \mid b$, which has been excluded, proving my claim. Thus the p-adic valuation of $y^2 + b^2$ is equal to that of $(x - a)^2 + 3a^2$ hence is odd, a contradiction since this would again imply that $\left(\frac{-1}{p}\right) = 1$. □

Another similar result is the following.

Proposition 6.7.7. *Let a be an odd integer, let b be an integer such that $3 \nmid b$, and assume that $t = a^3 - 4b^2$ is squarefree, not congruent to 1 modulo 8, but of any sign. Then the equation $y^2 = x^3 + t$ has no integral solution.*

Proof. I claim that x is odd. Indeed, otherwise, since t is odd, y would be odd, hence $y^2 \equiv 1 \pmod 8$, hence $t \equiv 1 \pmod 8$, contradicting our assumption. Thus x is odd and y is even. Writing $y = 2y_1$ we obtain

$$4(y_1^2 + b^2) = x^3 + a^3 = (x + a)(x(x - a) + a^2) .$$

Since $x - a$ is even and a is odd, it follows that $4 \mid x + a$. Writing $x + a = 4x_1$, we obtain

$$y_1^2 + b^2 = x_1((4x_1 - a)(4x_1 - 2a) + a^2) = x_1(16x_1^2 - 12ax_1 + 3a^2) .$$

Since a is odd we have $16x_1^2 - 12ax_1 + 3a^2 \equiv 3 \pmod 4$, hence as in the preceding proof there exists a prime $p \equiv 3 \pmod 4$ dividing it to an odd power. As above, this implies that p divides y_1 and b. I claim that $p \nmid x_1$. Indeed, otherwise $p \mid 3a^2$, hence either $p \mid a$ or $p = 3$. As above $p \mid a$ is impossible since it implies $p^2 \mid t$, a contradiction since t is squarefree, and $p = 3$ implies $3 \mid b$, which has been excluded. Thus the p-adic valuation of $y_1^2 + b^2$ is odd, a contradiction since this would imply $\left(\frac{-1}{p}\right) = 1$. □

Proposition 6.7.5 applies to negative squarefree t not congruent to 1 modulo 8 such that the class number of $\mathbb{Q}(\sqrt{t})$ is not divisible by 3. The two propositions above solve our equation for the following additional values of t with $|t| < 250$:

$t = -241, -129$ (class number divisible by 3), 7, 11, 13, 23, 39, 47, 53, 61, 67, 83, 87, 95, 109, 139, 155, 159, 167, 191, 215, 239 ($t > 0$).

Finally, note that we will solve the case $t = 1$ below (Corollary 6.5.3) as an application of a general theorem of Skolem.

6.7.3 The Case $p = 5$

In this case we can also give the complete answer as follows.

Proposition 6.7.8. *Assume $H(5,t)$. The only values of t for which the equation $y^2 = x^5 + t$ has a solution are $t = -1$ (with only solution $(x,y) = (1,0)$), $t = -19$ (with only solutions $(x,y) = (55, \pm 22434)$), and $t = -341$ (with only solutions $(x,y) = (377, \pm 2759646)$).*

Proof. The equation defining the set $A_5(t)$ of Proposition 6.7.3 is $t^2 + 10a^2t + 5a^4 \pm 1 = 0$. This has a rational solution in t if and only if the discriminant is a square, hence if and only if $20a^4 \mp 1 = b^2$ for some integer b. Looking modulo 4 shows that the sign must be $+$ so $b^2 = 20a^4 + 1$, hence $(2b)^2 = 5(2a)^4 + 4$. This is one of the equations that we will solve in Corollary 6.8.4 as a consequence of our study of squares in Lucas and Fibonacci sequences. We deduce from that corollary that $a = 0$ or $a = \pm 6$. The value $a = 0$ leads to $t = -1$ (giving the universally trivial solution $(x,y) = (1,0)$), and $a = \pm 6$ leads to $t = -19$, $(x,y) = (55, \pm 22434)$ and $t = -341$, $(x,y) = (377, \pm 2758646)$. □

The following is a strengthening of Corollary 6.7.4 in the case $p = 5$.

Corollary 6.7.9. *Let x and y be integers such that the pair (x,y) is not equal to $(1,0)$, $(55, \pm 22434)$, or $(377, \pm 2758646)$. Assume that $t = y^2 - x^5$ satisfies $H(t)$ (so that in particular x and y are coprime and x is odd). Then the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{t})$ is divisible by 5.*

Proof. Clear. □

Note that it is necessary to impose *some* conditions on x and y. For instance if $(x,y) = (2,5)$ we have $t = -7 \equiv 1 \pmod 8$, but the class number of $\mathbb{Q}(\sqrt{-7})$ is 1. However it can be shown that if we only assume that x and y are coprime, but t not necessarily squarefree, then the class number of the quadratic *order* of discriminant t (or $4t$ if $t \equiv 2$ or 3 modulo 4) is divisible by 5.

6.7.4 Application of the Bilu–Hanrot–Voutier Theorem

To treat the case $p \geqslant 7$, we use a remarkable theorem of the above authors. We need a definition.

Definition 6.7.10. *Let α and β be such that $\alpha + \beta$ and $\alpha\beta$ are nonzero coprime integers and such that α/β is not a root of unity.*

(1) *The Lucas sequence associated to α, β is the sequence defined by $u_n = u_n(\alpha,\beta) = (\alpha^n - \beta^n)/(\alpha - \beta)$ for $n \in \mathbb{Z}_{\geqslant 0}$.*
(2) *We say that a prime number p is a* primitive divisor *of u_n if $p \mid u_n$ but $p \nmid u_i$ for $0 < i < n$ and $p \nmid (\alpha - \beta)^2$.*

Note that I use the original name of Lucas sequence, but it should more properly be called a generalized Fibonacci sequence since the usual Lucas sequence is rather $u_n = \alpha^n + \beta^n$.

A special case of the theorem of Bilu, Hanrot, and Voutier is the following (see [Bil-Han-Vou] for the most general statements).

Theorem 6.7.11. *Let $u_n = u_n(\alpha, \beta)$ be a Lucas sequence as above. Then*

(1) *If $n > 30$, u_n always has a primitive divisor.*
(2) *If $5 < n < 30$ is prime and $u_n(\alpha, \beta)$ has no primitive divisors, then either $n = 7$ and $(\alpha, \beta) = ((1 + \sqrt{-7})/2, (1 - \sqrt{-7})/2)$, or $n = 7$ and $(\alpha, \beta) = ((1 + \sqrt{-19})/2, (1 - \sqrt{-19})/2)$, or $n = 13$ and $(\alpha, \beta) = ((1 + \sqrt{-7})/2, (1 - \sqrt{-7})/2)$.*

This theorem solves a century old problem, and its proof involves both very delicate estimates on linear forms in logarithms, and new algorithms for solving Thue equations. It is thus a beautiful mixture of difficult mathematics with an extensive rigorous computer computation (as the epigraph of the paper remarkably illustrates).

An immediate corollary of the above theorem to our problem is the following.

Corollary 6.7.12. *Let $p \geqslant 7$ be prime, and assume $H(p, t)$. The only value of t for which the equation $y^2 = x^p + t$ has a solution is $t = -1$ with only solution $(x, y) = (1, 0)$.*

Proof. Indeed, the equation defining the set $A_p(t)$ is $(\alpha^p - \beta^p)/(\alpha - \beta) = \pm 1$ with $\alpha = a + \sqrt{t}$ and $\beta = a - \sqrt{t}$, hence with the notation of the above definition $u_p(\alpha, \beta) = \pm 1$. We have $0 \in A_p(t)$ if and only if $t = \pm 1$, hence $t = -1$ since we assume $t < 0$. Otherwise it is clear that $\alpha + \beta$ and $\alpha\beta$ are integers, and α/β belongs to the imaginary quadratic field $\mathbb{Q}(\sqrt{t})$. Since $\alpha/\beta \neq \pm 1$ for $a \neq 0$ it can be a root of unity only when $t = -1$ or $t = -3$. However it is easily checked that for $t = -1$ the only nonzero values of a such that α/β is a root of unity are $a = \pm 1$, and for $t = -3$ they are $a = \pm 1$ and $a = \pm 3$, see Exercise 35. In all these cases the same exercise shows that for $p \geqslant 7$ we have $|u_p(\alpha, \beta)| > 1$. Thus these cases do not give any elements of $A_p(t)$, and we may therefore apply the above theorem. Thus for $p > 30$, $A_p(t)$ must have a primitive divisor, and in particular it cannot be equal to ± 1, while for $7 \leqslant p < 30$ all the possibilities listed in the theorem give $\alpha = (u + \sqrt{v})/2$ with u and v odd, which thus cannot be of the form $a + \sqrt{t}$. □

I would again like to emphasize that the above corollary, which immediately follows from the theorem of Bilu, Hanrot, and Voutier is very deep.

6.7.5 Special Cases with Fixed t

The above corollary essentially solves the problem when the condition $H(p,t)$ is satisfied. However it is not completely satisfactory for two reasons. The first is mathematical: we must comment on what we can do when the condition $H(p,t)$ is not satisfied, although we will have to assume $H(t)$. The second is pedagogical: in the study of Catalan's equation we will need the case $t=-1$, and to be entirely self-contained we treat it without using the difficult theorem of Bilu–Hanrot–Voutier. The following result is due to V.-A. Lebesgue (see [Leb]).

Proposition 6.7.13 (V.-A. Lebesgue). *For $p \geqslant 3$ prime the only integral solution to the equation $y^2 = x^p - 1$ is $(x,y) = (1,0)$.*

Proof. First note that since the class number of $\mathbb{Q}(\sqrt{-1})$ is equal to 1 the condition $H(p,-1)$ is satisfied for all p. Furthermore $t=-1$ does not occur in the special cases, so we must show that 0 is the only element of $A_p(t)$. Thus, let $a \in A_p(t)$, in other words by definition such that

$$\sum_{k=0}^{(p-1)/2} \binom{p}{2k} a^{2k} (-1)^{(p-1)/2-k} = \pm 1 \ .$$

Since $p \mid \binom{p}{2k}$ for $1 \leqslant k \leqslant (p-1)/2$ and $p \geqslant 3$ it follows by looking at the equation modulo p that the right hand side is equal to $(-1)^{(p-1)/2}$. We thus have $L=0$ with

$$L = \sum_{k=1}^{(p-1)/2} \binom{p}{2k} a^{2k} (-1)^{(p-1)/2-k} \ .$$

I claim that a is even. Indeed, otherwise looking at the equation modulo 2 we would obtain

$$\sum_{k=0}^{(p-1)/2} \binom{p}{2k} \equiv 1 \pmod 2 \ ,$$

which is absurd since the left hand side is equal to 2^{p-1} which is even. Now set

$$u_k = \binom{p}{2k} a^{2k} = \frac{p(p-1)}{2k(2k-1)} \binom{p-2}{2k-2} a^{2k} \ .$$

Since $u_1 = p(p-1)a^2/2$, we have

$$\frac{u_k}{u_1} = \frac{1}{k(2k-1)} \binom{p-2}{2k-2} a^{2k-2} \ ,$$

so that for $k > 1$ (hence $p > 3$) we have

$$v_2(u_k) - v_2(u_1) \geqslant (2k-2)v_2(a) - v_2(k) \geqslant (2k-2) - v_2(k)$$

since a is even. It is immediately checked that the rightmost expression is always greater than or equal to 1, hence that $v_2(u_k) > v_2(u_1)$ for $k > 1$. Since $L = \sum_{k=1}^{(p-1)/2}(-1)^{(p-1)/2-k}u_k$ it follows that $v_2(L) = v_2(u_1) = v_2((p(p-1)/2)a^2)$, which is impossible if $a \neq 0$ since $L = 0$. Thus we must have $a = 0$, proving the proposition. □

It is easy to generalize the above reasoning to other values of t (see Exercises 36 and 33), but thanks to the Bilu–Hanrot–Voutier theorem we do not need to do so. In fact, for small values of t satisfying $H(t)$ we have the following definitive result:

Theorem 6.7.14. *Assume $H(t)$, in other words that t is a squarefree negative integer such that $t \not\equiv 1 \pmod 8$. For $n \geqslant 3$ and $-100 \leqslant t \leqslant -1$ the Diophantine equations $y^2 = x^n + t$ do not have any integral solutions except for the solutions with $y = 0$ when $t = -1$, and for the pairs (t, n) given in the table below, for which the only solutions (x, y) are as indicated.*

(t,n)	(x,y)	(t,n)	(x,y)
$(-2,3)$	$(3,\pm5)$	$(-11,3)$	$(3,\pm4)$ and $(15,\pm58)$
$(-13,3)$	$(17,\pm70)$	$(-17,4)$	$(\pm3,\pm8)$
$(-19,3)$	$(7,\pm18)$	$(-19,5)$	$(55,\pm22434)$
$(-26,3)$	$(3,\pm1)$ and $(35,\pm207)$	$(-35,3)$	$(11,\pm36)$
$(-53,3)$	$(9,\pm26)$ and $(29,\pm156)$	$(-53,6)$	$(3,\pm26)$
$(-61,3)$	$(5,\pm8)$	$(-65,4)$	$(\pm3,\pm4)$
$(-67,3)$	$(23,\pm110)$	$(-74,3)$	$(99,\pm985)$
$(-74,5)$	$(3,\pm13)$	$(-77,4)$	$(\pm3,\pm2)$
$(-83,3)$	$(27,\pm140)$	$(-83,9)$	$(3,\pm140)$
$(-89,3)$	$(5,\pm6)$	$(-97,4)$	$(\pm7,\pm48)$

Solubility of $y^2 = x^n + t$ for (t, n) as in the Theorem

Proof. For $t = -1$, we have the trivial solutions $(x, y) = (1, 0)$ if n is odd, $(x, y) = (\pm1, 0)$ if n is even. Thanks to Proposition 6.7.1 we know that for $-100 < t < -1$ the only ones for which there are solutions with n even are the given ones. Otherwise we may restrict to $n = p$ an odd prime and deduce the others from that case. When the condition $H(p, t)$ is satisfied, we obtain the equations and the solutions of the theorem. The only values of t such that $-100 < t < -1$ for which $H(t)$ is true but the condition $H(p, t)$ is not satisfied are $t = -26$, -29, -38, -53, -59, -61, -83, and -89 for $p = 3$, and $t = -74$ and $t = -86$ for $p = 5$. In the case $p = 3$ we must find all integral solutions to $y^2 = x^3 + t$ for the 8 given values of t. This is done without difficulty by using the techniques of Section 8.7, see Exercise 27 of Chapter 8. On the other hand in the case $p = 5$ and $t = -74$ or $t = -86$, we must find the integral points on $y^2 = x^5 + t$ which is a hyperelliptic curve of genus 2. This is more difficult, and I refer either to Chapter 13 for the

general methods of attack of this kind of problem, or to the original paper by Mignotte and de Weger [Mig-Weg]. □

6.8 Linear Recurring Sequences

6.8.1 Squares in the Fibonacci and Lucas Sequences

We have already seen in Section 4.5.3 how to apply p-adic methods to find specific values of linear recurring sequences. I emphasize the fact that these methods (for instance using Strassmann's theorem) are really p-adic in nature, and not simply based on simple congruence arguments. In the present section, we will study similar problems which on the other hand can be solved by congruence arguments and quadratic reciprocity.

We let $\alpha = (1+\sqrt{5})/2$ and $\beta = (1-\sqrt{5})/2$ be the two roots of the equation $x^2 - x - 1 = 0$. We define classically the Fibonacci sequence F_n and the Lucas sequence L_n by the formulas

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad L_n = \alpha^n + \beta^n \ ,$$

so that the sequences F_n and L_n both satisfy the linear recursion $u_{n+1} = u_n + u_{n-1}$, with initial terms $F_0 = 0$, $F_1 = 1$ and $L_0 = 2$, $L_1 = 1$.

Before stating the Diophantine theorems, we need some elementary properties of these sequences, summarized in the following proposition.

Proposition 6.8.1. (1) $L_{-n} = (-1)^n L_n$, $F_{-n} = (-1)^{n-1} F_n$, $L_n^2 - 5F_n^2 = 4(-1)^n$, $2L_{m+n} = 5F_mF_n + L_mL_n$, $2F_{m+n} = F_mL_n + F_nL_m$, $L_{2m} = L_m^2 + 2(-1)^{m-1}$, $F_{2m} = F_mL_m$.
(2) $\gcd(L_n, F_n) = 1$ *if* $3 \nmid n$, $\gcd(L_n, F_n) = 2$ *if* $3 \mid n$.
(3) *When* $k \equiv \pm 2 \pmod 6$ *then for all* $t \in \mathbb{Z}$ *we have*

$$L_{n+2kt} \equiv (-1)^t L_n \pmod{L_k} \quad \textit{and} \quad F_{n+2kt} \equiv (-1)^t F_n \pmod{L_k} \ .$$

Proof. The formulas of (1) are proved by direct computation from the definitions in terms of α and β, which can be summarized by the equality $(L_n + F_n\sqrt{5})/2 = \alpha^n$. For (2), we note that since $|L_n^2 - 5F_n^2| = 4$, the GCD of L_n and F_n is equal to 1 or 2. Because of that same formula it is equal to 2 if and only if $2 \mid F_n$, and since evidently the sequence F_n modulo 2 is periodic of period 3, we see that $2 \mid F_n$ if and only if $3 \mid n$, proving (2).

For (3), since $2 \mid k$ we have

$$2L_{n+2k} = 5F_nF_{2k} + L_nL_{2k} = 5F_nF_kL_k + L_n(L_k^2 - 2) \equiv -2L_n \pmod{L_k} \ .$$

Since $3 \nmid k$ we have $2 \nmid L_k$, hence $L_{n+2k} \equiv -L_n \pmod{L_k}$ so the result for L follows by induction on t. Similarly

$$2F_{n+2k} = F_nL_{2k} + F_{2k}L_n = F_n(L_k^2 - 2) + F_kL_kL_n \equiv -2F_n \pmod{L_k} ,$$

and we conclude as before.

Theorem 6.8.2. (1) *For $n \geqslant 0$ we have $L_n = x^2$ with $x \in \mathbb{Z}$ if and only if $n = 1$ or $n = 3$.*
(2) *Similarly $L_n = 2x^2$ if and only if $n = 0$ or $n = 6$.*

Proof. Since $L_{2m} = L_m^2 + 2(-1)^{m-1}$, $L_{2m} = x^2$ implies that $|x^2 - L_m^2| = 2$, which is impossible. Thus we may assume that n is odd. Clearly $L_1 = 1$ and $L_3 = 4$ are squares, so we may assume that $n > 3$. We can write $n = r + 2 \cdot 3^s k$ with $r = 1$ or 3, $2 \mid k$ and $3 \nmid k$, hence $k \equiv \pm 2 \pmod 6$ and $k > 0$. By the above proposition we thus have

$$L_n \equiv (-1)^{3^s} L_r \equiv -L_r \pmod{L_k} .$$

On the other hand since $L_1 = 1$ and $L_3 = 4$, we have $-L_r = -1$ or -4. Note also that since $k/2 \equiv \pm 1 \pmod 3$, we have

$$L_k = L_{k/2}^2 + 2(-1)^{k/2-1} \equiv 1 \pm 2 \equiv 3 \pmod 4 ,$$

hence

$$\left(\frac{L_n}{L_k}\right) = \left(\frac{-L_r}{L_k}\right) = \left(\frac{-1}{L_k}\right) = -1 .$$

If follows that L_n cannot be a square, proving (1).

To prove (2), let $L_n = 2x^2$ with $x \in \mathbb{Z}$. We consider several cases.

• If n is odd, then $4x^4 = L_n^2 = 5F_n^2 - 4$, hence F_n is even, so that $x^4 = 5(F_n/2)^2 - 1$. But $x^4 \equiv 0$ or 1 modulo 8, hence $(F_n/2)^2 \equiv 5$ or 2 modulo 8, a contradiction.

• If $4 \mid n$ and $n \neq 0$, we can write $n = 2 \cdot 3^s k$ with $k \equiv \pm 2 \pmod 6$, so that by the proposition

$$2L_n \equiv -2L_0 \equiv -4 \pmod{L_k} ,$$

hence as above $\left(\frac{2L_n}{L_k}\right) = -1$ so that $2L_n$ cannot be a square.

• If $n \equiv 6 \pmod 8$ and $n \neq 6$, we can write $n = 6 + 2 \cdot 3^s k$ with $k \equiv \pm 2 \pmod 6$, so that by the proposition

$$2L_n \equiv -2L_6 \equiv -36 \pmod{L_k} .$$

On the other hand note that $3 \mid L_m$ if and only if $m \equiv 2 \pmod 4$, hence since $4 \mid k$ we have $3 \nmid L_k$. Thus as above $\left(\frac{2L_n}{L_k}\right) = -1$ so that $2L_n$ cannot be a square.

• If $n \equiv 2 \pmod 8$ then $L_{-n} = L_n$ and $-n \equiv 6 \pmod 8$, so the preceding reasoning (which is applicable for $n < 0$) shows that $L_n = 2x^2$ if and only if $-n = 6$, and in particular $n < 0$. □

Theorem 6.8.3. (1) *We have $F_n = x^2$ with $x \in \mathbb{Z}$ if and only if $n = 0, \pm 1, 2,$ or 12.*
(2) *Similarly $F_n = 2x^2$ if and only if $n = 0, \pm 3,$ or 6.*

Proof. The proof of this theorem is similar and left to the reader (see Exercise 37). □

As an application of the above theorem, we give the following corollary.

Corollary 6.8.4. *Consider the Diophantine equation*

$$y^2 = 5x^4 + a\,.$$

(1) *For $a = 1$, the only integral solutions are $(x, y) = (0, \pm 1)$ and $(\pm 2, \pm 9)$.*
(2) *For $a = -1$, the only integral solutions are $(x, y) = (\pm 1, \pm 2)$.*
(3) *For $a = 4$, the only integral solutions are $(x, y) = (0, \pm 2)$, $(\pm 1, \pm 3)$, $(\pm 12, \pm 322)$.*
(4) *For $a = -4$, the only integral solutions are $(x, y) = (\pm 1, \pm 1)$.*

Proof. If we write the equations as $y^2 - 5x^4 = \varepsilon b^2$ with $\varepsilon = \pm 1$ and $b = 1$ or $b = 2$, we see that we can apply the solution to the Pell equation $y^2 - 5X^2 = \pm 1$ or ± 4. The fundamental unit of the order $\mathbb{Z}[\sqrt{5}]$ is $2 + \sqrt{5} = \alpha^3$, of norm -1, hence the general solution with $X \geqslant 0$ to $y^2 - 5X^2 = \pm 1$ is given by $y + X\sqrt{5} = \alpha^{3n}$, hence

$$2x^2 = 2X = \frac{\alpha^{3n} - \beta^{3n}}{\alpha - \beta} = F_{3n}\,.$$

By the above theorem, this implies $n = 0$, ± 1, or 2. The value $n = 0$ gives the solution $x = 0$ to the first equation (hence $y = \pm 1$), and $n = 2$ gives the solution $x = \pm 2$ to the first equation (hence $y = \pm 9$). On the other hand $n = \pm 1$ gives the solution $x = \pm 1$ to the second equation (hence $y = \pm 2$).

Similarly the general solution to $y^2 - 5X^2 = \pm 4$ is given by $(y + X\sqrt{5})/2 = \alpha^n$, hence $x^2 = X = F_n$. By the above theorem this implies $n = 0$, ± 1, 2 or 12. The values $n = 0$, 2 and 12 give the solutions $x = 0$ (hence $y = \pm 2$), $x = \pm 1$ (hence $y = \pm 3$), $x = \pm 12$ (hence $y = \pm 322$) to the third equation, while $n = \pm 1$ gives the solution $x = \pm 1$ (hence $y = \pm 1$) to the fourth equation. □

Remark. Using a combination of Baker-type methods giving lower bounds for linear forms in 2 or 3 logarithms of algebraic numbers (see Chapter 12), and the Ribet–Taylor–Wiles level lowering method (see Chapter 15), Y. Bugeaud, M. Mignotte and S. Siksek have recently proved the following remarkable result:

Theorem 6.8.5 (Bugeaud–Mignotte–Siksek). (1) *The only nontrivial perfect powers in the Fibonacci sequence are $F_1 = F_2 = 1$, $F_6 = 8$, and $F_{12} = 144$.*

(2) *The only nontrivial perfect powers in the Lucas sequence are* $L_1 = 1$ *and* $L_3 = 4$.

We also mention without proof the following results of the same type.

Theorem 6.8.6 (Ljunggren, Ellenberg). *The only integral solutions to the Diophantine equation* $x^2 - 2y^4 = -1$ *are* $(x, y) = (\pm 1, \pm 1)$ *and* $(x, y) = (\pm 239, \pm 13)$.

Theorem 6.8.7 (Cohn, Ljunggren). (1) *For fixed* D *the Diophantine equation* $x^4 - Dy^2 = 1$ *has at most one integral solution with* $x > 0$ *and* $y > 0$, except *for* $D = 1785$ *for which it has the two solutions* $(x, y) = (13, 4)$ *and* $(239, 1352)$.

(2) *If* D *is prime, the above equation has such a solution if and only if* $D = 5$ *and* $D = 29$, *for which it has the respective solutions* $(x, y) = (3, 4)$ *and* $(x, y) = (99, 1820)$.

6.8.2 The Square Pyramid Problem

A classical problem due to E. Lucas asks for all integral solutions to the equation $y^2 = 1^2 + 2^2 + \cdots + x^2$, in other words to the Diophantine equation $x(x+1)(2x+1) = 6y^2$. This problem was until relatively recently solved only using rather sophisticated methods, but in the 1980's a completely elementary proof was found, which we paraphrase in this section, see [Ma] and [Ang]. We need some preliminary results.

Lemma 6.8.8. *The only integral solutions to the Diophantine equation* $y^2 = 8x^4 + 1$ *are* $(x, y) = (0, \pm 1)$ *and* $(\pm 1, \pm 3)$.

Proof. We may assume $y > 0$. Since y is odd we can write $y = 2s + 1$, so that $2x^4 = s(s + 1)$. If s is even there exist coprime integers u and v such that $s = 2u^4$ and $s + 1 = v^4$, so that $v^4 - 2u^4 = 1$. By Proposition 6.6.15 this implies $u = 0$, hence $s = 0$, $x = 0$ and $y = \pm 1$. So assume that s is odd. In this case there exist coprime integers u and v such that $s = u^4$ and $s + 1 = 2v^4$, so that $u^4 + 1 = 2v^4$. This implies that u is odd, hence (by looking modulo 8) that v is odd. If we set $a = |v^2 - u|$ and $b = |v^2 + u|$, we see that $a^2 + b^2 = 2v^4 + 2u^2 = (u^2 + 1)^2$, so that $(a, b, u^2 + 1)$ are the three sides of a Pythagorean triangle, and its area is equal to $ab/2 = |(v^4 - u^2)/2| = ((u^2 - 1)/2)^2$, a square. Since we will show that 1 is not a congruent number (Proposition 6.12.2), it follows that the triangle must be degenerate, i.e., that $u = \pm 1$, hence $s = 1$, $x = \pm 1$ and $y = 3$, proving the lemma. □

Remark. It would have been more pleasing to consider the more general equation $y^2 = 8x^4 + z^4$ with x, y and z pairwise coprime. Unfortunately, as is shown in Exercise 12 of Chapter 8, this equation has an *infinity* of integral

solutions (because the corresponding elliptic curve has nonzero rank), hence the result would not be suitable for our purposes.

We can now solve Lucas's problem for even values of x.

Proposition 6.8.9. *The only integral solutions to the Diophantine equation* $x(x+1)(2x+1) = 6y^2$ *with* $y \neq 0$ *and* x even *are* $(x,y) = (24, \pm 70)$.

Proof. Clearly x is nonnegative. Since x is even and x, $x+1$ and $2x+1$ are pairwise coprime, the equation implies that the odd numbers $x+1$ and $2x+1$ are either squares or triples of squares. It follows that $x+1 \not\equiv 2 \pmod 3$ and $2x+1 \not\equiv 2 \pmod 3$, which is equivalent to $x \equiv 0 \pmod 3$. Thus we can find integers s, t and u such that $x = 6s^2$, $x+1 = t^2$ and $2x+1 = u^2$, and of course u and t are odd and coprime. The equality $6s^2 = (u-t)(u+t)$ implies that $4 \mid 6s^2$ hence that $2 \mid s$, hence write $s = 2v$, so that $6v^2 = ((u-t)/2)((u+t)/2)$. Since u and t are coprime so are $(u-t)/2$ and $(u+t)/2$. Changing if necessary the signs of u and t it follows that there exist integers a and b such that either $(u+t)/2 = 6a^2$ and $(u-t)/2 = b^2$, or $(u+t)/2 = 3a^2$ and $(u-t)/2 = 2b^2$. In the first case we have $t = 6a^2 - b^2$ and $s = 2ab$, and since $6s^2 + 1 = t^2$ we obtain the equation $24a^2b^2 + 1 = (6a^2 - b^2)^2$, hence $36a^4 - 36a^2b^2 + b^4 = 1$ which can be rewritten by completing the square $(6a^2 - 3b^2)^2 - 8b^4 = 1$. By the above lemma, since $3 \mid (6a^2 - 3b^2)$ we have $b = \pm 1$ and $a = \pm 1$, giving $s = 2ab = \pm 2$ so that $x = 24$ hence $y = \pm 70$. In the second case we have $t = 3a^2 - 2b^2$ and $s = 2ab$, giving here the equation $24a^2b^2 + 1 = (3a^2 - 2b^2)^2$, hence $9a^4 - 36a^2b^2 + 4b^4 = 1$ so that $(3a^2 - 6b^2)^2 - 2(2b)^4 = 1$. By Proposition 6.6.15 (which is stronger than what we need) we deduce that $b = 0$, hence $9a^4 = 1$, which is impossible, so there are no solutions in the second case. □

To solve the problem in the odd case we make an analysis similar to that done in Section 6.8.1. We set $\alpha = 2+\sqrt{3}$, $\beta = 2-\sqrt{3}$, $M_n = (\alpha^n + \beta^n)/2$, and $G_n = (\alpha^n - \beta^n)/(\alpha - \beta)$. The reason for dividing by 2 in M_n is that $\alpha^n + \beta^n$ is trivially always an even integer. Clearly M_n and G_n both satisfy the linear recursion $u_{n+1} = 4u_n - u_{n-1}$ with initial terms $M_0 = 1$, $M_1 = 2$, $G_0 = 0$, $G_1 = 1$. We have of course an exact analogue of Proposition 6.8.1, which is in fact slightly simpler since $\alpha\beta = 1$ instead of -1 (i.e., a fundamental unit of norm 1) and since there is no denominator 2 in α and β (the full ring of integers of $\mathbb{Q}(\sqrt{3})$ is $\mathbb{Z}[\sqrt{3}]$).

Proposition 6.8.10. (1) $M_{-n} = M_n$, $G_{-n} = -G_n$, $M_n^2 - 3G_n^2 = 1$, $M_{m+n} = 3G_mG_n + M_mM_n$, $G_{m+n} = G_mM_n + G_nM_m$, $M_{2m} = 2M_m^2 - 1$, $G_{2m} = 2G_mM_m$.

(2) $\gcd(M_n, G_n) = 1$.

(3) *For any integers* k *and* t *in* $\mathbb{Z}$ *we have*

$$M_{n+2kt} \equiv (-1)^t M_n \pmod{M_k} \quad \textit{and} \quad G_{n+2kt} \equiv (-1)^t G_n \pmod{M_k}\,.$$

Proof. Essentially identical to the proof of Proposition 6.8.1 this time using $M_n + G_n\sqrt{3} = \alpha^n$. □

Lemma 6.8.11. *Assume that n is even. Then M_n is odd, $5 \nmid M_n$, $\left(\frac{5}{M_n}\right) = 1$ if and only if $3 \mid n$ and $\left(\frac{-2}{M_n}\right) = 1$ if and only if $4 \mid n$.*

Proof. Write $n = 2m$. Since $M_{2m} = 2M_m^2 - 1$, it is clear that M_n is odd, and since $M_m^2 \equiv 0$ or ± 1 modulo 5, $M_n \equiv -1$, 1 or 2 modulo 5 and in particular $5 \nmid M_n$. Since M_n satisfies a linear recursion with integral coefficients it is periodic modulo k for any given k, and for $k = 5$ the period is clearly $(1, 2, 2)$ of length 3, and for $k = 8$ the period is $(1, 2, 7, 2)$ of length 4, leading immediately to the desired results. □

The key proposition in the proof is the following result, first proved by Ma in [Ma].

Proposition 6.8.12 (Ma). *If $n \geqslant 0$, then M_n has the form $4x^2 + 3$ if and only if $n = 2$, hence $M_n = 7$.*

Proof. Assume that $M_n = 4x^2 + 3$, so that $M_n \equiv 3$ or 7 modulo 8. Since the period of M_n modulo 8 is $(1, 2, 7, 2)$, this implies that $n \equiv 2 \pmod 4$ or, equivalently, that $n \equiv \pm 2 \pmod 8$. Assume that $n > 2$, hence that $M_n > 7$, and write $n = 2t \cdot 2^s \pm 2$ with t odd and $s \geqslant 2$ (for $n = 2$ we could not choose t odd). By Proposition 6.8.10 we have

$$M_n \equiv (-1)^t M_{\pm 2} \equiv -7 \pmod{M_{2^s}},$$

hence $4x^2 \equiv -10 \pmod{M_{2^s}}$. Since $s \geqslant 2$, M_{2^s} is odd, hence it follows that

$$\left(\frac{-2}{M_{2^s}}\right)\left(\frac{5}{M_{2^s}}\right) = \left(\frac{-10}{M_{2^s}}\right) = \left(\frac{4x^2}{M_{2^s}}\right) = 1$$

since everything is nonzero by the above lemma. On the other hand, the above lemma also tells us that $\left(\frac{-2}{M_{2^s}}\right) = 1$ since $s \geqslant 2$, and that $\left(\frac{5}{M_{2^s}}\right) = -1$ since $3 \nmid 2^s$, so we obtain a contradiction, proving the proposition. □

Thanks to this proposition we can now completely solve Lucas's problem.

Theorem 6.8.13. *The only integral solutions with $y \neq 0$ to the Diophantine equation $x(x+1)(2x+1) = 6y^2$ are $(x, y) = (1, \pm 1)$ and $(x, y) = (24, \pm 70)$.*

Proof. The case where x is even has been proved in Proposition 6.8.9. So assume that x is odd. As in the even case, since x, $x + 1$, and $2x + 1$ are pairwise coprime, x is either a square or three times a square, hence $x \not\equiv 2 \pmod 3$. Since $x + 1$ is even and the other two factors are odd, it is either twice a square or six times a square, hence $x + 1 \not\equiv 1 \pmod 3$. Thus $x \equiv 1 \pmod 3$, hence $x + 1 \equiv 2 \pmod 3$ and $2x + 1 \equiv 0 \pmod 3$. It follows that there exist pairwise coprime integers s, t, and u such that $x = s^2$, $x + 1 = 2t^2$, and $2x + 1 = 3u^2$. We thus obtain the equation

$$(6u^2+1)^2 - 3(4tu)^2 = (4x+3)^2 - 8(x+1)(2x+1) = 1\ ,$$

and since $2+\sqrt{3}$ is the fundamental unit of $\mathbb{Z}[\sqrt{3}]$, we deduce that there exists $n \in \mathbb{Z}$ such that, using the above notation:

$$6u^2 + 1 + 4tu\sqrt{3} = \pm(M_n + G_n\sqrt{3})\ .$$

In particular $M_n = \pm(6u^2+1) = 6u^2+1$, since $M_n \geqslant 0$. On the other hand $6u^2+1 = 4x+3 = 4s^2+3$, so that M_n has the form $4s^2+3$. By Ma's result above this implies that $n = \pm 2$ and $M_n = 7$, hence $s = \pm 1$ so $x = 1$, as claimed, finishing the proof of the theorem. □

6.9 Fermat's "Last Theorem" $x^n + y^n = z^n$

6.9.1 Introduction

This is certainly the most famous of all Diophantine equations. It claims that for all $n \geqslant 3$ there are no integral solutions to $x^n + y^n = z^n$ with $xyz \neq 0$. We may clearly assume that x, y and z are pairwise coprime. Furthermore, since any integer $n \geqslant 3$ is either divisible by an odd prime number or by 4, it is sufficient to prove the result for $n = 4$ and for $n = p$ an odd prime.

For $n = 2$ Fermat's equation does have solutions, which we have parametrized completely in Corollary 6.3.13, and which we restate as follows.

Proposition 6.9.1. *The general solution in $\mathbb{Z}$ to the equation $x^2 + y^2 = z^2$ is*

$$x = d(s^2 - t^2), \quad y = 2dst, \quad z = d(s^2 + t^2)\ ,$$

where s and t are coprime integers such that $s \not\equiv t \pmod 2$ and $d \in \mathbb{Z}$, or the same with x and y exchanged. Furthermore we have $\gcd(x,y) = \gcd(x,z) = \gcd(y,z) = |d|$.

Corollary 6.9.2. *The general solution of $x^2 + y^2 = z^2$ with $\gcd(x,y) = 1$ and x odd is*

$$x = s^2 - t^2, \quad y = 2st, \quad z = \pm(s^2 + t^2)\ ,$$

and the general solution of $x^2 - y^2 = z^2$ with $\gcd(x,y) = 1$ and x odd is

$$x = \pm(s^2 + t^2), \quad y = 2st, \quad z = s^2 - t^2\ ,$$

where s and t are as above.

Proof. Immediate from the above proposition and the fact that two out of three sign changes can be included in the exchange of s and t or in the exchange of s with $-s$. □

We have shown in Theorem 6.4.5 that Fermat's equation does not have any solution for $n = 3$. We will give below a slightly different proof which

has the advantage of being generalizable to all *regular* prime exponents. In Proposition 6.6.14 we have shown that the equation $x^4 + y^4 = z^2$ has no nontrivial solutions, so a fortiori Fermat's equation does not have any nontrivial solution for $n = 4$. We may thus assume that n is an odd prime.

6.9.2 General Prime n: The First Case

From now on we assume that $n = p$ is an odd prime. In the traditional attacks on Fermat's Last "Theorem" (FLT in short), one distinguishes the so-called *first case* (or FLT I) in which we assume that $p \nmid xyz$, and the *second case* (or FLT II) in which we assume that $p \mid xyz$. In the modern attack which culminated in the work of Wiles and Taylor–Wiles solving FLT completely, the distinction between these two cases is unimportant.

The first case is much easier to treat (although nobody knows a complete proof of the first case using traditional methods), and in fact using techniques in which we will not go into, it is not too difficult to give a very simple and effective *algorithm* to check FLT I. This has in fact been done on a computer for $p < 10^{18}$ at least. On the other hand the second case depends on some "luck" which in practice is always true, but cannot be proved to be the case. Thus it may be that for some p the traditional method for proving FLT II fails, in that it does not succeed in proving the result (of course since FLT II is true by Wiles, it will not find a counterexample either).

There exist several elementary but nontrivial results on FLT I. We prove two of them. A first is a straightforward p-adic approach (more precisely a congruence approach modulo p^2), and I am indebted to A. Kraus for pointing it out in an unpublished course. A second is a remarkable result due to Sophie Germain, and generalized by Wendt.

6.9.3 Congruence Criteria

We begin by the following.

Proposition 6.9.3. *The following three conditions are equivalent.*

(1) *There exists three p-adic units α, β and γ such that $\alpha^p + \beta^p = \gamma^p$ (in other words FLT I is soluble p-adically).*
(2) *There exists three integers a, b, c in $\mathbb{Z}$ such that $p \nmid abc$ with $a^p + b^p \equiv c^p \pmod{p^2}$.*
(3) *There exists $a \in \mathbb{Z}$ such that a is not congruent to 0 or -1 modulo p with $(a+1)^p \equiv a^p + 1 \pmod{p^2}$.*

Proof. From the binomial theorem it is clear that if $u \equiv 1 \pmod{p\mathbb{Z}_p}$ then $u^p \equiv 1 \pmod{p^2\mathbb{Z}_p}$. Thus if $u \equiv v \pmod{p\mathbb{Z}_p}$ and u and v are p-adic units, then $u^p \equiv v^p \pmod{p^2\mathbb{Z}_p}$. We will use this several times without further mention. Taking a, b and c to be residues modulo p of α, β and γ thus shows

that (1) implies (2). Conversely, assume (2). We would like to apply Hensel's lemma. However, the congruence is not quite good enough, so we have to do one step by hand. Let $a^p + b^p = c^p + kp^2$ for some $k \in \mathbb{Z}$, and set $d = c + kp$, so that $p \nmid d$. Then by the binomial theorem $d^p \equiv c^p + kp^2 c^{p-1} \pmod{p^3}$, so that

$$a^p + b^p - d^p \equiv kp^2(1 - c^{p-1}) \equiv 0 \pmod{p^3}$$

since $p \nmid c$. We can now apply Hensel's lemma (Proposition 4.1.37) to the polynomial $f(X) = X^p + b^p - d^p$ and to $\alpha = a$: we have $|f'(a)|_p = |pa^{p-1}|_p = 1/p$ since $p \nmid a$, while $|f(a)|_p \leqslant 1/p^3$ by the above, so $|f(a)|_p < |f'(a)|_p^2$, hence Hensel's lemma is applicable, proving (1).

Clearly (3) implies (2). Conversely, assume (2), i.e., that $c^p \equiv a^p + b^p \pmod{p^2}$ with $p \nmid abc$. In particular $c \equiv a + b \pmod{p}$. Thus, if we set $A = ba^{-1}$ modulo p, then by the above remark $A^p \equiv b^p a^{-p} \pmod{p^2}$ and $(A+1)^p \equiv c^p a^{-p} \pmod{p^2}$, so that $(A+1)^p \equiv A^p + 1 \pmod{p^2}$, proving (3) and the proposition. □

Corollary 6.9.4. *FLT I cannot be proved by congruence conditions (i.e., p-adically) if and only if condition (3) of the proposition is satisfied for some a such that $1 \leqslant a \leqslant (p-1)/2$.*

Proof. Indeed, condition (3) is invariant when we change a modulo p, and also under the change $a \mapsto p - 1 - a$, so the result is clear. □

Corollary 6.9.5. *If for all $a \in \mathbb{Z}$ such that $1 \leqslant a \leqslant (p-1)/2$ we have $(a+1)^p - a^p - 1 \not\equiv 0 \pmod{p^2}$, then the first case of FLT is true for p.*

Proof. Indeed, if $a^p + b^p = c^p$ with $p \nmid abc$ then condition (2) of the proposition is satisfied, hence by (3), as above there exists a such that $1 \leqslant a \leqslant (p-1)/2$ with $(a+1)^p - a^p - 1 \equiv 0 \pmod{p^2}$, proving the corollary. □

For instance, thanks to this corollary we can assert that FLT I is true for $p = 3$, 5, 11, 17, 23, 29, 41, 47, 53, 71, 89, 101, 107, 113, 131, 137, 149, 167, 173, 191, 197, which are the prime numbers less than 200 satisfying the condition of the corollary.

We will see below that a theorem of Wieferich (Corollary 6.9.10) says that it is sufficient to take $a = 1$ in the above corollary, in other words that FLT I is true as soon as $2^p - 2 \not\equiv 0 \mod p^2$.

6.9.4 The Criteria of Wendt and Germain

As mentioned there is another elementary and more powerful approach to FLT I, initially due to Sophie Germain, and generalized by Wendt, as follows.

Proposition 6.9.6 (Wendt). *Let $p > 2$ be an odd prime, and $k \geqslant 1$ be an integer. Assume that the following conditions are satisfied.*

(1) $k \equiv \pm 2 \pmod 6$.
(2) $q = kp + 1$ *is a prime number.*
(3) $q \nmid (k^k - 1)R(X^k - 1, (X+1)^k - 1)$, *where* $R(P, Q)$ *denotes the resultant of the polynomials* P *and* Q.

Then FLT I is valid, in other words if $x^p + y^p + z^p = 0$ *then* $p \mid xyz$.

Proof. Assume that $x^p + y^p + z^p = 0$ with $p \nmid xyz$. We may of course as usual assume that x, y, and z are pairwise coprime. We can write

$$-x^p = y^p + z^p = (y+z)(y^{p-1} - y^{p-2}z + \cdots + z^{p-1}) .$$

Clearly the two factors are relatively prime: we cannot have $p \mid (y+z)$ otherwise $p \mid x$, and if $r \neq p$ is a prime dividing both factors then $y \equiv -z \pmod r$ hence the second factor is congruent to py^{p-1} modulo r, and since $r \neq p$ we have $r \mid y$, hence $r \mid z$ contradicting the fact that y and z are coprime. Since p is odd (otherwise we would have to include signs), it follows that there exist coprime integers a and s such that $y + z = a^p$ and $y^{p-1} - y^{p-2}z + \cdots + z^{p-1} = s^p$. By symmetry, there exist b and c such that $z + x = b^p$ and $x + y = c^p$.

Consider now the prime $q = kp + 1$. The Fermat equation implies that

$$x^{(q-1)/k} + y^{(q-1)/k} + z^{(q-1)/k} \equiv 0 \pmod q .$$

I claim that $q \mid xyz$. Indeed, assume by contradiction that $q \nmid xyz$, and let $u = (x/z)^{(q-1)/k} \bmod q$, which makes sense since $q \nmid z$. Since $q \nmid x$ we have $u^k - 1 \equiv 0 \pmod q$. On the other hand $u + 1 \equiv -(y/z)^{(q-1)/k} \pmod q$, and since k is even and $q \nmid y$ we deduce that $(u+1)^k - 1 \equiv 0 \pmod q$. It follows that the polynomials $X^k - 1$ and $(X+1)^k - 1$ have the common root u modulo q, contradicting the assumption that $q \nmid R(X^k - 1, (X+1)^k - 1)$.

Thus $q \mid xyz$, and by symmetry we may assume for instance that $q \mid x$. Thus

$$\begin{aligned} 0 \equiv 2x = (x+y) + (z+x) - (y+z) &= c^p + b^p + (-a)^p \\ &= c^{(q-1)/k} + b^{(q-1)/k} + (-a)^{(q-1)/k} \pmod q . \end{aligned}$$

As above, it follows that $q \mid abc$. Since $q \mid x$ and x, y and z are pairwise coprime, we cannot have $q \mid b^p = z + x$ or $q \mid c^p = x + y$. Thus $q \mid a$. It follows that $y \equiv -z \pmod q$, hence $s^p \equiv py^{p-1} \pmod q$. On the other hand $y = (x+y) - x \equiv c^p \pmod q$, so that

$$s^{(q-1)/k} = s^p \equiv pc^{((q-1)/k)(p-1)} \pmod q ,$$

and since $q \nmid c$ we have $p \equiv d^{(q-1)/k} \pmod q$ with $d = s/c^{p-1}$ modulo q. Since a and s are coprime we have $q \nmid s$ hence $q \nmid d$, so $p^k \equiv 1 \pmod q$. Since k is even it follows that

$$1 = (-1)^k = (kp - q)^k \equiv k^k p^k \equiv k^k \pmod q ,$$

contradicting the assumption that $q \nmid k^k - 1$. □

Note that we have not used explicitly the assumption that $k \not\equiv 0 \pmod 6$. However, if $k \equiv 0 \pmod 6$ then $\exp(2i\pi/3)$ is a common root of $X^k - 1$ and $(X+1)^k - 1$ in $\mathbb{C}$, hence the resultant of these polynomials is equal to 0 (over $\mathbb{C}$, hence over any ring), so that the condition on q can never be satisfied. In other words (2) and (3) together imply (1).

A computer search shows that for every prime $p \geqslant 3$ up to very large bounds we can find an integer k satisfying the conditions of the proposition, and it can reasonably be conjectured that such a k always exists, so that in practice FLT I can always be checked thanks to this criterion.

The following is S. Germain's initial criterion:

Corollary 6.9.7. *Let $p > 2$ be an odd prime, and assume that $q = 2p+1$ is also a prime. Then FLT I is valid, in other words if $x^p + y^p + z^p = 0$ then $p \mid xyz$.*

Proof. Since for $k = 2$ we have $(k^k - 1)R(X^k - 1, (X+1)^k - 1) = -3^2$, the condition of the proposition is $q \neq 3$, which is always true. □

6.9.5 Kummer's Criterion: Regular Primes

A less elementary attack on FLT I uses algebraic number theory. It gives a result which is usually weaker than the above proposition since an infinity of p cannot be obtained by this attack. However it has the great advantage that it can be generalized to the second case FLT II, while none of the above elementary approaches can.

In the sequel, we let $\zeta = \zeta_p$ be a primitive pth root of unity in $\mathbb{C}$, we let $K = \mathbb{Q}(\zeta)$, and we recall that the ring of integers of K is equal to $\mathbb{Z}[\zeta]$. We set $\pi = 1 - \zeta$, and recall that the ideal $\pi\mathbb{Z}_K$ is a prime ideal such that $(\pi\mathbb{Z}_K)^{p-1} = p\mathbb{Z}_K$, and p is the only prime number ramified in K. The first successful attacks on FLT were based on the possibility of unique factorization in $\mathbb{Z}[\zeta]$. Unfortunately this is true for only a limited number of small values of p. With the work of E. Kummer it was realized that one could achieve the same result with the much weaker hypothesis that p does not divide the class number h_p of $\mathbb{Z}_K$. Such a prime is called a *regular* prime. Note that it is known that there are infinitely many irregular (i.e., nonregular) primes, see Proposition 9.6.17, but that it is unknown (although widely believed) that there are infinitely many regular primes. In fact, there should be a positive density equal to $1 - 1/e$ of regular primes among all prime numbers. The irregular primes below 100 are $p = 37$, 59, and 67. See Exercise 32 of Chapter 9 for an efficient regularity test.

We thus assume that p is a regular prime, i.e., that $p \nmid h_p$. The usefulness of this assumption comes from the following easy fact: if an ideal $\mathfrak{a}$ of K is such that $\mathfrak{a}^p$ is a principal ideal, then so is $\mathfrak{a}$ itself. Indeed, since p and h_p

are coprime, we can find integers u and v such that $up + vh_p = 1$, so that $\mathfrak{a} = (\mathfrak{a}^p)^u(\mathfrak{a}^{h_p})^v$. Now by assumption $\mathfrak{a}^p$ is a principal ideal, and by definition of the class group, so is $\mathfrak{a}^{h_p}$, proving our claim.

Proposition 6.9.8. *If $p \geqslant 3$ is a regular prime then FLT I holds.*

Proof. First note that if $p = 3$ and $p \nmid xyz$ we have x^3, y^3, and z^3 congruent to ± 1 modulo 9, which is impossible if $x^3 + y^3 = z^3$, so we may assume that $p \geqslant 5$. The equation $x^p + y^p = z^p$ can be written

$$(x + y)(x + \zeta y) \cdots (x + \zeta^{p-1} y) = z^p \ .$$

Since x and y are coprime, as ideals (otherwise it does not make sense since $\mathbb{Z}_K$ is not necessarily a PID) the factors on the left hand side are pairwise coprime: indeed, if some prime ideal $\mathfrak{p}$ divides $x + \zeta^i y$ and $x + \zeta^j y$ for $i \neq j$, it divides also $(\zeta^i - \zeta^j)y$ and $(\zeta^j - \zeta^i)x$, hence $\zeta^i - \zeta^j$. Thus $\mathfrak{p} = \pi$, so that $\pi \mid z$, hence $p \mid z$ contrary to our hypothesis. We thus have a product of pairwise coprime ideals which is equal to the pth power of an ideal, so that each of them is a pth power. Thus for each j we have $(x + \zeta^j y)\mathbb{Z}_K = \mathfrak{a}_j^p$ for some ideal $\mathfrak{a}_j$. By the above remark, since p is a regular prime this implies that $\mathfrak{a}_j$ itself is a principal ideal, say $\mathfrak{a}_j = \alpha_j \mathbb{Z}_K$. In particular, for $j = 1$ we can write $x + \zeta y = \alpha^p u$ with u a unit of K.

Denote complex conjugation by $\overline{\ }$. By Lemma 3.5.18, which is an immediate consequence of Kronecker's theorem on roots of unity, $u/\overline{u}$ is a root of unity, hence of the form $\eta = \pm\zeta^m$ for some m. On the other hand, since $\pi \mid (\zeta^j - \zeta^{-j})$ for all j, it is clear that for any $\beta \in \mathbb{Z}[\zeta]$ we have $\overline{\beta} \equiv \beta \pmod{\pi}$, so $\overline{\alpha} \equiv \alpha \pmod{\pi}$. Since $\pi \nmid z$, it follows that $\pi \nmid \alpha$, hence $\overline{\alpha}/\alpha \equiv 1 \pmod{\pi}$. Using the binomial expansion and the fact that $\pi^{(p-1)} \mid p\mathbb{Z}_K$, we deduce that $(\overline{\alpha}/\alpha)^p \equiv 1 \pmod{\pi^p}$. Dividing $x + \zeta y$ by its complex conjugate (and remembering that both are coprime to π), we obtain $(x+\zeta y)/(x+\zeta^{-1}y) \equiv \eta \pmod{\pi^p}$, in other words

$$x + \zeta y - \eta(x + \zeta^{-1} y) \equiv 0 \pmod{\pi^p} \ .$$

I claim that $m = 1$. Indeed, assume otherwise. If $m = 0$ we multiply the above congruence by ζ, and if $m = p - 1$ we multiply it by ζ^2, otherwise we do nothing. Thus we see that there exists a polynomial $f(T) \in \mathbb{Z}[T]$ of degree at most equal to $p-2 \geqslant 3$ (since we have assumed $p \geqslant 5$), not divisible by p, and such that $f(\zeta) \equiv 0 \pmod{\pi^p}$. Set $g(X) = f(1 - X)$. It is also of degree at most equal to $p - 2$ and not divisible by p, and $g(\pi) \equiv 0 \pmod{\pi^p}$. However it is clear that different monomials in $g(\pi)$ have valuations which are noncongruent modulo $p-1$, hence are distinct, a contradiction. It follows that $m = 1$, proving my claim. Thus $\eta = \pm\zeta$, and our congruence reads $x + \zeta y \mp (x\zeta + y) = (x \mp y)(1 \mp \zeta) \equiv 0 \pmod{\pi^p}$ hence $x \mp y \equiv 0 \pmod{p}$. We cannot have $x + y \equiv 0 \pmod{p}$, otherwise $p \mid z$. Thus $y \equiv x \pmod{p}$. We may now apply the same reasoning to the equation $(-x)^p + z^p = y^p$ and deduce

that $-z \equiv x \pmod{p}$. It follows that $0 = x^p + y^p - z^p \equiv 3x^p \pmod{p}$, and since $p \nmid x$, we obtain $p = 3$ which has been excluded and treated directly, finishing the proof of FLT I when p is a regular prime. □

For instance, the irregular primes less than or equal to 200 are $p = 37$, 59, 67, 101, 103, 131, 149, 157, so that FLT I is true up to $p = 200$ for all but those primes.

Remark. It is interesting to note that the prime numbers p for which FLT I can be proved using congruence conditions (i.e., Proposition 6.9.5) and those for which it can be proved using global methods as above (i.e., Proposition 6.9.8) are essentially independent. For instance by Proposition 6.9.5, FLT I cannot be proved by congruence conditions for $p = 7$ or $p = 13$, but since these are regular primes, FLT I follows from Proposition 6.9.8. On the other hand, since $p = 101$ and $p = 131$ are irregular primes, FLT I does not follow immediately from Proposition 6.9.8, although it does follow by congruence conditions from Proposition 6.9.5. In fact, combining the two approaches, we have thus proved FLT I for all primes $p \leqslant 200$ except for $p = 37$, 59, 67, 103, 157.

If we go up to $p = 5000$, there are 668 odd primes, and among those 279 can be solved by local considerations (Corollary 6.9.5), 407 by global considerations (Proposition 6.9.8), and 522 by one or the other. Of course, using Wendt's criterion given above (Proposition 6.9.6), all cases can be solved.

Asymptotically, it is expected (but not proved) that Corollary 6.9.5 can solve a proportion of $1 - \exp(-1/2) = 0.393\ldots$ of prime numbers, while Proposition 6.9.8 can solve a proportion of $\exp(-1/2) = 0.607\ldots$ of prime numbers, so that if they are independent one or the other can solve a proportion of $1 - \exp(-1/2) + \exp(-1) = 0.761\ldots$

6.9.6 The Criteria of Furtwängler and Wieferich

Theorem 6.9.9 (Furtwängler). *Let $p \geqslant 3$ be prime, let x, y, and z be pairwise coprime nonzero integers such that $x^p + y^p = z^p$, and assume that $p \nmid yz$. Then for every $q \mid yz$ we have $q^{p-1} \equiv 1 \pmod{p^2}$.*

Note that since x, y, and z are pairwise coprime, at most one can be divisible by p, so the condition $p \nmid yz$ can always be achieved by permuting x, y, and $-z$.

Proof. By multiplicativity, it is sufficient to prove the result for a prime number q such that $q \mid yz$, and by symmetry we may assume that $q \mid y$. Let $\zeta = \zeta_p$. As in the proof of Kummer's theorem on FLT I (Proposition 6.9.8), since x and y are coprime and $p \nmid z$ the ideals $(x + \zeta^i y)\mathbb{Z}[\zeta]$ are pth powers of ideals for all i. In particular if we set $\alpha = (x + y)^{p-2}(x + \zeta y)$, the ideal $\alpha\mathbb{Z}[\zeta]$ is a pth power. Furthermore we have $x + \zeta y = x + y + (\zeta - 1)y$, hence $\alpha = (x+y)^{p-1} + (\zeta - 1)u$ with $u = y(x+y)^{p-2} \in \mathbb{Z}$. Since $(x+y) \mid x^p + y^p = z^p$ we have $p \nmid (x + y)$, hence $(x + y)^{p-1} \equiv 1 \pmod{p}$, and in particular $\alpha \equiv$

$1+(\zeta-1)u \pmod{\mathfrak{p}^2}$, where $\mathfrak{p} = (\zeta-1)\mathbb{Z}[\zeta]$ is the unique prime ideal of $\mathbb{Q}(\zeta)$ above p. On the other hand $\zeta^{-u} = (1+(\zeta-1))^{-u} \equiv 1-(\zeta-1)u \pmod{\mathfrak{p}^2}$, so that $\zeta^{-u}\alpha \equiv 1 \pmod{\mathfrak{p}^2}$, hence $\zeta^{-u}\alpha$ is a primary element in the sense of Eisenstein reciprocity (see Definition 3.6.34, where ℓ must be replaced by p and $\mathcal{L}$ by $\mathfrak{p}$).

Since $p \nmid y$ and $q \mid y$, we have $q \neq p$, and it is immediate to check that $q \nmid \mathcal{N}(\alpha)$, since y is coprime to x and z. Thus applying Eisenstein's reciprocity law (Theorem 3.6.38) we have

$$\left(\frac{q}{\zeta^{-u}\alpha}\right)_p = \left(\frac{\zeta^{-u}\alpha}{q}\right)_p = \left(\frac{\zeta}{q}\right)_p^{-u}\left(\frac{\alpha}{q}\right)_p .$$

Since $\zeta^{-u}\alpha\mathbb{Z}[\zeta] = \mathfrak{a}^p$ for some ideal $\mathfrak{a}$, by definition we have $\left(\frac{q}{\zeta^{-u}\alpha}\right)_p = \left(\frac{q}{\mathfrak{a}}\right)_p^p = 1$ since $\left(\frac{\cdot}{\mathfrak{a}}\right)_p$ has order p. Furthermore, since $q \mid y$ we have $x+\zeta y = x+y+y(\zeta-1) \equiv x+y \pmod{q\mathbb{Z}[\zeta]}$, hence $\alpha \equiv (x+y)^{p-1} \pmod{q\mathbb{Z}[\zeta]}$. Since the value of $\left(\frac{\alpha}{q}\right)_p$ depends only on the class of α in $\mathbb{Z}[\zeta]/q\mathbb{Z}[\zeta]$, and since $(x+y)^{p-1} \equiv 1 \pmod{p}$ is trivially a primary element it follows once again from Eisenstein reciprocity that

$$\left(\frac{\alpha}{q}\right)_p = \left(\frac{(x+y)^{p-1}}{q}\right)_p = \left(\frac{q}{(x+y)^{p-1}}\right)_p = 1 ,$$

because the ideal $(x+y)\mathbb{Z}[\zeta]$ is a pth power. Combining all these relations we deduce that $\left(\frac{\zeta}{q}\right)_p^u = 1$.

Let $q\mathbb{Z}[\zeta] = \prod_{1\leqslant i\leqslant g}\mathfrak{q}_i$ be the prime ideal decomposition of q in $\mathbb{Z}[\zeta]$, so that $\mathcal{N}(\mathfrak{q}_i) = q^f$ and $g = (p-1)/f$ for some $f \mid (p-1)$. By definition, for any $\mathfrak{q} = \mathfrak{q}_i$ we have

$$\left(\frac{\zeta}{\mathfrak{q}}\right)_p \equiv \zeta^{(q^f-1)/p} \pmod{\mathfrak{q}} ,$$

and since both sides are pth roots of unity and p and q are distinct primes it follows that we have *equality* in the above congruence, hence by multiplicativity that

$$\left(\frac{\zeta}{q}\right)_p = \zeta^{g(q^f-1)/p} .$$

It follows that the identity $\left(\frac{\zeta}{q}\right)_p^u = 1$ that we have shown above is equivalent to $ug(q^f-1)/p \equiv 0 \pmod{p}$. Since $g \mid (p-1)$, $p \nmid g$, and since $p \nmid y$ and $p \nmid (x+y)$, we have $p \nmid u$. It follows that $q^f \equiv 1 \pmod{p^2}$, proving the theorem since $f \mid (p-1)$. □

Corollary 6.9.10 (Wieferich). *If FLT I for a prime exponent $p \geqslant 3$ has a nonzero solution then $2^{p-1} \equiv 1 \pmod{p^2}$.*

Proof. Indeed, if $x^p + y^p = z^p$ with $p \nmid xyz$, then exactly one of x, y, or z is even. We may thus assume that $2 \mid y$, so the result follows from the theorem. □

Remarks.

(1) The only known values of p such that $2^{p-1} \equiv 1 \pmod{p^2}$ are $p = 1093$ and $p = 3511$, and there are no others up to $1.25 \cdot 10^{15}$. On simple probabilistic grounds it is however believed that there exist infinitely many, and that their number up to X should be of the order of $\log(\log(X))$.

(2) Wieferich's criterion has been generalized by many authors, replacing 2 by larger integers, and it is by combining these criteria that FLT I has been proved by "classical" methods up to 10^{18} as has already been mentioned.

6.9.7 General Prime n: The Second Case

The second case of FLT, denoted FLT II, is more difficult for several reasons. We begin by a p-adic remark.

Proposition 6.9.11. *For every prime number ℓ there exist nonzero elements α, β and γ in $\mathbb{Z}_\ell$ such that $\alpha\beta\gamma \equiv 0 \pmod{\ell}$ and $\alpha^p + \beta^p = \gamma^p$.*

Proof. Set $F(X) = X^p + \ell^p - 1$. Assume first that $\ell \neq p$. Then $F(X) \equiv (X-1)(X^{p-1} + \cdots + 1) \pmod{\ell}$. Since $\ell \neq p$, it follows that 1 is a simple root of $F(X) \equiv 0 \pmod{\ell}$, hence by Hensel's lemma (Proposition 4.1.37) $F(X)$ has a root $\alpha \in \mathbb{Z}_\ell$, thus proving the proposition in this case with $\beta = \ell$ and $\gamma = 1$. Assume now that $\ell = p$. Then $|F(1)|_p = p^{-p}$ and $|F'(1)|_p = p^{-1}$. Since $p \geqslant 3$, we can once again conclude from Hensel's lemma that $F(X)$ has a root in $\mathbb{Z}_p$, proving the proposition. □

We keep the notation of the first case. We begin by two results of Kummer on units.

Lemma 6.9.12. *Let p be a prime number, let $\zeta = \zeta_p$ be a primitive pth root of unity, let $K = \mathbb{Q}(\zeta)$ and let $\pi = 1 - \zeta$ generate the prime ideal $\mathfrak{p}$ of $\mathbb{Z}_K$ such that $p\mathbb{Z}_K = \mathfrak{p}^{p-1}$. Let $\beta \in \mathbb{Z}_K$ be prime to $\mathfrak{p}$ and assume that the congruence $\alpha_0^p \equiv \beta \pmod{\mathfrak{p}^p}$ has a solution in $\mathbb{Z}_K$, or even in $\mathbb{Z}_\mathfrak{p}$. If $L = K(\beta^{1/p})$, then $\mathfrak{p}$ is unramified in the extension L/K.*

Proof. Assume first that $\alpha_0^p \equiv \beta \pmod{\mathfrak{p}^{p+1}}$. Since the absolute ramification index $e = e(\mathfrak{p}/p)$ is equal to $p-1$, Lemma 4.1.41 with $r = 2$ tells us that there exists a $\mathfrak{p}$-adic unit α such that $\beta = \alpha^p$. Thus the polynomial $X^p - \beta$ is totally split in $K_\mathfrak{p}$, and since by Theorem 4.4.41 the splitting of a prime ideal $\mathfrak{p}$ in L/K mimics the splitting of the defining polynomial of L/K in $K_\mathfrak{p}$, it follows that $\mathfrak{p}$ is totally split in L/K, and in particular is unramified.

Assume now that $v_{\mathfrak{p}}(\beta - \alpha_0^p) = p$. Since the statement is trivial when $L = K$, we may assume that $L \neq K$. Set $\eta = (\beta^{1/p} - \alpha_0)/\pi$, so that $L = K(\eta)$. The minimal monic polynomial $f(X)$ of η over K is

$$((\pi X + \alpha_0)^p - \beta)/\pi^p \equiv X^p + p\pi\alpha_0^{p-1}/\pi^p X + (\alpha_0^p - \beta)/\pi^p \pmod{\mathfrak{p}} .$$

Since this polynomial is monic and all its coefficients are $\mathfrak{p}$-integral (recall that p/π^{p-1} is even a $\mathfrak{p}$-adic unit), it follows that η is $\mathfrak{p}$-integral (more correctly $\mathfrak{P}$-integral for any prime ideal $\mathfrak{P}$ of L above $\mathfrak{p}$, but it is shorter to talk this way), and since the only prime ideals which can divide the denominator of η are divisors of $\mathfrak{p}$, it follows that $\eta \in \mathbb{Z}_L$. Now recall that the discriminant of η is up to sign the resultant of $f(X)$ with $f'(X)$. However since p/π^{p-1} is a $\mathfrak{p}$-adic unit, the formula above shows that for any $x \in \mathbb{Z}_L$ we have $f'(x) \equiv px^{p-1} + p/\pi^{p-1}\alpha_0^{p-1} \equiv p/\pi^{p-1}\alpha_0^{p-1} \not\equiv 0 \pmod{\mathfrak{p}}$, so that the discriminant of η is coprime to $\mathfrak{p}$. Since $L = K(\eta)$ the relative discriminant ideal of the extension L/K divides that of η, hence is prime to $\mathfrak{p}$, so that $\mathfrak{p}$ is unramified in L/K as claimed. In fact in this case it is not difficult to show that $\mathfrak{p}$ is inert in L/K. □

Corollary 6.9.13. *Let p be a regular prime, and let ε be a unit of K such that the congruence $\varepsilon \equiv \alpha^p \pmod{\pi^p}$ has a solution in $\mathbb{Z}_K$. Then $\varepsilon = u^p$ for some $u \in \mathbb{Z}_K$ (necessarily a unit).*

Proof. Assume the contrary, and consider the extension $L = K(\varepsilon^{1/p})$. Since ε is not a pth power and $\zeta \in K$ it follows that L/K is a cyclic extension of degree p (the simplest case of a Kummer extension). The relative ideal discriminant of this extension divides the discriminant of the polynomial $X^p - \varepsilon$, which is equal to $(-1)^{(p-1)/2}p^p\varepsilon^{p-1}$. Since ε is a unit, it follows that it divides $p^p\mathbb{Z}_K$, hence that $\mathfrak{p} = \pi\mathbb{Z}_K$ is the only prime ideal which can divide it. However by the above lemma, under the above conditions we know that even $\mathfrak{p}$ is unramified. Thus no finite prime can ramify in the extension L/K, and since K is totally complex, L/K is an unramified Abelian extension. Applying one of the basic results of class field theory, this tells us that L/K is a subextension of the Hilbert class field H/K. In particular, $p = [L : K]$ divides $h_p = [H : K]$, contrary to the assumption that p is a regular prime. □

The above proof using quite elementary results of class field theory is very simple. A direct proof without using class field theory would take two pages and be much more painful.

We now begin the proof of FLT II for regular primes. We will use Fermat's method of infinite descent. For this to work we need to study an equation which will descend to itself, so we will prove a stronger result.

Proposition 6.9.14. *Let $p \geqslant 3$ be a regular prime, and recall that $\pi = 1 - \zeta$ and $\mathfrak{p} = \pi\mathbb{Z}_K$. There are no solutions to $x^p + y^p = \varepsilon z^p$ with x, y, z in $\mathbb{Z}_K$, with $\mathfrak{p} \mid z$, $\mathfrak{p} \nmid xy$, and ε a unit of K. In particular FLT II holds.*

Proof. Assume the contrary. We again write the equation in the form

$$(x+y)(x+\zeta y)\cdots(x+\zeta^{p-1}y)=\varepsilon z^p\ .$$

At least one of the factors on the left must be divisible by $\mathfrak{p}$, hence all of them are. On the other hand if $\mathfrak{q}$ is any ideal of $\mathbb{Z}_K$, it is clear that if $i\neq j$, $\mathfrak{q}$ divides both $(x+\zeta^i y)\mathbb{Z}_K$ and $(x+\zeta^j y)\mathbb{Z}_K$ if and only if both $x+\zeta^i y$ and $x+\zeta^j y$ belong to $\mathfrak{q}$, which implies that πy and πx belong to $\mathfrak{q}$, hence that $\mathfrak{q}$ divides $\mathfrak{p}\mathfrak{a}$ where $\mathfrak{a}$ is the ideal GCD of $x\mathbb{Z}_K$ and $y\mathbb{Z}_K$. But conversely $\mathfrak{a}$ clearly divides both $(x+\zeta^i y)\mathbb{Z}_K$ and $(x+\zeta^j y)\mathbb{Z}_K$ and is coprime to $\mathfrak{p}$ since x and y are, so that $\mathfrak{p}\mathfrak{a}$ divides both. We have thus proved that the ideal GCD of any two distinct factors in the above product is equal to $\mathfrak{p}\mathfrak{a}$. In particular, the p residues modulo $\mathfrak{p}$ of the $(x+\zeta^j y)/\pi$ are all distinct, and since $\mathbb{Z}_K/\mathfrak{p}$ has p elements, these residues form a complete system of representatives modulo $\mathfrak{p}$. In particular exactly one of them is divisible by $\mathfrak{p}$. Changing y into $y\zeta^j$ for some j, we may assume that $\mathfrak{p}^2\mid(x+y)$. It follows that $v_\mathfrak{p}(x+\zeta^j y)=1$ for $1\leqslant j\leqslant p-1$, hence that $v_\mathfrak{p}(x+y)=p(n-1)+1$, where $n=v_\mathfrak{p}(z)$. In particular, we see that $n\geqslant 2$.

Since the product of the ideals $(x+\zeta^j y)\mathbb{Z}_K$ is the pth power of an ideal and since the GCD of any two is equal to $\mathfrak{p}\mathfrak{a}$, it follows that there exist ideals $\mathfrak{b}_j$ such that $(x+\zeta^j y)\mathbb{Z}_K=\mathfrak{p}\mathfrak{a}\mathfrak{b}_j^p$ for $0\leqslant j\leqslant p-1$. Now we know that in any ideal class there exists an integral ideal coprime to any fixed ideal. In particular, we can find an integral ideal $\mathfrak{c}_0$ belonging to the ideal class of $\mathfrak{a}^{-1}\mathfrak{b}_0^{-1}$ and coprime to $\mathfrak{p}$. We set $\mathfrak{c}=\mathfrak{a}\mathfrak{c}_0$, which is still coprime to $\mathfrak{p}$ and belongs to the ideal class of $\mathfrak{b}_0^{-1}$. Since $\mathfrak{a}\mathfrak{b}_0^p=((x+y)/\pi)\mathbb{Z}_K$ and $\mathfrak{c}\mathfrak{b}_0$ are principal ideals, it follows that $\mathfrak{a}^{-1}\mathfrak{c}^p=(\mathfrak{a}\mathfrak{b}_0^p)^{-1}(\mathfrak{c}\mathfrak{b}_0)^p$ is a principal ideal $\beta\mathbb{Z}_K$, say, and $\beta\in\mathbb{Z}_K$ since $\mathfrak{a}\mid\mathfrak{c}$. Multiplying by β/π our p equations, we obtain

$$((\beta x+\zeta^j\beta y)/\pi)\mathbb{Z}_K=(\mathfrak{c}\mathfrak{b}_j)^p\ .$$

Thus the pth power of the ideal $\mathfrak{c}\mathfrak{b}_j$ is a principal ideal, and since p is a regular prime, as in FLT I we deduce that $\mathfrak{c}\mathfrak{b}_j$ itself is a principal ideal $\alpha_j\mathbb{Z}_K$, so that for some units ε_j we have

$$\beta x+\zeta^j\beta y=\pi\varepsilon_j\alpha_j^p\ .$$

Recall that $\mathfrak{a}$ and $\mathfrak{c}$ are prime to $\mathfrak{p}$, hence β also. Since we know $v_\mathfrak{p}(x+\zeta^j y)$ for all j, we deduce that α_j is prime to $\mathfrak{p}$ for $1\leqslant j\leqslant p-1$, and that $v_\mathfrak{p}(\alpha_0)=n-1$. Adding to the equation for $j=1$ ζ times the equation for $p-1$ we obtain

$$(1+\zeta)\beta(x+y)=\pi(\varepsilon_1\alpha_1^p+\zeta\varepsilon_{p-1}\alpha_{p-1}^p)\ ,$$

and since the equation for $j=0$ gives $\beta(x+y)=\pi\varepsilon_0\alpha_0^p$, we get

$$\varepsilon_1\alpha_1^p+\zeta\varepsilon_{p-1}\alpha_{p-1}^p=(1+\zeta)\varepsilon_0\alpha_0^p\ .$$

Since $n \geqslant 2$, $v_{\mathfrak{p}}(\alpha_0) = n-1$ and $v_{\mathfrak{p}}(\alpha_j) = 0$ for $1 \leqslant j \leqslant p-1$, it follows that $\zeta\varepsilon_{p-1}\varepsilon_1^{-1} \equiv (-\alpha_1/\alpha_{p-1})^p \pmod{\mathfrak{p}^p}$. Now by the crucial Corollary 6.9.13 proved above, this implies that $\zeta\varepsilon_{p-1}\varepsilon_1^{-1} = \eta^p$ for some unit η. Note that this is really the only difficult step in the proof, the rest being quite standard and automatic. Thus, dividing by ε_1 we obtain

$$\alpha_1^p + (\eta\alpha_{p-1})^p = (1+\zeta)\varepsilon_0\varepsilon_1^{-1}\alpha_0^p \ ,$$

where we note that $(1+\zeta)\varepsilon_0\varepsilon_1^{-1}$ is a unit, for instance because $(1+\zeta)(\zeta+\zeta^3+\cdots+\zeta^{p-2}) = -1$. We have thus obtained a new solution to our Diophantine equation $x^p + y^p = \varepsilon z^p$, such that $v_{\mathfrak{p}}(z) = v_{\mathfrak{p}}(\alpha_0) = n-1$. If we had started with a solution where $v_{\mathfrak{p}}(z)$ was minimal, we would thus obtain a solution with a strictly smaller value of $v_{\mathfrak{p}}(z)$, a contradiction, proving the first statement of the proposition. In addition, if $x^p + y^p = z^p$ with $p \mid x$ for instance, we can write instead $y^p + (-z)^p = (-x)^p$, so we may always assume in FLT II that $p \mid z$, proving the second statement, hence FLT in general for a regular prime. □

Remark. Denote by h_p^+ the class number of the totally real subfield $K^+ = \mathbb{Q}(\zeta+\zeta^{-1})$ of K, of index 2. By Proposition 3.5.20, we know that $h_p^+ \mid h_p$. It can be shown with not too much extra trouble that FLT holds if the weaker condition $p \nmid h_p^+$ is satisfied. The advantage of this is that in fact we do not know of *any* p such that $p \mid h_p^+$. The hypothesis that such p do not exist is known as *Vandiver's conjecture*. It is however believed among experts that this conjecture is probably false, although the smallest counterexample may be rather large (it has been verified up to several million). The problem with this is that, although as already mentioned, there is an algorithm to verify FLT I, if one finds a p such that $p \mid h_p^+$ (a counterexample to Vandiver's conjecture) it may be that one does not know of any way to prove FLT using classical methods (i.e., not using Wiles) for that p.

6.10 An Example of Runge's Method

A good description of this method can be found in a paper by G. Walsh, see [Wals]. We will only give a typical example, and note that we will again use this method in the context of Catalan's equation, see Section 6.11. We begin by the following lemma, which is typical of Diophantine approximation techniques in which we need to bound both the denominator and the absolute value of certain coefficients.

Lemma 6.10.1. *Let $S(X) = \sum_{k\geqslant 0} s_k X^k$ be a power series with integral coefficients such that $s_0 = 1$ and not identically equal to 1, let $d \geqslant 2$ be an integer, and write $S(X)^{1/d} = \sum_{k\geqslant 0} a_k X^k$ with $a_0 = 1$. Then*

(1) *We have $D_k a_k \in \mathbb{Z}$, where $D_k = d^k \prod_{p\mid d} p^{v_p(k!)}$.*

(2) *Let k_0 be the smallest strictly positive index such that $s_{k_0} \neq 0$, and assume that there exists a prime p dividing d such that $v_p(s_{k_0}) = 0$. Then when $k_0 \mid k$ we have $v_p(a_k) = -(kv_p(d) + v_p(k!))$.*

(3) *Assume that S has a nonzero radius of convergence R in $\mathbb{C}$, and let $M = \inf_{|z|<R,\ S(z)=0} |z|$ be the infimum of the zeros of $S(z)$ in the open disk of radius R if there exists such a zero, otherwise let M be arbitrary such that $0 < M < R$, and finally let $N = \sum_{k\geqslant 0} |s_k| M^k$. Then $M \leqslant 1$, and for all k we have the inequality $|a_k| \leqslant N^{1/d} M^{-k}$.*

Proof. (1). Set $g(X) = \sum_{k\geqslant 1} s_k X^k$ and write $g(X)^j = \sum_{k\geqslant j} g_{j,k} X^k$. We have

$$S(X)^{1/d} = (1+g(X))^{1/d} = 1 + \sum_{j\geqslant 1} \binom{1/d}{j} \sum_{k\geqslant j} g_{j,k} X^k$$
$$= 1 + \sum_{k\geqslant 1} X^k \sum_{1\leqslant j\leqslant k} \binom{1/d}{j} g_{j,k} \ ,$$

so that $a_k = \sum_{1\leqslant j\leqslant k} \binom{1/d}{j} g_{j,k}$. Since $g_{j,k} \in \mathbb{Z}$, Lemma 4.2.8 implies that $D_k a_k \in \mathbb{Z}$ with $D_k = \prod_{p\mid d} p^{kv_p(d)+v_p(k!)}$, proving (1).

(2). We have $g(X) = \sum_{k\geqslant k_0} s_k X^k$, hence $g(X)^j = \sum_{k\geqslant jk_0} g_{j,k} X^k$ with $g_{j,jk_0} = s_{k_0}^j$, and $a_k = \sum_{1\leqslant j\leqslant k/k_0} \binom{1/d}{j} g_{j,k}$. By Lemma 4.2.8, if $p \mid d$ we have $v_p(\binom{1/d}{j}) = -(jv_p(d) + v_p(j!))$, which is a strictly decreasing function of j. Since $v_p(g_{k/k_0,k}) = (k/k_0)v_p(s_0) = 0$, it follows that $v_p(a_k) = -(kv_p(d) + v_p(k!))$, proving (2).

(3). First note that the series S defines an analytic function for $|z| < R$, hence $S(z)$ has only a finite number of zeros in this disc, and since $S(0) = 1$ we deduce that $0 < M < R$. I claim that $M \leqslant 1$. We consider two cases. If $S(X)$ is not a polynomial, then $s_k \neq 0$ for an infinity of k, and since $s_k \in \mathbb{Z}$ it follows that $R \leqslant 1$, hence $M < R \leqslant 1$. On the other hand, if $S(X)$ is a polynomial of degree n, say, then the product of the roots of S is equal to $(-1)^n/s_n$, and since $s_n \in \mathbb{Z}$ we have $|(-1)^n/s_n| \leqslant 1$ so at least one root must have a modulus less than or equal to 1, as claimed.

To obtain an inequality for $|a_k|$ we simply apply Cauchy's formula. If C_r denotes the circle of radius r centered at the origin, then if $r < M$ we have

$$a_k = \frac{1}{2i\pi} \int_{C_r} \frac{S(z)^{1/d}}{z^{k+1}} dz \ ,$$

since $S(z)$ has no zeros or pole in $|z| \leqslant r$, so that we can choose a fixed determination of the logarithm to define $S(z)^{1/d} = \exp(\log(S(z))/d)$. Thus

$$|a_k| \leqslant r^{-k} \left(\sup_{|z|=r} |S(z)| \right)^{1/d} \leqslant N^{1/d} r^{-k} \ .$$

Since this is true for all $r < M$ we obtain (3). □

We also need the following completely elementary lemma.

Lemma 6.10.2. *Assume that for some integer $d \geqslant 1$ and real numbers a, b and r we have the inequality $(a-r)^d < b < (a+r)^d$. Then we have $|\operatorname{sign}(r)b^{1/d} - a| < |r|$.*

Proof. If d is odd, then $a - r < b^{1/d} < a + r$ (where hereafter, $b^{1/d}$ denotes the unique dth root of b when d is odd), hence $r > 0$ and $|b^{1/d} - a| < r$. If d is even then $b > 0$ and $|a - r| < b^{1/d} < |a + r|$ (where hereafter $b^{1/d}$ denotes the unique positive dth roof of b when d is even and $b > 0$). The first inequality gives $r - b^{1/d} < a < r + b^{1/d}$. The second inequality gives $a > -r + b^{1/d}$ or $a < -r - b^{1/d}$. If $r > 0$ the inequalities $a > r - b^{1/d}$ and $a < -r - b^{1/d}$ are incompatible, hence $-r + b^{1/d} < a < r + b^{1/d}$, in other words once again $|b^{1/d} - a| < r$. If $r < 0$ the inequalities $a < r + b^{1/d}$ and $a > -r + b^{1/d}$ are incompatible, hence $r - b^{1/d} < a < -r - b^{1/d}$, in other words $|b^{1/d} + a| < |r|$. □

Proposition 6.10.3. *Let $f(X) = \sum_{0 \leqslant i \leqslant n} f_i X^i \in \mathbb{Z}[X]$ be a monic polynomial of degree n, let $r \geqslant 2$ be an integer, set $d = \gcd(r, n)$, $m = n/d$, and let $h(X)$ be the polynomial of degree m obtained by truncating the power series expansion in $1/X$ of $f(X)^{1/d}$. We assume that $f(X)$ is not identically equal to $h(X)^d$ (so that in particular $d > 1$). Let U (resp., L) be the largest (resp., smallest) real number which is a root of one of the two polynomials $g_1(X) = f(X) - (h(X) - 1/D_m)^d$ and $g_{-1}(X) = f(X) - (h(X) + 1/D_m)^d$.*

(1) *If (x, y) is an integral solution to the Diophantine equation $y^r = f(x)$ then either $L \leqslant x \leqslant U$ or x is a root of the nonzero polynomial $f(x) - h(x)^d$.*

(2) *Let k_0 be the largest index such that $k_0 < n$ with $f_{k_0} \neq 0$ (which must exist otherwise $f(X) = (X^{n/d})^d$ is a dth power), and assume that $(n - k_0) \mid m$. If in addition there exists a prime $p \mid d$ such that $v_p(f_{k_0}) = 0$ then when $x \in \mathbb{Z}$ we have $f(x) - h(x)^d \notin \mathbb{Z}$, and in particular $f(x) - h(x)^d$ has no integral roots.*

Proof. By definition of $h(x)$ we formally have $f(X)^{1/d} = h(X) + O(1/X)$ hence for $a = \pm 1$ we obtain $g_a(X) = (da/D_m)X^{n-m} + O(X^{n-m-1})$, so that the degree of $g_a(X)$ is equal to $n - m$ and the sign of its leading term is equal to a.

If $x > U$ we have $g_1(x) > 0$ and $g_{-1}(x) < 0$, in other words $(h(x) - 1/D_m)^d < f(x) < (h(x) + 1/D_m)^d$, hence by the above lemma $|f(x)^{1/d} - h(x)| < 1/D_m$. Similarly, if $x < L$ we have $\operatorname{sign}(g_1(x)) = (-1)^{n-m}$ and $\operatorname{sign}(g_{-1}(x)) = (-1)^{n-m-1}$, hence if $n - m$ is even we obtain the same conclusion, while if $n - m$ is odd we have $(h(x) + 1/D_m)^d < f(x) < (h(x) - 1/D_m)^d$, hence by the above lemma $|f(x)^{1/d} + h(x)| < 1/D_m$, and this can happen only if d is even. Thus in any case when $x > U$ or $x < L$ there exists $\varepsilon_1 = \pm 1$ such that $|f(x)^{1/d} - \varepsilon_1 h(x)| < 1/D_m$, and we have $\varepsilon_1^d = 1$.

Now let (x,y) be an integral solution to $y^r = f(x)$ with $x > U$ or $x < L$. Writing $Y = y^{r/d}$ we see that $f(x)^{1/d} = \varepsilon_2 Y \in \mathbb{Z}$ where $\varepsilon_2 = \pm 1$ is such that $\varepsilon_2^d = 1$. If we set $I = \varepsilon_2 D_m Y - \varepsilon_1 D_m h(x)$ it follows from the above inequality that $|I| < 1$. On the other hand, by Lemma 6.10.1 applied to the series $S(X) = X^n f(1/X)$ and the fact that $D_k \mid D_m$ if $k \leqslant m$, we know that $D_m h(X) \in \mathbb{Z}[X]$, hence $D_m h(x) \in \mathbb{Z}$, so $I \in \mathbb{Z}$. Since $|I| < 1$ it follows that $I = 0$, in other words $Y = \varepsilon_1 \varepsilon_2 h(x)$. Since $\varepsilon_1^d = \varepsilon_2^d = 1$ we thus have $f(x) = Y^d = h(x)^d$, so that x is a root of the nonzero polynomial $f(x) - h(x)^d$, proving (1).

For (2), let $x \in \mathbb{Z}$ be such that $f(x) - h(x)^d \in \mathbb{Z}$, hence $h(x)^d \in \mathbb{Z}$. Since $h(X) \in \mathbb{Q}[X]$, $h(x) \in \mathbb{Q}$ and $h(x)$ is an algebraic integer, hence $h(x) \in \mathbb{Z}$. However, with the notation Lemma 6.10.1, we have $h(x) = \sum_{0 \leqslant k \leqslant m} a_k x^{m-k}$, and since $k_0 \mid m$ we have by the lemma $v_p(a_m) = -(m v_p(d) + v_p(m!))$, while for $k < m$ we have

$$v_p(a_k x^{m-k}) \geqslant v_p(a_k) \geqslant -(k v_p(d) + v_p(k!)) > -(m v_p(d) + v_p(m!)) = v_p(a_m) .$$

Thus $v_p(h(x)) = v_p(a_m) < 0$, so $h(x) \notin \mathbb{Z}$, a contradiction. □

Remarks.

(1) It is easy to see that the type of reasoning used in the proposition can be generalized as soon as we are able to compute y (or some integral power of y) as a formal power series in x. This is the case, for instance, for hyperelliptic equations of the form $y^2 = f(x)$ with $f \in \mathbb{Z}[X]$, the leading term of $f(X)$ being of the form $a^2 X^{2k}$ for $a \in \mathbb{Z}$. More generally still, the method can easily be extended to equations of the form $g(y) = f(x)$, where f and g are *monic* polynomials of *noncoprime degree* (see Exercise 42).

(2) More generally, let $E \in \mathbb{Q}$ be some expression involving a possible solution to a Diophantine equation. Then we say that we use Runge's method if on the one hand we find some *analytic bound* of the form $|E| < \varepsilon$ for some small ε, say, and on the other hand if we can find an *arithmetic bound* D for the denominator of E. Then if $D\varepsilon < 1$ we deduce as above that $E = 0$, leading to very strict restrictions on the possible solution.

(3) It has not been necessary to use the bounds for a_k obtained in Lemma 6.10.1, since we can obtain much better inequalities for x directly as we have done above. In other situations however these bounds (or stronger ones obtained by similar methods) are the only available ones.

(4) Clearly this type of method can only apply to the search for *integer* solutions to Diophantine equations, and not rational solutions.

(5) The above method cannot apply to equations $y^r = f(x)$ where r and n are coprime (for instance, think of the problem of finding integral points on elliptic curves $y^2 = x^3 + ax + b$), or to such equations where f is nonmonic, with a leading term not an exact rth power (for instance, think of the "trivial" Pell equation $y^2 = dx^2 + 1$).

As an example, we have:

Corollary 6.10.4. (1) *The only integer solutions to* $y^2 = x^4+x^3+x^2+x+1$ *are* $(x,y) = (-1,\pm 1)$, $(0,\pm 1)$, *and* $(3,\pm 11)$.
(2) *The only integer solutions to* $y^2 = x^6 - x^4 + 1$ *are* $(x,y) = (\pm 2,\pm 7)$, $(x,y) = (\pm 1,\pm 1)$, *and* $(0,\pm 1)$.

Proof. For (1), we easily find that $L = -1$ and $U = 3$, and the second condition is satisfied with $k_0 = 3$. Thus we need only to look at $-1 \leqslant x \leqslant 3$ to prove the corollary, which is immediate. We leave (2) to the reader (Exercise 41). □

6.11 First Results on Catalan's Equation

I am very much indebted to Yu. Bilu and R. Schoof for help in writing this section and showing me their simplifications of the proofs of Cassels's and Ko Chao's theorems. I also invite the reader to read the notes of M. Mischler available on the Web [Mis].

6.11.1 Introduction

Catalan's conjecture, now a theorem, is the following:

Theorem 6.11.1 (Mihăilescu). *If* n *and* m *are greater than or equal to* 2 *the only nonzero integral solutions to*

$$x^m - y^n = 1$$

are $m = 2$, $n = 3$, $x = \pm 3$, $y = 2$.

This conjecture was formulated by Catalan in 1844 (see [Cat]) and received much attention. As already mentioned in Chapter 1, it was finally solved in 2002 by P. Mihăilescu. Complete proofs are available on the Web and at least two books are being written on the subject. We will prove this conjecture in two parts. First, in this section we prove the classical results of Cassels on the subject (see [Cas3]) which are essential for the final proof. Then in Chapter 16 the reader will find Mihăilescu's complete proof of the conjecture in an essentially self-contained form except that we will have to assume the validity of an important theorem of F. Thaine.

First, as for FLT we may evidently restrict ourselves to the case where m and n are prime numbers (we do not have to treat the special case n or m equal to 4 since the conjecture is enunciated also for $n = 2$ or $m = 2$). In addition the conjecture is clearly true if $m = n$, see Exercise 45.

Theorem 6.11.2. *Let* p *and* q *be distinct primes, and let* x *and* y *be nonzero integers such that* $x^p - y^q = 1$. *Then* $p = 2$, $q = 3$, $x = \pm 3$ *and* $y = 2$.

Note that we have already proved this theorem for $q = 2$ (see Proposition 6.7.13). We will prove it for $p = 2$ below (see Theorem 6.11.8).

Since we can write $y^q = (x-1)((x^p-1)/(x-1))$, we can expect as usual that each factor on the right will be close to a qth power. Indeed, first note the following.

Lemma 6.11.3. *Let p be prime, let $x \in \mathbb{Z}$ be such that $x \neq 1$, and set $r_p(x) = (x^p-1)/(x-1)$.*

(1) *If p divides one of the numbers $(x-1)$ or $r_p(x)$ it divides both.*
(2) *If $d = \gcd(x-1, r_p(x))$ then $d = 1$ or $d = p$.*
(3) *If $d = p$ and $p > 2$, then $r_p(x) \equiv p \pmod{p^2}$.*

Proof. Expanding $r_p(x) = ((x-1+1)^p - 1)/(x-1)$ by the binomial theorem we can write

$$r_p(x) = (x-1)^{p-1} + p + (x-1)\sum_{k=1}^{p-2}\binom{p}{k+1}(x-1)^{k-1}$$

and all three results of the lemma immediately follow from this and the fact that $p \mid \binom{p}{k+1}$ for $1 \leqslant k \leqslant p-2$. Note that (3) is trivially false for $p = 2$. □

Corollary 6.11.4. *Let (x, y, p, q) be such that $x^p - y^q = 1$. Then $\gcd(r_p(x), x-1) = p$ if $p \mid y$ and $\gcd(r_p(x), x-1) = 1$ otherwise.*

Proof. Since $y^q = (x-1)r_p(x)$ it follows that $p \mid y$ if and only if p divides either $x-1$ or $r_p(x)$, hence by the above lemma, if and only if $\gcd(r_p(x), x-1) = p$. □

The fundamental result of Cassels is the following.

Theorem 6.11.5 (Cassels). *Let p and q be primes, and let x and y be nonzero integers such that $x^p - y^q = 1$. Then $p \mid y$ and $q \mid x$.*

Thus the case $\gcd(r_p(x), x-1) = 1$ of the above corollary does not happen. The proof of this theorem is the object of the next subsections, but we immediately give the most important consequence.

Corollary 6.11.6. *If x and y are nonzero integers and p and q are odd primes such that $x^p - y^q = 1$ there exist nonzero integers a and b, and positive integers u and v with $q \nmid u$ and $p \nmid v$ such that*

$$x = qbu,\ x-1 = p^{q-1}a^q,\ \frac{x^p-1}{x-1} = pv^q,$$
$$y = pav,\ y+1 = q^{p-1}b^p,\ \frac{y^q+1}{y+1} = qu^p\ .$$

Proof. Since $p \mid y$, by the above corollary we have $\gcd(r_p(x), x-1) = p$, so by Lemma 6.11.3 (3) we have $r_p(x) \equiv p \pmod{p^2}$, and in particular $v_p(r_p(x)) = 1$. Thus the relation $y^q = (x-1)r_p(x)$ implies that there exist integers a and v with $p \nmid v$ such that $x - 1 = p^{q-1}a^q$, $r_p(x) = pv^q$, hence $y = pav$, and since $r_p(x) > 0$, we also have $v > 0$. This shows half of the relations of the theorem, and the other half follow by symmetry, changing (x, y, p, q) into $(-y, -x, q, p)$ and noting that p and q are odd. □

6.11.2 The Theorems of Nagell and Ko Chao

Since by Proposition 6.7.13 we know that the equation $x^p - y^q = 1$ has no solutions with $xy \neq 0$ for $q = 2$, we may assume that $q \neq 2$. The first important step, due to Nagell, is to prove Theorem 6.11.5 for $p = 2$. This will enable us to finish the proof of Catalan's conjecture in that case (or, equivalently, of the equation $y^2 = x^n + t$ with $t = 1$).

Proposition 6.11.7 (Nagell). *If x and y are nonzero integers and q is a prime such that $x^2 - y^q = 1$ then $2 \mid y$ and $q \mid x$.*

Proof. As already mentioned, we may assume that $q \neq 2$, and since $xy \neq 0$, we have $y > 0$ and we may assume $x > 0$. If y is odd, then x is even, hence $x - 1$ and $x + 1$ are coprime, and since $(x-1)(x+1) = y^q$ this means that $x - 1$ and $x + 1$ are both qth powers, which is impossible since two distinct qth powers cannot differ by 2. Thus $2 \mid y$.

Assume by contradiction that $q \nmid x$. From the equality $x^2 = (y+1)r_q(-y) = (y+1)((y^q+1)/(y+1))$ and Lemma 6.11.3, we deduce that $y + 1$ and $(y^q + 1)/(y + 1)$ (which are positive) are both squares, so we write $y + 1 = a^2$, $(y^q + 1)/(y + 1) = b^2$, hence $x = ab$, with $a > 0$, $b > 0$. In particular, since $y \neq 0$, y is not a square.

On the other hand if $\alpha = x + y^{(q-1)/2}\sqrt{y} \in \mathbb{Z}[\sqrt{y}]$, then the norm of α is equal to 1, and α is an algebraic integer, so it is a unit of the order $\mathbb{Z}[\sqrt{y}]$. By Proposition 6.3.16 we know that the group of units of a real quadratic order is equal to $\{\pm 1\}$ times an infinite cyclic group. Furthermore $\varepsilon = a + \sqrt{y}$ is clearly a fundamental unit (i.e., a generator strictly greater than 1 of the infinite cyclic group): indeed, let $\varepsilon_0 = u + v\sqrt{y}$ be the fundamental unit, so that $\varepsilon = \varepsilon_0^k$ for some k. Then $\varepsilon_0 - \overline{\varepsilon_0} = 2v\sqrt{y}$ divides $\varepsilon_0^k - \overline{\varepsilon_0^k} = 2\sqrt{y}$, hence $v \mid 1$, so $v = 1$ and $\varepsilon = \varepsilon_0$ as claimed. It follows that there exists $k > 0$ such that

$$x + y^{(q-1)/2}\sqrt{y} = (a + \sqrt{y})^k .$$

We first reduce this equation modulo y. We obtain $x \equiv a^k + ka^{k-1}\sqrt{y} \pmod{y\mathbb{Z}[\sqrt{y}]}$, in other words $y \mid a^k - x$ and $y \mid ka^{k-1}$, and since y and a are coprime, $y \mid k$. Since y is even, it follows that k is even.

We now reduce the above equality modulo a, using $x = ab \equiv 0 \pmod{a}$, and $y = a^2 - 1 \equiv -1 \pmod{a}$, so we obtain $(-1)^{(q-1)/2}\sqrt{y} \equiv y^{k/2} \equiv (-1)^{k/2}$

(mod $a\mathbb{Z}[\sqrt{y}]$), in other words $a \mid 1$, so $a = 1$, contradicting the assumption $y \neq 0$. □

We can now easily prove the theorem of Ko Chao (see [Ko]), using a proof due to E. Chein.

Theorem 6.11.8 (Ko Chao). *If q is prime there are no nonzero solutions to the equation $x^2 - y^q = 1$ apart from $(x, y) = (\pm 3, 2)$ for $q = 3$.*

Proof. We may clearly assume $q \neq 2$. Furthermore, we have proved in Corollary 6.5.3 that there are no solutions for $q = 3$ apart from the given ones. We may thus assume that $q \geqslant 5$. By Nagell's result, we know that x is odd, and we may of course assume $x > 0$. Choose $\varepsilon = \pm 1$ such that $x \equiv \varepsilon \pmod 4$. As in the proof of Corollary 6.11.6 the equality $(x - \varepsilon)(x + \varepsilon) = y^q$ with $v_2(x+\varepsilon) = 1$ implies that there exist positive integers a and b such that $x - \varepsilon = 2^{q-1}a^q$ and $x + \varepsilon = 2b^q$. Since $q \geqslant 5$ we have $a^q = (b^q - \varepsilon)/2^{q-2} < b^q$, hence $a < b$. On the other hand we have

$$(b^2 - 2\varepsilon a)\frac{b^{2q} - (2\varepsilon a)^q}{b^2 - 2\varepsilon a} = b^{2q} - (2\varepsilon a)^q = \left(\frac{x+\varepsilon}{2}\right)^2 - 2\varepsilon(x-\varepsilon) = \left(\frac{x-3\varepsilon}{2}\right)^2 .$$

By Nagell's proposition above, we know that $q \mid x$. Since $q \geqslant 5$, it follows that $q \nmid (x - 3\varepsilon)/2$, hence by Lemma 6.11.3 the two factors on the left are coprime, hence are both squares. However since we have seen above that $a < b$, and $a > 0$, we have

$$(b-1)^2 = b^2 - 2b + 1 < b^2 - 2a < b^2 < b^2 + 2a < b^2 + 2b + 1 = (b+1)^2 ,$$

which shows that $b^2 - 2\varepsilon a$ cannot be a square, a contradiction. □

6.11.3 Some Lemmas on Binomial Series

Before proceeding to the proof of Cassels's theorem below we need an arithmetic result and two analytic results. The arithmetic result is the following.

Lemma 6.11.9. *Set $w(j) = j + v_q(j!)$. Then $q^{w(j)}\binom{p/q}{j}$ is an integer not divisible by q, and $w(j)$ is a strictly increasing function of j.*

Proof. By Lemma 4.2.8 (2) (a) and (c), we know that $\binom{p/q}{j}$ is an ℓ-adic integer for $\ell \neq q$, and that its q-adic valuation is equal to $-w(j)$, proving the first assertion. Since $w(j+1) - w(j) = 1 + v_q(j+1) \geqslant 1$ the second assertion is also clear. □

The first analytic result that we need is the following.

Lemma 6.11.10. (1) *For all $x > 0$ we have $(x+1)\log(x+1) > x\log(x)$.*

(2) *Let $b \in \mathbb{R}_{>1}$. The function $(b^t+1)^{1/t}$ is a decreasing function of t from $\mathbb{R}_{>0}$ to $R_{>0}$ and the function $(b^t-1)^{1/t}$ is an increasing function of t from $\mathbb{R}_{>0}$ to $R_{>0}$.*

(3) *Assume that $q > p \in \mathbb{R}_{>0}$. If $a \in \mathbb{R}_{\geqslant 1}$ then $(a^q+1)^p < (a^p+1)^q$ and if $a \in \mathbb{R}_{>1}$ then $(a^q-1)^p > (a^p-1)^q$.*

Proof. Since $\log(x)$ is an increasing function of x and $\log(x+1) > 0$ we have $(x+1)\log(x+1) > x\log(x+1) > x\log(x)$ so (1) is clear. For (2), we note that for $\varepsilon = \pm 1$ the derivative of the logarithm of $(b^t+\varepsilon)^{1/t}$ is equal to $b^t\log(b^t) - (b^t+\varepsilon)\log(b^t+\varepsilon)$ which has the sign of $-\varepsilon$ by (1), so (2) follows. Applying the first inequality of (2) to $t = p$ and $t = q$, we deduce that $(a^q+1)^{1/q} < (a^p+1)^{1/p}$, giving the first inequality of (3) for $a > 1$, and the second follows similarly. Note that the first inequality of (3) is also trivially true if $a = 1$. □

The second analytic result that we need is more delicate.

Lemma 6.11.11. *Assume that $p > q$, set $F(t) = ((1+t)^p - t^p)^{1/q}$, let $m = \lfloor p/q \rfloor + 1$, and denote by $F_m(t)$ the sum of the terms of degree at most equal to m in the Taylor series expansion of $F(t)$ around $t = 0$. Then for all $t \in \mathbb{R}$ such that $|t| \leqslant 1/2$ we have*

$$|F(t) - F_m(t)| \leqslant \frac{|t|^{m+1}}{(1-|t|)^2} .$$

Proof. Set $G(t) = (1+t)^{p/q}$. It is clear that the Taylor coefficients of $F(t)$ and $G(t)$ around $t = 0$ are the same to order strictly less than p, and in particular to order m since $m \leqslant p/3 + 1 < p$ (since $p \geqslant 5$). In what follows, assume that $|t| < 1$. By the Taylor–Lagrange formula applied to the functions $x^{1/q}$ and $G(x)$ respectively there exist t_1 and t_2 such that

$$\begin{aligned} |F(t) - F_m(t)| &\leqslant |F(t) - G(t)| + |G(t) - F_m(t)| \\ &\leqslant \frac{|t|^p}{q} t_1^{1/q-1} + |t|^{m+1} \frac{1}{(m+1)!} G^{(m+1)}(t_2) \\ &\leqslant \frac{|t|^p}{q} t_1^{1/q-1} + |t|^{m+1} \binom{p/q}{m+1} (1+t_2)^{p/q-m-1} , \end{aligned}$$

with t_1 between $(1+t)^p$ and $(1+t)^p - t^p$, and t_2 between 0 and t. Now note that $p/q < m \leqslant p/q + 1$, so that $-1 \leqslant p/q - m < 0$ and for all $j \geqslant 1$ $0 < p/q - (m-j) = j - (m - p/q) < j$ hence

$$0 < \prod_{1 \leqslant j \leqslant m} (p/q - (m-j)) < \prod_{1 \leqslant j \leqslant m} j = m! .$$

It follows that

$$\left|\binom{p/q}{m+1}\right| = \frac{(m-p/q)}{m+1}\frac{\prod_{1\leqslant j\leqslant m}(p/q-(m-j))}{m!} \leqslant \frac{1}{m+1}\,.$$

Since $1/q-1<0$ and $p/q-m-1<0$ we must estimate t_1 and $1+t_2$ from below. If $t>0$ both $(1+t)^p$ and $(1+t)^p-t^p$ are greater than 1, so $t_1>1>1-t^p$. If $t<0$ then $(1+t)^p=(1-|t|)^p$ and $(1+t)^p-t^p=(1-|t|)^p+|t|^p>(1-|t|)^p$, so that $t_1>(1-|t|)^p$ in all cases. On the other hand we have trivially $|1+t_2|\geqslant 1-|t|$. Putting everything together we obtain

$$|F(t)-F_m(t)| \leqslant \frac{|t|^p}{q}(1-|t|)^{-p+p/q}+\frac{|t|^{m+1}}{m+1}(1-|t|)^{p/q-m-1}\,.$$

The above inequality is valid for all t such that $|t|<1$. If we assume that $|t|\leqslant 1/2$ then $|t|^{p-m-1}\leqslant(1-|t|)^{p-m-1}$ (since $m\leqslant p-1$), hence $|t|^p(1-|t|)^{-p+p/q}\leqslant|t|^{m+1}(1-|t|)^{p/q-m-1}$. It follows that

$$|F(t)-F_m(t)| \leqslant \left(\frac{1}{q}+\frac{1}{m+1}\right)|t|^{m+1}(1-|t|)^{p/q-m-1}\,.$$

Since $p/q-m-1\geqslant -2$ and $1/q+1/(m+1)\leqslant 1$ the lemma follows. □

6.11.4 Proof of Cassels's Theorem 6.11.5

We now prove Cassels's theorem saying that if p and q are primes and $x^p-y^q=1$ with $xy\neq 0$ then $q\mid x$ and $p\mid y$. We have already seen that the case $p=q$ is impossible. By Proposition 6.7.13 the case $q=2$ is impossible, and Nagell's Proposition 6.11.7 is the special case $p=2$ (in fact in this case Ko Chao's Theorem 6.11.8 shows that the only nontrivial solutions occur for $(x,y)=(\pm 3,2)$ and $q=3$). We may thus assume that p and q are distinct odd primes. It is then sufficient to prove that $p\mid y$ since when p and q are odd we can change (p,q,x,y) into $(q,p,-y,-x)$. The proof of Theorem 6.11.5 will be done by considering separately the cases $p<q$ and $p>q$. We begin by the case $p<q$ which is considerably simpler.

Proposition 6.11.12. *Let x and y be nonzero integers and p and q be odd primes such that $x^p-y^q=1$. Then if $p<q$ we have $p\mid y$.*

Proof. Assume on the contrary that $p\nmid y$. It follows from Corollary 6.11.4 that $x-1$ and $r_p(x)$ are coprime, and since their product is a qth power, they both are. We can thus write $x-1=a^q$ for some integer a, and $a\neq 0$ (otherwise $y=0$) and $a\neq -1$ (otherwise $x=0$), hence $(a^q+1)^p-y^q=1$. Consider the function $f(z)=(a^q+1)^p-z^q-1$, which is trivially a decreasing function of z. Assume first that $a\geqslant 1$. Then $f(a^p)=(a^q+1)^p-a^{pq}-1>0$ by the binomial expansion, while $f(a^p+1)=(a^q+1)^p-(a^p+1)^q-1<0$ by (3) of Lemma 6.11.10. Since f is strictly decreasing it follows that y which is such that $f(y)=0$ is not an integer, a contradiction. Similarly, assume that $a<0$,

so that in fact $a \leqslant -2$, and set $b = -a$. Then since p and q are odd $f(a^p) = (a^q+1)^p - a^{pq} - 1 = -((b^q-1)^p - b^{pq} + 1) > 0$ by the binomial expansion, while $f(a^p+1) = (a^q+1)^p - (a^p+1)^q - 1 = -((b^q-1)^p - (b^p-1)^q + 1) < 0$ again by (3) of the Lemma 6.11.10 since $b > 1$. Once again we obtain a contradiction, proving the proposition. □

The following corollary, essentially due to S. Hyyrö, will be used for the case $p > q$.

Corollary 6.11.13. *With the same assumptions as above (and in particular $p < q$) we have $|y| \geqslant p^{q-1} + p$.*

Proof. Since by the above proposition we have $p \mid y$, as in Corollary 6.11.6 we deduce that there exist integers a and v with $a \neq 0$ and $v > 0$ such that $x - 1 = p^{q-1}a^p$, $(x^p-1)/(x-1) = pv^q$ and $y = pav$. Set $P(X) = X^p - 1 - p(X-1)$. Since $P(1) = P'(1) = 0$, it follows that $(X-1)^2 \mid P(X)$, hence that $(x-1) \mid (x^p-1)/(x-1) - p = p(v^q-1)$. Since $p^{q-1} \mid x-1$ it follows that $v^q \equiv 1 \pmod{p^{q-2}}$. However the order of the multiplicative group modulo p^{q-2} is equal to $p^{q-3}(p-1)$, and since $q > p$ this is coprime to q. As usual this implies that $v \equiv 1 \pmod{p^{q-2}}$.

On the other hand, I claim that $v > 1$. Indeed, assume otherwise that $v = 1$, in other words $x^{p-1} + \cdots + x + 1 = p$. If $x > 1$ then $2^{p-1} > p$ so this is impossible. Since p and q are odd primes and $a \neq 0$ we have $|x-1| = p^{q-1}|a|^p \geqslant 9$, hence when $x \leqslant 1$ we must have in fact $z = -x \geqslant 8$. But then since $p-1$ is even we have

$$p = z^{p-1} - z^{p-2} + \cdots + 1 \geqslant z^{p-1}(z-1) \geqslant z^{p-1} \geqslant 2^{p-1} ,$$

a contradiction which proves my claim. Since $v \equiv 1 \pmod{p^{q-2}}$, it follows that $v \geqslant p^{q-2}+1$, hence $|y| = pav \geqslant pv \geqslant p^{q-1}+p$, proving the corollary. □

We now prove the more difficult case $p > q$ of Cassels's theorem.

Proposition 6.11.14. *Let x and y be nonzero integers and p and q be odd primes such that $x^p - y^q = 1$. Then if $p > q$ we have $p \mid y$.*

Proof. We keep all the notation of Lemma 6.11.11 and begin as for the case $p < q$ (Proposition 6.11.12): assuming by contradiction that $p \nmid y$ and using Corollary 6.11.4, we deduce that there exists $a \in \mathbb{Z} \setminus \{0\}$ such that $x - 1 = a^q$, hence $y^q = (a^q+1)^p - 1$, so that $y = a^p F(1/a^q)$. Thus if we set $z = a^{mq-p}y - a^{mq}F_m(1/a^q)$ we have $z = a^{mq}(F(1/a^q) - F_m(1/a^q))$. Applying Lemma 6.11.11 to $t = 1/a^q$ (which satisfies $|t| \leqslant 1/2$ since $a \neq \pm 1$) we obtain

$$|z| \leqslant \frac{|a|^q}{(|a|^q-1)^2} \leqslant \frac{1}{|a|^q - 2} \leqslant \frac{1}{|x| - 3} .$$

By Taylor's theorem we have $t^m F_m(1/t) = \sum_{0 \leqslant j \leqslant m} \binom{p/q}{j} t^{m-j}$, and by Lemma 6.11.9 $D = q^{m+v_q(m!)}$ is a common denominator of all the $\binom{p/q}{j}$

for $0 \leqslant j \leqslant m$. It follows that $Da^{mq}F_m(1/a^q) \in \mathbb{Z}$, and since $mq \geqslant p$ that $Dz \in \mathbb{Z}$. We now estimate the size of Dz. By Hyyrö's Corollary 6.11.13 (with (p,q,x,y) replaced by $(q,p,-y,-x)$) we have $|x| \geqslant q^{p-1}+q \geqslant q^{p-1}+3$, so by the above estimate for $|z|$ we have

$$|Dz| \leqslant \frac{D}{|x|-3} \leqslant q^{m+v_q(m!)-(p-1)} .$$

Now for $m \geqslant 1$ we have $v_q(m!) < m/(q-1)$, and since $m < p/q+1$ we have

$$m+v_q(m!)-(p-1) < m\frac{q}{q-1}-(p-1) = \frac{3-(p-2)(q-2)}{q-1} \leqslant 0$$

since $q \geqslant 3$ and $p \geqslant 5$ (note that it is essential that the above inequality be strict). Thus $|Dz| < 1$, and since $Dz \in \mathbb{Z}$, it follows that $Dz = 0$. However note that

$$Dz = Da^{mq-p}y - \sum_{0 \leqslant j \leqslant m} D\binom{p/q}{j} a^{q(m-j)} ,$$

and by Lemma 6.11.9 we have

$$v_q\left(\binom{p/q}{j}\right) < v_q\left(\binom{p/q}{m}\right) = v_q(D)$$

for $0 \leqslant j \leqslant m-1$, so that $0 = Dz \equiv D\binom{p/q}{m} \not\equiv 0 \pmod{q}$ by the same lemma. This contradiction finishes the proof of the proposition hence of Cassels's theorem. □

Remark. The reasoning that we have just used is a special case of Runge's method seen in Section 6.10 in a slightly different context.

We have seen that Corollary 6.11.6 summarizes the most important consequences of Cassels's theorem. For future reference, we note that Hyrrö's Corollary 6.11.13 is valid without restriction on p and q:

Proposition 6.11.15. *Let p, q be odd primes and x, y be nonzero integers such that $x^p - y^q = 1$. Then $|x| \geqslant q^{p-1}+q$ and $|y| \geqslant p^{q-1}+p$.*

Proof. Since we can change (p,q,x,y) into $(q,p,-y,-x)$, it is enough to prove the statement for y. If $p < q$, this is Hyrrö's result. Otherwise we have $p \geqslant q$, hence $p > q$ since $p \neq q$. By Cassels's Corollary 6.11.6 we have $y+1 = q^{p-1}b^p$, hence $|y| \geqslant q^{p-1}-1$. I claim that when $p > q$ we have $q^{p-1} > p^{q-1}+p$, which will prove the proposition. Indeed, set $f(x) = \log(x)/(x-1)$, so that

$$f(q)-f(p) = \frac{\log(q^{p-1})-\log(p^{q-1})}{(p-1)(q-1)} .$$

The inequality to be proved is thus equivalent to $f(q)-f(p) > \log(1+1/p^{q-2})/((p-1)(q-1))$, and since $\log(1+x) < x$ for $x > 0$, this will follow

from the inequality $f(q) - f(p) > 1/(p^{q-2}(p-1)(q-1))$. Now by the mean value theorem we have $f(q) - f(p) = (q-p)f'(c)$ for some $c \in]q,p[$. We have $f'(x) = -(x\log(x) - (x-1))/(x(x-1)^2)$, and this is easily seen to be strictly negative as soon as $x > 1$. Furthermore we easily check that $f''(x) > 0$ for $x \geqslant 2$, hence it follows that $f'(q) < f'(c) < f'(p) < 0$, hence $(q-p)f'(q) > (q-p)f'(c) > (q-p)f'(p) > 0$ since $p > q$. It is thus sufficient to prove that $(q-p)f'(p) > 1/(p^{q-2}(p-1)(q-1))$, in other words that $(p-q)(q-1)p^{q-2}(p\log(p) - (p-1))/(p(p-1)) > 1$, or

$$(p-q)(q-1)p^{q-2}\left(\frac{\log(p)}{p-1} - \frac{1}{p}\right) > 1\,.$$

Now an immediate study shows that for $x \geqslant 5$ we have $\log(x)/(x-1) > 2/x$. Since $p > q \geqslant 3$ are odd we have $p \geqslant 5$, hence

$$(p-q)(q-1)p^{q-2}\left(\frac{\log(p)}{p-1} - \frac{1}{p}\right) > 2(p-q)(q-1)p^{q-3} > 1$$

since $q \geqslant 3$, proving the proposition. □

6.12 Congruent Numbers

We give a short description of the congruent number problem, and refer to the excellent book by N. Koblitz [Kob2] which is entirely devoted to that problem.

6.12.1 Reduction to an Elliptic Curve

Recall from the introduction that a *congruent number* is an integer n which is the area of a right-angled triangle with rational sides (i.e., a Pythagorean triangle). Since an area is homogeneous of degree 2, it is clear that we can assume without loss of generality that n is squarefree. For instance, from the well-known $(3,4,5)$ triangle we deduce that $n = 6$ is a congruent number. Several problems can be asked about congruent numbers, but the most important are the following: give a criterion for determining whether or not a given number n is congruent; if it is, determine a corresponding Pythagorean triangle. Both problems are difficult, and we will say a little of what is known on both.

Proposition 6.12.1. *A number n is a congruent number if and only if there exists a rational point on the curve $y^2 = x(x^2 - n^2)$ with $y \neq 0$. More precisely, if (a,b,c) is a Pythagorean triangle of area n, then the four points $(a(a \pm c)/2, a^2(a \pm c)/2)$ and $(b(b \pm c)/2, b^2(b \pm c)/2)$ are points on the curve with nonzero y coordinate, and conversely such a point (x,y) gives rise to a Pythagorean triangle (a,b,c) of area n with $a = |y/x|$, $b = 2n|x/y|$ and $c = (x^2 + n^2)/|y|$.*

Proof. The proof consists in simple verifications: if for example $x = a(a+c)/2$, $y = a^2(a+c)/2$ and $n = ab/2$ is the area of the triangle, then

$$x(x^2-n^2) = a\frac{a+c}{2}\frac{a^2(a+c)^2-a^2b^2}{4} = \frac{a^3(a+c)}{8}(a^2+2ac+c^2-b^2)$$
$$= \frac{a^4(a+c)^2}{4} = y^2 ,$$

since $c^2 = a^2+b^2$. The other cases follow by exchanging a and b and/or changing c into $-c$ (even if this has little geometrical meaning). Conversely, if (x,y) is a rational point on the curve with $y \neq 0$ and if a, b, c are as given in the proposition, then a, b, c are strictly positive, and we have

$$a^2+b^2 = \frac{y^2}{x^2}+4n^2\frac{x^2}{y^2} = \frac{x^2-n^2}{x}+\frac{4n^2x}{x^2-n^2} = \frac{(x^2-n^2)^2+4n^2x^2}{x(x^2-n^2)}$$
$$= \frac{(x^2+n^2)^2}{y^2} = c^2 .$$

□

Thanks to this proposition, an easy computer search reveals for instance that the integers $n = 5$, 6 and 7 are congruent numbers. However, the corresponding triangles are not as simple as the one for 6: for $n = 5$ we find (for instance) the point $(x,y) = (-4,6)$, giving the triangle $(3/2, 20/3, 41/6)$; for $n = 7$ we find the point $(x,y) = (-63/16, 735/64)$, giving the triangle $(35/12, 24/5, 337/60)$, which is already a little more complicated. On the other hand, a more extended computer search does not give any solution for $n = 1$, 2 and 3, and indeed these are not congruent numbers. However this is more difficult and needs a proof. We simply give the example of $n = 1$.

Proposition 6.12.2. *The number $n = 1$ is not congruent.*

Proof. Assume by contradiction that 1 is a congruent number, so that there exists $(x.y) \in \mathbb{Q}^2$ with $y \neq 0$ such that $y^2 = x(x^2-1)$. Writing $x = p/q$ and $y = u/v$ with $\gcd(p,q) = \gcd(u,v) = 1$, we obtain $(q^4/v^2)u^2 = pq(p^2-q^2)$. Since $\gcd(u,v) = 1$, it follows that $v^2 \mid q^4$, i.e., $v \mid q^2$, so that $pq(p^2-q^2)$ is the square of an integer. Since $\gcd(p,q) = 1$, the three factors are pairwise coprime, hence they are all three squares. Writing $p = p_1^2$, $q = q_1^2$ and $p^2-q^2 = w^2$ we obtain the equation $p_1^4-q_1^4 = w^2$. By Proposition 6.6.14, we know that this equation has no nontrivial solutions. Since $q \neq 0$ hence $q_1 \neq 0$, the only possible solution is thus with $w = 0$, in other words $p = \pm q$ hence $y = 0$, a contradiction. □

6.12.2 Use of the Birch and Swinnerton-Dyer Conjecture

By Proposition 6.12.1, we know that n is a congruent number if and only if there exists a point (x,y) on the curve $y^2 = x(x^2-n^2)$ with $y \neq 0$. Such

curves are called *elliptic curves*, and are among the most beautiful objects in mathematics, certainly in number theory. Fermat noticed in the seventeenth century (in another language) that such curves, considered in projective coordinates, have an abelian *group law*, obtained simply by taking secants and tangents though known points. This observation was strengthened by Mordell in the beginning of the twentieth century who proved that this group is finitely generated, in other words isomorphic to $T \times \mathbb{Z}^r$, where T is a finite group. The group T can easily be determined. For instance for our curves it is independent of n and always isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (the elements of T are the three points with $y = 0$ together with the point at infinity of projective coordinates $(0, 1, 0)$). On the other hand the *rank* r is in general very difficult to compute. From Proposition 6.12.1 and our assertion concerning T, it is clear that n is a congruent number if and only if the rank of the corresponding elliptic curve is strictly positive. In particular, if n is congruent, i.e., if there exists a Pythagorean triangle of area n, then there exist infinitely many, obtained by taking multiples of the given one for the group law on the curve (see Exercise 43).

Luckily, the BSD conjecture predicts that the rank r should be equal to the order of vanishing at $s = 1$ of a certain natural analytic L-function attached to the elliptic curve. Unfortunately, even this conjecture does not answer the problem completely, although on a computer it does give strong indications: the reason is that it is impossible to prove (except of course in certain cases) that a certain analytic function vanishes exactly at a given point.

There is one important special case where it does give a result. Like most L-functions, the L-function of an elliptic curve satisfies a functional equation, specifically of the form $\Lambda(2 - s) = \varepsilon\Lambda(s)$, where $\Lambda(s)$ is equal to $L(s)$ times a suitable gamma and exponential factor, and $\varepsilon = \pm 1$ is the so-called *sign of the functional equation* (what else?). Thus, when $\varepsilon = -1$, we *know* that $L(1) = 0$, so that assuming the BSD conjecture we have $r > 0$, hence n is a congruent number. It is easily shown that when n is integral and squarefree (which we always assume), then $\varepsilon = -1$ if and only if $n \equiv 5$, 6 or 7 modulo 8. It follows that, assuming the conjecture, all of these numbers should be congruent, and indeed, we have seen that 5, 6 and 7 are indeed congruent.

On the other hand, when $\varepsilon = 1$, the order of vanishing of $L(s)$ at $s = 1$ is even, so assuming the conjecture the rank r should be *even*. It is in fact very often equal to 0, but not always. For instance we have $r = 0$ for $n = 1$, 2 or 3, so that these numbers are not congruent. On the other hand it can be shown that we have $r = 2$ for $n = 34$, 41 and 65 for instance (and for no other squarefree $n \leqslant 100$), so that these numbers are indeed congruent.

The most precise conjecture on the distribution of congruent numbers is thus the following, where the second part comes from random matrix theory as in the case of sums of two cubes, so is quite speculative but well supported by numerical evidence, see [Kea-Sna].

Conjecture 6.12.3. (1) *Any squarefree integer congruent to* 5, 6, *or* 7 *modulo* 8 *is a congruent number.*

(2) *Denote by* $C(X)$ *the set of squarefree integers less than or equal to* X *which are congruent to* 1, 2, *or* 3 *modulo* 8 *and which are congruent numbers. Then* $C(X)$ *has density* 0, *more precisely there exists a strictly positive constant* c *such that*

$$C(X) \sim cX^{3/4}\log(X)^{11/8} .$$

6.12.3 Tunnell's Theorem

The congruent number problem was finally completely solved by Tunnell in 1980, up to a weak form of the BSD conjecture. For this, in addition to the standard ingredients in the theory of elliptic curves and the related theory of modular forms, he used modular forms of *half-integral weight*. In fact, we will see in Chapter 10 that the theta function attached to a Dirichlet character is the prototypical example of such a form. It is impossible to enter into the details of Tunnell's proof, but we give his result:

Theorem 6.12.4 (Tunnell). *Let* n *be a squarefree natural number.*

(1) *Assume that* n *is odd. Then if* n *is a congruent number the number of solutions in* $\mathbb{Z}$ *of* $n = x^2 + 2y^2 + 8z^2$ *with* z *odd is equal to the number of solutions with* z *even.*

(2) *Assume that* n *is even. Then if* n *is a congruent number the number of solutions in* $\mathbb{Z}$ *of* $n/2 = x^2 + 4y^2 + 8z^2$ *with* z *odd is equal to the number of solutions with* z *even.*

In both cases if a weak form of the BSD conjecture holds (more precisely if $L(E,1) = 0$ *implies that* $r > 0$ *for the corresponding elliptic curve), then the converse also holds.*

The enormous advantage of this theorem is that it is very easy to check Tunnell's conditions, since we are dealing with representations by positive definite ternary forms which can easily be enumerated. In particular, it is easy (up to BSD) to make exhaustive tables of congruent numbers up to any desired reasonable limit. Thus the problem is completely solved, except of course that we must wait for the solution to the BSD conjecture to be absolutely sure. Note that this is one of the most beautiful and important conjectures in all of mathematics, and that a 1 million dollar Clay prize has been offered for its solution (see also Section 10.6).

For instance, we see from Tunnell's result what was already expected from the BSD conjecture, i.e., that the (squarefree integral) congruent numbers less than or equal to 100 are the numbers congruent to 5, 6 or 7 modulo 8 together with the three numbers $n = 34$, 41 and 65.

In the following table, which does not depend on BSD since in the range of the table we only have curves of analytic rank 0 or 1 or of proven rank 2

or 3, the entry in row numbered R and column C (with C going from 1 to 64) gives the rank of the elliptic curve corresponding to $n = R + C$, so that n is congruent if and only if the entry is at least equal to 1.

	1111111111222222222233333333334444444444555555555566666
	1234567890123456789012345678901234567890123456789012345678901234
0	0000111000001110000111110001111002001110200011100001111100011110
64	2000111000001111000111110001111100001110000011110001111100011110
128	0000111222001110200111110201111020021110000011100001111100011110
192	0200111000001111020111110021111102001110000011110001111100011110
256	2002111020001110000111110001111000201110002011100201111120011111
320	0020111002001111000111110001111120001110000011112021111100011111
384	0200111000201110000111111020111100000111002001110020111111020111111
448	0000111020001111200111110001111100001110000011110001111120011110
512	0200111000001110000111110001111202021112000011102001111100011110
576	0002111020001111000111110201111120001112000011110001111100011110
640	0002111000201112020111110001111002001110000011102001111100011110
704	0000111000001111202111110021111100001110000011110001111120011110
768	0000111220001110000111112001111000001110000011100001111100011111
832	0000111200001111020111110001111102001110000211110001111122011111
896	0000111220001110002111110001111000001110000011100001111100011111
960	0000111000001111000111112021111002011100020111100011111100011110
1024	2002111000001112000111110001111020021110000011102001111120011110
1088	0000111000001111200111112001111102001110002011110001111122011110
1152	0220111000021110200111110201111022001110002211102001111100011110
1216	2000111200001111200111112201111120021310000011110001111100011111
1280	0200111000021110000111112001111000001112200011100201111100211111
1344	0200111000001111000111110001111100201110022011112001111100011111
1408	0022111000201110000111110201111000201110200011100001111100011111
1472	0002111002021111000111110001111100001110200011110001111100011111
1536	0000111200001110000111112001111000001110000211100001111100211110
1600	0000111002001111000111112001111120201112000011112021111100211110
1664	0200111000001110000111110001111000001112200011100001111100011110
1728	0020111200001111220111110001111102001112020011110001111120011111
1792	0200111000001110000111110001111000021110000011100001111100011111
1856	0202111000001111000111110001111102001110000011110001111100011111
1920	0000111000001110002111110001111000001110000011100021111100011111
1984	0000111000201111000111112001111100021110000011110221111100011110

Congruent Numbers up to $n = 2048$

6.13 Some Unsolved Diophantine Problems

Evidently there are infinitely more unsolved Diophantine problems than there are solved ones, and we have already mentioned a few. We recall them here, and add a couple more. They all have some aesthetic value, and many people have tried to solve them.

For many other such problems, we refer to the vast literature on the subject, for instance the books by Mordell [Mor] and Guy [Guy]. Note that we do not mention other well-known problems such as Waring's problem, Goldbach's conjecture, or the twin prime conjecture, since these problems are of quite a different nature and are not tackled using the tools developed in this course.

In most cases, the reason for which the Diophantine equations are unsolved is that they reduce to finding rational points on curves or higher dimensional varieties which are of *general type*, in a suitable sense. For curves, this means curves of genus greater than or equal to 2, for surfaces it really means surfaces of general type. We have no algorithmic way of searching for

the complete set of points except in very special situations. On the other hand, if the Diophantine problem reduces to finding rational points on more special kinds of varieties, for instance curves of genus 1 or K3 surfaces, then even though we do not have real algorithms for finding rational points, we do have a lot of available methods.

Here is a small list, including some that we have already mentioned.

(1) Show that the quadratic forms $x^2+2y^2+5z^2+xz$, $x^2+3y^2+6z^2+xy+2yz$, and $x^2+3y^2+7z^2+xy+xz$ represent all odd positive integers (see Section 5.4.3). It is known that they represent all sufficiently large odd integers, but the bound is ineffective.

(2) Show that any squarefree integer congruent to 4, 6, 7, or 8 modulo 9 is a sum of two cubes of elements of $\mathbb{Q}$ (Conjecture 6.4.18).

(3) Show that an integer n is a sum of three cubes of integers if and only if $n \not\equiv 4 \pmod 9$ (it is clear that this latter condition is necessary). In addition show that there are infinitely many representations, in other words that if $n \not\equiv 4 \pmod 9$ the Diophantine equation $x^3 + y^3 + z^3 = n$ has infinitely many integer solutions (Conjecture 6.4.21).

(4) Prove that every integer is a sum of four cubes of integers, in other words that for all n the Diophantine equation $x^3 + y^3 + z^3 + t^3 = n$ has an integer solution (Dem'janenko's Theorem 6.4.25 shows that this is true when $n \not\equiv \pm 4 \pmod 9$). In fact, show that it has an integer solution with $t = x$, in other words that the equation $2x^3 + y^3 + z^3 = n$ has an integer solution (Conjecture 6.4.23).

(5) Prove that any squarefree integer n congruent to 5, 6, or 7 modulo 8 is a congruent number, in other words that the equation $y^2 = x^3 - n^2x$ has a solution in rational numbers with $y \neq 0$ (Conjecture 6.12.3). This would follow from the Birch and Swinnerton Dyer conjecture, in fact from a weak form of it.

(6) The *rational cuboid* problem: does there exist a rectangular parallelepiped all of whose sides, face diagonals and main diagonals are rational? In other words, does there exist nonzero rational numbers a, b and c such that $a^2 + b^2$, $a^2 + c^2$, $b^2 + c^2$ and $a^2 + b^2 + c^2$ are all rational squares? The answer is positive if any one condition is dropped: for instance $(a, b, c) = (44, 117, 240)$ satisfies the first three conditions but not the fourth, and $(a, b, c) = (117, 520, 756)$ satisfies the first, second, and fourth conditions, but not the third.

(7) The $4/n$ problem: is it true that for any integer $n > 1$ there exist positive integers a, b, and c such that $4/n = 1/a + 1/b + 1/c$? Note that it is very easy to find arithmetic progressions of n for which this is true other than the set of multiples of a given integer (for instance $n = 3k + 2$), that the number of counterexamples has asymptotic density zero, that the smallest counterexample, if any, is necessarily a prime number, and that for a given n there seems to be a large number of solutions a, b, c, see Exercise 46. The problem is that we do not know how to prove that

this large number is at least equal to 1! See Exercise 48 for a very similar but much easier problem.

6.14 Exercises for Chapter 6

1.

(a) Solve the Diophantine equation $y^2 = (x+1)^3 - x^3$ in integers.
(b) Solve the Diophantine equation $(x-y)^5 = x^3 - y^3$ by reducing it to the above equation.

2. Prove that for any positive integer n there exists x, y, and z such that $n = x^2 + y^2 + z^3$.

3. Let C be the curve $y^2 = x^\ell + t$ with $\ell \geqslant 3$ prime. Compute $|C(\mathbb{F}_q)|$ in characteristic 2 and ℓ and when $t = 0$ in $\mathbb{F}_q$.

4. Show that, as stated in the text, the general integral solution to $ax + by + cz = 0$ is $x = mb/\gcd(a,b) - \ell c/\gcd(a,c)$, $y = kc/\gcd(b,c) - ma/\gcd(a,b)$, $z = \ell a/\gcd(a,c) - kb/\gcd(b,c)$ for any integers k, ℓ and m.

5. Consider the parametrization given by Proposition 6.3.6. It is quite trivial to see how to obtain the values of s, t and d corresponding to the solutions $(x_0, -y_0, z_0)$ and $(-x_0, y_0, z_0)$.

(a) Find the values for s, t and d (which are unique up to a simultaneous change of sign of s and t) corresponding to the point (x_0, y_0, z_0) itself.
(b) More generally, if (x, y, z) is a solution of $Ax^2 + By^2 = Cz^2$ with the parameters s, t and d, find the corresponding parameters for the solutions $(-x, y, z)$, $(x, -y, z)$ and $(x, y, -z)$.

6. Using the particular solution $(1, 0, 1)$ to the equation $x^2 + Ny^2 = z^2$, give a complete family of disjoint parametric solutions to this equation. It will be useful to distinguish the cases N odd, $N \equiv 2 \pmod 4$, $4 \mid N$ with $v_2(N)$ even and finally $4 \mid N$ with $v_2(N)$ odd.

7. Prove that the general integral solution of $x^2 + y^2 = 2z^2$ with x and y coprime is given by $x = \pm(s^2 + 2st - t^2)$, $y = \pm(s^2 - 2st - t^2)$, $z = \pm(s^2 + t^2)$, where s and t are coprime integers of opposite parity and the $\pm$ signs are independent.

8. Let Q be an indefinite quadratic form, and with the usual Gram–Schmidt notation assume that $|\mu_{i,j}| \leqslant 1/2$ for all $j < i$. Show that $|(\mathbf{b}_i^* + \mu_{i,i-1}\mathbf{b}_{i-1}^*)^2| \geqslant (1/\gamma + 1/4)|(\mathbf{b}_{i-1}^*)^2|$ implies $|(\mathbf{b}_i^*)^2| \geqslant (1/\gamma + 1/4 - \mu_{i,i-1}^2)|(\mathbf{b}_{i-1}^*)^2|$, but that the converse is not necessarily true.

9. Let C be a cube of side a in Euclidean three-space $\mathbb{R}^3$. Assume that all the vertices of C have coordinates in $\mathbb{Z}^3$. Translating C, we assume that one of its vertices is at the origin, and we denote by (x_j, y_j, z_j) the coordinates of the 3 vertices of C adjacent to the origin.

(a) Let M be the 3×3 matrix whose rows are the (x_j, y_j, z_j). Compute explicitly MM^t.
(b) For $1 \leqslant j \leqslant 3$ let α_j be the complex number $\alpha_j = x_j + iy_j$. Deduce from (a) that $\alpha_1^2 + \alpha_2^2 + \alpha_3^2$.
(c) Find the general solution to the equation $x^2 + y^2 + z^2 = 0$ in the Euclidean ring $\mathbb{Z}[i]$, generalizing Corollary 6.3.13.
(d) Deduce finally a parametrization of triples $((x_1, y_1), (x_2, y_2), (x_3, y_3))$ of points in $\mathbb{Z}^2$ which are the orthogonal projections of cubes C as above.

(e) Give a few numerical examples of such triples.

10. Let D be a nonsquare integer (in fact rational number is sufficient). Prove that the general *rational* solution to the Diophantine equation $x^2 - Dy^2 = 1$ is given by $x = \pm(s^2 + D)/(s^2 - D)$, $y = 2s/(s^2 - D)$ for $s \in \mathbb{Q}$.

11. Let $f(X) = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$ be a polynomial with integer coefficients, $a_n \neq 0$ and $a_0 \neq 0$. If $c/d \in \mathbb{Q}$ is a root of $f(X) = 0$ with $\gcd(c, d) = 1$, show that $d \mid a_n$ and $c \mid a_0$.

12. Let S be the cubic surface with affine equation $x^3 + y^3 + z^3 = 10$, on which there is the evident point $P = (1, 1, 2)$.

(a) In view of Manin's conjecture 6.4.1, using tangents at the point P find a two parameter family of rational points on S.

(b) Show that none of these points (except the point P) have all three coordinates strictly positive.

(c) By iterating the processs starting from one of the new rational points, find a rational point on S with strictly positive coordinates other than $(1, 1, 2)$, $(1, 2, 1)$ and $(2, 1, 1)$.

13. Show that the equation $27x^3+2y^3+3z^3 = 0$ has no solutions with x, y, z integers such that $\gcd(y, z) = 1$, although the equation $x^3+2y^3+3z^3 = 0$ has an infinity of rational solutions (you may need to use the chapters on elliptic curves for this). This shows that the cubefree condition in Lemma 6.4.3 is necessary.

14. Show that an immediate corollary of Theorem 6.4.5 is the following: the equation $x^3 + cy^3 + cz^3 = 0$ has no solutions in nonzero integers when $c = 1$, 9, p or p^2 with $p \equiv 2$ or 5 modulo 9, except for $c = 4$ where it has the unique solution $(x, y, z) = (-2, 1, 1)$ (up to multiplication by a constant), and it has no solutions with $3 \mid x$ when $c = p$ or p^2 with $p \equiv 8 \pmod 9$.

15. (Taken from [Cas2].) Let p and q be prime numbers such that $p \equiv 2 \pmod 9$ and $q \equiv 5 \pmod 9$, and let $c = pq$. Theorem 6.4.5 (3) asserts that the equation $x^3+y^3+cz^3 = 0$ does not have any solutions with $3 \mid z$. The aim of this exercise is to show that it does not have any nontrivial solutions at all. For this, let ρ be a primitive cube root of unity, and set $\lambda = \rho - \rho^{-1} = \sqrt{-3}$. We will show more generally by descent that our equation has no solutions in $\mathbb{Z}[\rho]$. Without loss of generality, let (x, y, z) be a pairwise coprime solution to our equation in $\mathbb{Z}[\rho]$ with $|xyz|$ minimal.

(a) By factoring our equation, show that there exist elements α, β, γ, u, v, and w in $\mathbb{Z}[\rho]$ with u, v, and w pairwise coprime, such that either

$$x + y = \alpha u^3, \quad \rho x + \rho^{-1} y = \beta v^3, \quad \rho^{-1} x + \rho y = \gamma w^3, \quad \alpha\beta\gamma = c, \quad \text{or}$$
$$x + y = \lambda\alpha u^3, \quad \rho x + \rho^{-1} y = \lambda\beta v^3, \quad \rho^{-1} x + \rho y = \lambda\gamma w^3, \quad \alpha\beta\gamma = c\,,$$

and hence $\alpha u^3 + \beta v^3 + \gamma w^3 = 0$ and $\alpha\beta\gamma = c$ in both cases.

(b) Noting that we may multiply simultanously x, y, and z by any unit, show that without loss of generality we may assume that (α, β, γ) is a permutation of $(\pm 1, \pm 1, \pm c)$ or of $(\pm 1, \pm p, \pm q)$.

(c) As in the proof of Theorem 6.4.5 (3), prove that $u^3+pv^3+qw^3 \equiv 0 \pmod{9\mathbb{Z}[\rho]}$ is impossible with u, v, and w pairwise coprime.

(d) Prove that $|uvw| < |xyz|$, and hence deduce by descent that our equation $x^3 + y^3 + cz^3 = 0$ has no nontrivial solutions.

16.

(a) Show that one can give a more general theorem than Theorem 6.4.12 by replacing condition (1) by $c \not\equiv \pm 1 \pmod 9$ and $3 \nmid f$ (recall that this is automatic if $c \equiv \pm 3 \pmod 9$), removing condition (3), and finally replacing condition (4) by the following: for every suitable divisor $\mathfrak{b}$ of b there exists a generator α of $\mathfrak{b}^e$ such that if we set $\alpha\varepsilon^j = x_0^{(j)} + x_1^{(j)}\theta + x_2^{(j)}\theta^2$ with $x_i^{(j)} \in \mathbb{Q}$ then for all j such that $0 \leqslant j \leqslant 2$ we have $v_3(x_2^{(j)}) = 0$ when $e = 1$, or $v_3({x_1^{(j)}}^2 - 4x_0^{(j)}x_2^{(j)}) = 0$ when $e = 2$.

(b) However, show that if the equation $ax^3 + by^3 + cz^3 = 0$ is everywhere locally soluble, then the above result is not stronger than Theorem 6.4.12 (in other words conditions (1) and (3) of that theorem are satisfied), hence the result of (a) cannot give additional examples of failure of the Hasse principle.

17. Keep the assumptions of Lemma 6.4.6, but in addition assume that $c \not\equiv \pm 1 \pmod 9$, and write $c = c_1c_2^2$ with c_1 and c_2 coprime and squarefree.

(a) Show that $f = c_2$ and that 1, θ, θ^2/f is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$.

(b) Deduce that if $m \mid (u_0 + u_1\theta + u_2\theta^2)\mathbb{Z}_K$ then $m \mid \gcd(u_0, u_1, fu_2)$.

(c) If $x^3 + by^3 + cz^3 = 0$ with b and c cubefree, x, y, z pairwise coprime and $c \not\equiv \pm 1 \pmod 9$, show that with the notation of Lemma 6.4.9, for every $m \mid \mathfrak{b}_2 = b\mathbb{Z}_K/\mathfrak{b}_1$ we have $m^2 \mid b$, $m \mid f$ and for every prime $p \mid m$ then c/b is a nonzero cube modulo p.

(d) It follows that by using this as a new definition of suitable divisor of b, Theorems 6.4.10 and 6.4.12 are still valid. However, as in the preceding exercise show that if the equation is locally soluble this cannot give any additional examples of the failure of the Hasse principle.

18. In most results on the equation $x^3 + by^3 + cz^3 = 0$ given in the text we have assumed that $c \not\equiv \pm 1 \pmod 9$. Assume now that $c \equiv \pm 1 \pmod 9$. With the notation of the preceding exercise it can be shown that 1, θ, $(\theta^2 + c\theta + c_2^2)/(3c_2)$ is an integral basis of K, hence that $f = 3c_2$, and that 3 ramifies as $3\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2^2$ with $\mathfrak{p}_1 \neq \mathfrak{p}_2$ (see for instance Sections 6.4.3 and 6.4.4 of [Coh0]). Let x, y, z be pairwise coprime integers such that $x^3 + by^3 + cz^3 = 0$, where b and c are assumed cubefree.

(a) Show that if we replace the assumption $c \not\equiv \pm 1 \pmod 9$ by $3 \nmid y$ the conclusion of Theorem 6.4.10 and Proposition 6.4.11 still hold. In other words if we make this replacement and keep the other assumptions, then if $x^3 + by^3 + cz^3 = 0$ with x, y, z pairwise coprime we must have $3 \mid y$.

(b) Assume now that $3 \mid y$, hence that $c \equiv \pm 1 \pmod 9$. Show that there exist integral ideals $\mathfrak{a}_i$ and $\mathfrak{b}_i$ such that $L\mathbb{Z}_K = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{b}_1\mathfrak{a}_1^3$, $Q\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{b}_2\mathfrak{a}_2^3$, $\mathfrak{b}_1\mathfrak{b}_2 = b\mathbb{Z}_K$, $\mathfrak{a}_1\mathfrak{a}_2\mathfrak{p}_1\mathfrak{p}_2 = y\mathbb{Z}_K$, $\gcd(\mathfrak{a}_1, \mathfrak{a}_2) = \mathbb{Z}_K$, $\gcd(L\mathbb{Z}_K, Q\mathbb{Z}_K) = \mathfrak{p}_1\mathfrak{p}_2\gcd(\mathfrak{b}_1, \mathfrak{b}_2)$, $\mathfrak{p}_2 \nmid \mathfrak{a}_1\mathfrak{b}_1$, and $\mathfrak{p}_1 \nmid \mathfrak{a}_2\mathfrak{b}_2$.

(c) In addition show that the ideal $\mathfrak{b}_1$ is a suitable divisor of b such that $\mathfrak{p}_2 \nmid \mathfrak{b}_1$ and $\mathfrak{p}_1 \nmid \mathfrak{b}_2 = b\mathbb{Z}_K/\mathfrak{b}_1$.

(d) Deduce that Theorems 6.4.10 and 6.4.11 are still valid if we modify the definition of suitable divisor $\mathfrak{b}$ by adding that $\mathfrak{p}_2 \nmid \mathfrak{b}$ and $\mathfrak{p}_1 \nmid b\mathbb{Z}_K/\mathfrak{b}$.

(e) Although this is slightly stronger than the results given in the text, does this give any additional examples of the failure of the Hasse principle? (I do not know the answer to this question.)

19. Prove that if the assumptions of Theorem 6.4.12 on c are satisfied, in other words if $c \not\equiv \pm 1 \pmod 9$ and $c \not\equiv 0 \pmod 9$ (this last condition being in fact unnecessary), if the exponent of the class group of $K = \mathbb{Q}(c^{1/3})$ is equal to 1 or 2 and if the fundamental unit ε of K is such that $\varepsilon \equiv \pm 1 \pmod{3\mathbb{Z}_K}$, then in fact $c \equiv \pm 3 \pmod 9$.

20. Prove Proposition 6.4.17 by writing $x^3+y^3=(x+y)(x^2-xy+y^2)$.

21. Find parameters d, s, and t in Proposition 6.4.26 giving the solution $(w,x,y,z)=(1,6,8,-9)$ to $w^3+x^3+y^3+z^3=0$.

22. Let (a_1,a_2,a_3,a_4) be four integers satisfying $a_1^3+a_2^3+a_3^3+a_4^3=0$ with $a_i\neq -a_j$ for any (i,j).

(a) Show that there exist a (partial) parametrization of $w^3+x^3+y^3+z^3=0$ of the form

$$(w,x,y,z)=(a_1u^2+buv-a_2v^2,a_2u^2-buv-a_1v^2,\\ a_3u^2+cuv-a_4v^2,a_4u^2-cuv-a_3v^2)$$

with b and c *rational* numbers (not necessarily integers) if and only if $P=-(a_1+a_2)(a_3+a_4)$ is a square, and express b and c as a rational function of the a_i and of the square root of P.

(b) Find the parametrizations coming from the integral solutions $(3,5,4,-6)$ and $(1,-9,-10,12)$, and show that $(1,6,8,-9)$ (in any order) does not give rise to any such parametrization.

(c) By considering the integral solution $(12,86,159,-167)$, show that b is not always an integer (when b or c is not an integer one can multiply the a_i, b and c by a common denominator of b and c to obtain an integral parametrization).

(d) Give a complete parametrization of (a_1,a_2,a_3,a_4) such that $a_1^3+a_2^3+a_3^3+a_4^3=0$, P a square and $b=-a_1$, $c=-a_3$, and deduce that there exist an infinity of parametrizations as in (a).

23. Find all integral solutions to the Diophantine equation $y^2=x^3+16$.

24. Let K be a quadratic field and let $\alpha\in\mathbb{Z}_K$.

(a) Assume that K is an imaginary quadratic field of odd class number and different from $\mathbb{Q}(i)$. Show that $\alpha\overline{\alpha}$ is a square in $\mathbb{Z}$ if and only $\alpha=n\beta^2$ for some $n\in\mathbb{Z}$ and $\beta\in\mathbb{Z}_K$, thus in particular proving Lemma 6.5.6.

(b) How must this statement be modified if K is real quadratic of odd class number?

(c) Give examples showing that the result is false if $K=\mathbb{Q}(i)$ or if K does not have odd class number.

25.

(a) Find an analogue of Corollary 6.6.3 for everywhere local solubility in every completion of $K=\mathbb{Q}(i)$, with $i^2=-1$ (show for instance that the local condition at 2 is $c\equiv 1$, 2, or -3 modulo $\mathfrak{p}_2^7$, where $\mathfrak{p}_2=(1+i)\mathbb{Z}_K$).

(b) What about the field $K=\mathbb{Q}(\zeta_8)$ generated by a primitive 8th root of unity?

26. Using a descent method, find all coprime integer solutions to the Diophantine equation $x^4+y^4=2z^4$.

27. Using Corollary 6.6.10 prove that the equation $x^4+y^4=c$ with $c=7361$ has no rational solutions, although it is everywhere locally soluble by Corollary 6.6.3, and although the groups $E_c(\mathbb{Q})$ and $F_c(\mathbb{Q})$ have rank 2.

28. It follows from Proposition 5.7.3 and its proof that the equation $2y^2=x^4-17$ is everywhere locally soluble, but not globally soluble. The aim of this exercise is to give an alternate proof of this last fact.

(a) Prove that if x, y is a rational solution, there exist a, b, and c in $\mathbb{Z}$ such that $x=a/c$, $y=b/c^2$, $\gcd(a,b,c)=1$, and

$$(5a^2+17c^2+4b)(5a^2+17c^2-4b)=17(a^2+5c^2)^2\ .$$

(b) Show that $p = 2$ is the only prime which can divide both factors on the left.
(c) Deduce that for a suitable choice of signs and $e = 1$ or 2, there exist u and v in $\mathbb{Z}$ such that

$$5a^2 + 17c^2 \pm 4b = 17eu^2, \quad 5a^2 + 17c^2 \mp 4b = ev^2, \quad \text{and} \quad a^2 + 5c^2 = euv$$

(d) Show that there does not exist any solution of these equations in $\mathbb{Q}_{17}$, hence that our initial equation has no global solution.

29. Generalize Exercise 28 as follows. Assume that c is a sum of two squares, say $c = c_0^2 + c_1^2$. Using the identity

$$(ca^2 + c_0d^2 + c_1b)(ca^2 + c_0d^2 - c_1b) = c(c_0a^2 + d^2)^2$$

already used in Exercise 28, give sufficient conditions for the equation $y^2 = cx^4 - 1$ to have no rational solutions (hence for the equation $x^4 + y^2 = cz^4$ to have no nontrivial integer solutions.

30.
(a) Show that the equation $x^5 + 2y^5 + 4z^5 \equiv 0 \pmod{11}$ has no nontrivial solutions, although 11 apparently has nothing to do with the exponent or the coefficients.
(b) Show that if $p \nmid ABC$ and $p > 11$ the equation $Ax^5 + By^5 + Cz^5 = 0$ has a nontrivial solution in $\mathbb{Z}_p$.

31. Generalizing Propositions 6.7.3, 6.7.5 and 6.7.8, find the integral solutions to the Diophantine equation $y^2 = x^p + 4t$ for general p, then for $p = 3$ and $p = 5$, with the same assumptions on t as in the above propositions. As an example, find all the integral solutions to $y^2 = x^3 - 4$.

32. Assume $H(p,t)$. Prove that if $a \in A_p(t)$ then $|a| \leqslant p\sqrt{-t}/\pi$, hence that apart from the special solutions, if (x,y) is a solution to $y^2 = x^p + t$ we have $x = a^2 - t$ with $|a| \leqslant p\sqrt{-t}/\pi$. Hint: write the defining equation for $A_p(t)$ in terms of $\theta = \operatorname{atan}(\sqrt{-t}/a)$.

33. Assume $H(p,t)$. Looking now also at 3-adic valuations and using a similar reasoning to the preceding exercise, prove that if t is congruent to 3, 12, 15, 21, or 24 modulo 27 and not congruent to -1 or 3 modulo 16, or when $t \equiv 14 \pmod{24}$ there are no integer solutions to the Diophantine equation $y^2 = x^p + t$ (for these two exercises, see [Cohn1] if you need help).

34. Give explicitly 6 (resp., 16) integral points $(x,y) \in \mathbb{Z}^2$ satisfying the Diophantine equation $y^2 = x^3 + t$ for $t = -39$ (resp., $t = 17$). Note that in these cases, we have $t \equiv 1 \pmod{8}$ (and even $t > 0$ in the second). Using the techniques of Section 8.7, one can show that there are no other solutions.

35.
(a) Prove that the only roots of unity of the form $(a + \sqrt{t})/(a - \sqrt{t})$ with $a \neq 0$ obtained for $a = \pm 1$ when $t = -1$, and for $a = \pm 1$ or $a = \pm 3$ when $t = -3$.
(b) With the notation of the proof of Corollary 6.7.12, prove that if $p \geqslant 7$ we have $|u_p(a + \sqrt{t}, a - \sqrt{t})| > 1$ for the above values of t and a.

36. Assume $H(p,t)$. Using a similar reasoning to that of Proposition 6.7.13, prove that if $t \equiv 3 \pmod{4}$ with $v_2(t+1)$ odd the equation $y^2 = x^p + t$ has no integral solutions.

37. Prove Theorem 6.8.3 (1) by considering separately the cases $n \equiv 1 \pmod{4}$, $n \equiv 3 \pmod{4}$, $n \equiv 0 \pmod{6}$ and $n \equiv \pm 2 \pmod{6}$. Similarly, prove (2).

38. Using the results of Section 6.8.1, find all integral solutions to the Diophantine equations $5y^2 = x^4 + a$ for $a = \pm 1$ and $a = \pm 4$.

39. Find all integers n such that $F_n = 3x^2$ or $L_n = 3x^2$ for some $x \in \mathbb{Z}$.

40. (Bremner–Tzanakis.) Let P, Q be nonzero integers, and consider the sequence $F_n = F_n(P,Q)$ defined by $F_0 = 0$, $F_1 = 1$, and $F_{n+1} = PF_n - QF_{n-1}$. This generalizes the Fibonacci sequence which corresponds to $(P,Q) = (1,-1)$. A natural problem, which we have solved in the text for the Fibonacci sequence, is to ask for which n is $F_n(P,Q)$ a perfect square. We now ask the converse problem: given $n \geqslant 1$, for which (P,Q) can $F_n(P,Q)$ be a perfect square.

(a) Show that the answer to the direct problem is trivial when $(P,Q) = (\pm 1, 1)$ and $(\pm 2, 1)$.
(b) Show that if we do not assume $\gcd(P,Q) = 1$, there exists a solution to the inverse problem for any even n. Thus from now on we exclude the values found in (a) and we assume $\gcd(P,Q) = 1$.
(c) Give a complete parametrization of the coprime pairs (P,Q) other than that of (a) which solve the converse problem for $1 \leqslant n \leqslant 6$. See Exercise 7 of Chapter 8 for the other values of n.

41.

(a) Prove Corollary 6.10.4 (2).
(b) Show that there are 14 integer solutions (x,y) to the Diophantine equation $y^2 = x^4 - 3x^3 - 4x^2 + 2x + 4$.
(c) Show that the only integer solutions (x,y) to the Diophantine equation $y^2 = x^4 - 5x^3 - 5x^2 - 5x - 2$ are $(x,y) = (-129, \pm 16958)$, $(-1, \pm 2)$, and $(6, \pm 2)$.
(d) Show that there are 16 integer solutions (x,y) to the Diophantine equation $y^2 = x^6 - 3x^5 + 3x^4 - x^3 - 4x^2 + 4x + 1$.
(e) Find all the solutions to Diophantus's equation $y^2 = x^6 + x^2 + 1$ for which x is a rational number whose denominator is at most equal to 4 (see Section 13.3.4).

42. Try to generalize Proposition 6.10.3 to equations of the form $g(y) = f(x)$, where f is a monic polynomial of degree n, g a monic polynomial of degree d such that $d \mid n$ (for help, see for instance [Ten]).

43. Assume that (a,b,c) are the sides of a Pythagorean triangle of area n. Using the group law on the corresponding elliptic curve (more precisely the formula for doubling a point, obtained by computing the coordinates of the third point of intersection of a tangent), find another Pythagorean triangle with the same area. It is easy to show that repeating this process gives an infinite number of them.

44. Let ℓ and p be odd prime numbers. We will say that condition $C(\ell,p)$ is satisfied if there exist integers a, b and c such that the congruence $ax^\ell + by^\ell + cz^\ell \equiv 0 \pmod{p}$ has no solutions in $\mathbb{Z}$. This implies in particular that for such integers the Fermat-type equation $ax^\ell + by^\ell + cz^\ell = 0$ has no nontrivial solution in $\mathbb{Z}$. Assume that $C(\ell,p)$ is satisfied.

(a) Show that $p \equiv 1 \pmod{2\ell}$.
(b) Using the Weil bounds, show that $p \leqslant B(\ell)$, where $B(\ell)$ is an explicit function depending only on ℓ. It follows that for a given ℓ the set $E(\ell)$ of primes p such that condition $C(\ell,p)$ is satisfied is finite.
(c) Using a computer algebra system for the higher values, show that $E(3) = \emptyset$, $E(5) = \{11\}$, $E(7) = \{29, 43, 71\}$, $E(11) = \{23, 67, 89, 199, 419\}$, $E(13) = \{53, 79, 131, 157, 313, 547\}$.
(d) For $\ell = 5$, 7, 11 and 13 give explicit values of a, b and c for which one can easily prove that $ax^\ell + by^\ell + cz^\ell = 0$ has no nontrivial solution in $\mathbb{Z}$ by congruence arguments.

45. Let $m \in \mathbb{Z}_{\geqslant 2}$. Show that $x^m - y^m = 1$ is impossible in nonzero integers x and y (when for instance $x > y > 0$ prove that $x^m - y^m \geqslant m + 1$, and proceed similarly otherwise).

46. This exercise gives some easy results on the rational cuboid problem.

(a) Show that if there exists $k \equiv 3 \pmod 4$ such that $k \mid (n+4)$ then there exist positive integers a, b, and c such that $4/n = 1/a + 1/b + 1/c$ (for instance this is the case if $n \equiv 2 \pmod 3$).

(b) Deduce that if $n+4$ is *not* the sum of two integer squares, the equation has a solution (it can be shown that the number of integers $n \leqslant X$ which are sums of two squares is asymptotic to $CX/\sqrt{\log(X)}$ for a suitable constant $C > 0$, so this shows that exceptions to the rational cuboid problem, if they exist, have asymptotic density zero).

(c) Find more general criteria than (a).

(d) Assume that $4/n = 1/a+1/b+1/c$ with $a \leqslant b \leqslant c$. Prove that $n/2 < a \leqslant 3n/4$, that $an/(4a-n) < b \leqslant 2an/(4a-n)$, and deduce that for given n the number $N(n)$ of solutions is finite. More precisely, show that $N(n) \leqslant n^2 \log(n)/16 + O(n^2)$ (this bound is far from optimal).

47. Let $n \in \mathbb{Z}_{\geqslant 2}$ be an integer. Prove that there exist positive integers a and b such that $3/p = 1/a + 1/b$ if and only if not all prime divisors of n are congruent to 1 modulo 3.

48. Show that every positive rational number m/n can be written as $m/n = 1/a_1 + 1/a_2 + \cdots + 1/a_s$ for some s, with $1 \leqslant a_1 < a_2 < \cdots < a_s$. (Hint: reduce to rational numbers less than $1/N$ for some N by using the divergence of the harmonic series $\sum 1/k$, and then use induction.)

8. Diophantine Aspects of Elliptic Curves

8.1 Elliptic Curves over $\mathbb{Q}$

8.1.1 Introduction

The Hasse–Minkowski theorem implies that the existence of rational points on a curve of genus 0 can be decided by local arguments, and then the rational points have a parametrization in terms of rational functions of a single parameter $t \in \mathbb{P}_1(\mathbb{Q})$, or equivalently a pair of coprime integers (see for example Corollary 6.3.6).

On the other hand the parametrization of the group of rational points on an elliptic curve is of a more difficult kind, and we have already seen several examples where the local to global principles fail. Since it is the simplest case after curves of genus 0, the Diophantine aspects of elliptic curves have been extensively studied, and even though far from being solved, several techniques have been developed. Many proofs are quite difficult and involved, hence some of them will be omitted.

There are two main questions, and correspondingly two main theorems about Diophantine aspects of elliptic curves. The first one is the existence and structure of the set of *rational* solutions. The answer to this is that this set is an abelian group (in essence this is due to Fermat), but the more difficult theorem due to Mordell is that this group is *finitely generated*, in other words isomorphic to $E_t \times \mathbb{Z}^r$, where E_t is a finite abelian group consisting of the rational torsion points on the curve. It is very easy to compute E_t effectively. On the other hand the integer r, called the algebraic *rank* of the curve, is much more difficult to compute, and no general algorithm is known.

The second question concerns the set of *integral* points on the curve. Here the situation is more satisfactory: a theorem of C.-L. Siegel says that this set is *finite*, without giving any effective way of computing it. However, recent techniques based on Baker-type bounds due to S. David on elliptic logarithms, combined with the use of the LLL algorithm, make the search for the complete set of integral points almost automatic when (and that is of course a big "when") one knows explicitly the group of rational points, see for example the book by Smart [Sma]. We will give an outline of this method.

8.1.2 Basic Results and Conjectures

There are basically five main results and conjectures on this subject (not counting the existence of the group law, due in essence to Fermat in the seventeenth century). In increasing order of difficulty, these are the Mordell–Weil theorem, proved in the case of $\mathbb{Q}$ by Mordell in the 1920's, Siegel's theorem, proved in the 1930's, the isogeny conjecture, proved by Faltings in the 1980's together with the Mordell conjecture, the Taniyama–Shimura–Weil conjecture, proved by Wiles et al. between 1995 and 2000, and finally the Birch–Swinnerton-Dyer conjecture, still unproved.

We begin by the celebrated theorem of Mordell (or Mordell–Weil in the case of number fields).

Theorem 8.1.1 (Mordell). *Let E be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is a finitely generated abelian group. In other words the torsion subgroup $E_t(\mathbb{Q})$ of all $T \in E(\mathbb{Q})$ such that there exists a nonzero integer k such that $k \cdot T = 0$ is finite, and there exists an integer r (called the algebraic* rank*) and points $P_i \in E(\mathbb{Q})$ for $1 \leqslant i \leqslant r$ such that any point $P \in E(\mathbb{Q})$ can be written uniquely as $P = T + \sum_{1 \leqslant i \leqslant r} x_i \cdot P_i$, with $T \in E_t(\mathbb{Q})$ and the $x_i \in \mathbb{Z}$.*

The proof of this theorem is not too difficult, and we will give one below (see Theorem 8.2.7 and Corollary 8.3.8). However, an important point must be noted: it is easy to compute $E_t(\mathbb{Q})$ algorithmically (more on this below), but it is difficult (and in fact there is no rigorous algorithm known) to compute the rank r and a fortiori the generators P_i. It is conjectured that r is unbounded, and the present record is $r = 24$ (see [Mar-McM]) using a method first introduced by Mestre, see 10.

The second theorem, due to Siegel, deals with *integral points*. Here an important remark must be made. The group of rational points does not depend on the particular *model* chosen for the curve E: if we transform the equation(s) of E by a birational transformation, the structure of the group of rational points will be unchanged. This is absolutely not true for the set of integral points, which depends on the chosen model. To give an example in the even simpler case of genus 0, the curve $x^2 + y^2 = 1$ has only $(\pm 1, 0)$ and $(0, \pm 1)$ as integral points, while the $\mathbb{Q}$-isomorphic curve $x^2 + y^2 = 25$ has $(\pm 5, 0)$, $(\pm 4, \pm 3)$, $(\pm 3, \pm 4)$ and $(0, \pm 5)$ as integral points. Thus when one speaks of the set of integral points, it is always with respect to an equation or sets of equations. Furthermore, the notion of projective coordinates loses much of its meaning (when is the projective point (x, y, z) an integral point? it cannot be when x, y, and z are integral since any rational point has a representative of that form. It could be when x/z and y/z are integral, but why choose z as special coordinate?). Siegel's theorem is as follows.

Theorem 8.1.2 (Siegel). *Let $f(x, y) = 0$ be the affine equation of a non-singular plane cubic with integer coefficients. There exist only a finite number*

of pairs $(a,b) \in \mathbb{Z}^2$ *such that* $f(a,b) = 0$*, in other words the equation has only a finite number of integral points* (*possibly none*).

This theorem is fundamentally *ineffective*, in other words it does not give any bound on the size of the solutions, or even on their number. A breakthrough in these and many other types of similar subjects was made by Baker at the end of the 1960's by his results on linear forms in logarithms of algebraic numbers (see Chapter 12 for an overview). Baker's results transformed all of this type of problems into *effective* results, although with huge constants. Soon afterward it was realized that the use of lattice reduction algorithms, and in particular the LLL algorithm when it was invented, could drastically reduce these huge bounds to a point where they can be used for practical computations.

As noted in the introduction, finding integral points on an elliptic curve in practice has become a routine (if not completely trivial) task, and we will devote Section 8.7 to a detailed explanation. We will proceed as follows. We first need a finite generating system $(P_i)_{1 \leqslant i \leqslant n}$ (not necessarily a basis) of the Mordell–Weil group, and this is of course the hardest part. Second, we use Baker-type bounds on linear forms in *elliptic logarithms* (see above) to find a huge but effective upper bound on the integer coefficients x_i of the integral points expressed as a linear combination of the P_i (for the group law of the curve). Third, using the LLL algorithm in a suitable manner, possibly two or three times, we reduce the upper bound to something manageable, often less than 10, see Section 2.3.5. Fourth and final step, we explore systematically all the possible linear combinations of the P_i with coefficients up to the bound that has been found, and all the integral points will be found during this search. Of course many things must be explained, and many tricks exist to improve on the above method (see [Sma]), but the main thing to understand is that the method is quite straightforward.

To explain in more detail the other results, we now introduce the notion of *minimal model* and of *reduction* modulo a prime. By making a suitable change of variables, we may always assume that our elliptic curve is given by an equation $y^2 = x^3 + ax + b$ with a and b integral. If a prime number p does not divide the discriminant of the curve $\mathrm{disc}(E) = -16(4a^3 + 27b^2)$, it is clear that the curve obtained by taking the reduction modulo p of a and b is still an elliptic curve, i.e., is nonsingular. For those p which divide $\mathrm{disc}(E)$ the curve is singular, but we may hope that by using other changes of variables certain other p may become acceptable. The fact is that the right context in which to consider this problem is that of generalized Weierstrass equations of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

already considered in the preceding chapter.

The main result is that there exists a *minimal model* in generalized Weierstrass form with the $a_i \in \mathbb{Z}$, which among other properties has the smallest

possible discriminant. However this is not a satisfactory definition: the important property is that if p divides this minimal discriminant then whatever birational transformation is applied, the equation of the curve will remain singular at p. It is to be noted that the existence of a minimal model is due in large part (but not only) to the fact that $\mathbb{Z}$ is a principal ideal domain. An elliptic curve over a number field of class number strictly greater than 1 does not always have a global minimal model.

Let E be given by a minimal Weierstrass equation. We now introduce the global L function of E. When p does not divide the (minimal) discriminant of E, the reduction of E modulo p is nonsingular hence defines an elliptic curve over $\mathbb{F}_p$. We have seen in Section 7.3.4 how to define $L_p(E,T)$ in that case. When p does divide the minimal discriminant, we must proceed a little differently. The singularity of the curve is necessarily unique, and by Proposition 7.1.4 (which can easily be extended to more general equations) it can come in one of three types. Assume for simplicity that the equation is $y^2 = x^3+a_2x^2+a_4x+a_6$ as in the proposition. The only possible singularity is at a point $P_0 = (x_0, 0)$, where x_0 is a multiple root of the third degree polynomial. If P_0 is a cusp (resp., a double point with distinct tangents defined over K, resp., a double point with distinct tangents not defined over K), in other words if we have additive (resp., split multiplicative, resp., nonsplit multiplicative) reduction, we set $L_p(E,T) = 1$ (resp., $L_p(E,T) = 1/(1-T)$, resp., $L_p(E,T) = 1/(1+T)$). By the example following Proposition 7.1.4, these three formulas can be unified using the single formula $L_p(E,T) = 1/(1-a_pT)$, where as usual $a_p = p+1-|E(\mathbb{F}_p)|$. Thus for *all* primes p we can write

$$L_p(E,T) = \frac{1}{1-a_pT+\chi(p)pT^2} ,$$

where $\chi(p) = 1$ if p is a prime of good reduction, and $\chi(p) = 0$ otherwise.

Now that we have all the local L-functions, the global L-function of E is defined as the Euler product

$$L(E,s) = \prod_p L_p(E,p^{-s}) = \prod_p \frac{1}{1-a_pp^{-s}+\chi(p)p^{1-2s}} ,$$

which gives of course a Dirichlet series $L(E,s) = \sum_{n\geqslant 1} a_n n^{-s}$ by expanding. Hasse's inequality immediately implies that the above Euler product (as well as the Dirichlet series) is absolutely convergent for $\Re(s) > 3/2$. The third important result on elliptic curves is the following:

Theorem 8.1.3. *Let E and E' be two elliptic curves defined over $\mathbb{Q}$. If E and E' are isogenous over $\mathbb{Q}$ then $L(E,s) = L(E',s)$, and conversely, if $L(E,s) = L(E',s)$ then E and E' are isogenous over $\mathbb{Q}$.*

The first part of this theorem is not too difficult, but the converse (known previously as the *isogeny conjecture*) is a deep theorem of Faltings, proved

in the same paper as the proof of Mordell's conjecture. Note that this this theorem is mainly important for theoretical reasons.

The fourth important theorem on elliptic curves over $\mathbb{Q}$ is the extremely difficult and famous result of Wiles et al. (which, by using an older but also highly nontrivial result of Ribet, implies FLT, see Chapter 15 for details) proving the Taniyama–Shimura–Weil conjecture, and which states the following.

Theorem 8.1.4 (Wiles et al.). *The function $L(E,s)$ has an analytic continuation to the whole complex plane into a holomorphic function. Furthermore there exists a positive integer N (which has the same prime divisors as the discriminant* $\mathrm{disc}(E)$ *of a minimal model, and which divides it), called the* conductor *of the curve, such that if we set*

$$\Lambda(E,s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)\ ,$$

then Λ satisfies the functional equation $\Lambda(E,2-s) = \varepsilon(E)\Lambda(E,s)$, where $\varepsilon(E) = \pm 1$.

The number $\varepsilon(E)$ is of course called the sign of the functional equation, and also the *root number*. It is to be noted that there exists a tedious but easy algorithm due to Tate for computing the minimal model and the conductor (see for example [Coh0]). There exists a more recent and even more tedious algorithm for computing $\varepsilon(E)$, due to Mestre–Henniart and Halberstadt.

Another way to state the above theorem which is useful for computation is the following. For lack of space we cannot give the definition and properties of modular forms, but we will come back to them in Chapter 15.

Theorem 8.1.5. *There exists a modular cusp form f of weight 2 for $\Gamma_0(N)$ which is a Hecke eigenform for all Hecke operators (in other words a newform), such that the L function $L(f,s)$ is equal to $L(E,s)$.*

We will also need the following property of the conductor, which we of course assume since we have not defined it.

Proposition 8.1.6. *Let E be an elliptic curve defined over $\mathbb{Q}$, let N be its conductor, let p be a prime number, and denote by $\overline{E}$ the reduction modulo p of a minimal model of E, considered as a curve over $\mathbb{F}_p$. Then $p \mid N$ if and only if $\overline{E}$ is singular, $p^2 \mid N$ if and only if the singularity of $\overline{E}$ is a cusp (i.e., additive reduction), hence $p \| N$ if and only if the singularity of $\overline{E}$ is a node (i.e., multiplicative reduction).*

The fifth and last important aspect of the theory of elliptic curves over $\mathbb{Q}$ is unfortunately in a conjectural state: it is the conjecture of Birch and Swinnerton-Dyer (BSD for short). As mentioned elsewhere, in the author's opinion it is the most beautiful and important conjecture in the whole of number theory (together with analogous or more general conjectures of the same type), and probably in the whole of mathematics.

Conjecture 8.1.7. *Let E be an elliptic curve defined over $\mathbb{Q}$. The algebraic rank r defined by Mordell's theorem is equal to the order of vanishing of $L(E,s)$ at $s=1$. More precisely,*

$$\lim_{s\to 1}\frac{L(E,s)}{(s-1)^r}=\frac{L^{(r)}(E,1)}{r!}=\omega_1(E)\frac{|Ш(E)|R(E)c_\infty(E)\prod_{p|N}c_p(E)}{|E_t(\mathbb{Q})|^2}\,,$$

where $\omega_1(E)$ is the real period of E, $Ш(E)$ is the so-called Tate–Shafarevitch group of E, $R(E)$ is the regulator of E, and the $c_p(E)$ are small integers called the Tamagawa numbers, where $c_\infty(E)$ is the number of connected components of $E(\mathbb{R})$, and $c_p(E)$ is an analogous quantity corresponding to $E(\mathbb{Q}_p)$.

The real period $\omega_1(E)$ has been defined in Section 7.3.2, but we will not give here the definition of $Ш(E)$ and $R(E)$, which will be (partially) introduced when necessary. The main point to note is that all the quantities on the right hand side are in principle computable (although there is no known *algorithm* to compute $R(E)$), except for $Ш(E)$ which is not even known to be finite in general, except when $r\leqslant 1$. See Section 8.5.6 for an example.

Because of this conjecture the order of $L(E,s)$ at $s=1$ is called the *analytic rank*, and the main statement of the conjecture is that it is equal to the ordinary (or algebraic) rank.

The main results concerning this conjecture are due to Coates–Wiles, Gross–Zagier, Kolyvagin, Rubin and others. A weak but sufficient form of the known results is the following:

Theorem 8.1.8 (Kolyvagin et al.). *Let E be an elliptic curve defined over $\mathbb{Q}$. Then*

(1) *If the analytic rank is equal to 0, in other words if $L(E,1)\neq 0$, then $r=0$.*
(2) *If the analytic rank is equal to 1, in other words if $L(E,1)=0$ and $L'(E,1)\neq 0$, then $r=1$.*
(3) *In both of these cases, $Ш(E)$ is finite and the BSD conjecture is valid up to a controlled rational factor.*

Remark. Note that it is easy to check numerically that a given quantity such as $L(E,1)$ or $L'(E,1)$ is *non*zero, but that it is impossible in general to prove numerically that a certain quantity is *equal* to 0. Thus, when we say that $L(E,1)=0$, we mean in fact that the sign of the functional equation $\varepsilon(E)$ is equal to -1 (which can be checked algorithmically), so that indeed $L(E,1)=0$. We also have:

Corollary 8.1.9. *Let E be an elliptic curve defined over $\mathbb{Q}$, let r be its (algebraic) rank, denote by r_{an} its analytic rank, and let $\varepsilon(E)$ the sign of the functional equation. Then*

(1) *If $r\geqslant 2$, then $r_{an}\geqslant 2$.*

(2) *If* $r = 2$, $\varepsilon(E) = 1$, *and* $L''(E,1) \neq 0$, *then* $r_{an} = 2$.
(3) *If* $r = 3$, $\varepsilon(E) = -1$, *and* $L'''(E,1) \neq 0$, *then* $r_{an} = 3$.

Proof. Immediate and left to the reader (Exercise 1). □

Notwithstanding this corollary, which is in fact a restatement of the theorem, one can reasonably say that nothing is known on the BSD conjecture when the analytic rank is greater than or equal to 2, even for a single curve.

Let us give two examples. To be able to find explicit lower bounds for the class number of imaginary quadratic fields, Goldfeld had shown long ago that it would be sufficient to find an L-function with suitable properties, and having a zero of order at least 3 at $s = 1$. The L-functions attached to modular elliptic curves over $\mathbb{Q}$ (at the time it was not known that all elliptic curves over $\mathbb{Q}$ are modular by Wiles et al.) do satisfy the necessary properties, but there remained to prove that one has a zero of order at least 3. The above corollary tells us that to find such an L-function it is enough to find an elliptic curve of rank at least 3, which is very easy. For instance there exists a curve of rank 3 of conductor 5077 (and thanks to the work of Cremona, it is known that this is the smallest conductor), see Section 8.5.6 for more properties of this curve. To prove that the L function has a zero of order 3 is immediate since we can compute algorithmically the sign of the functional equation, which is equal to -1 (it better be, otherwise BSD is false!), and using the methods of Section 8.5.3 it is also easy to compute numerically that $L'''(E,1) \neq 0$.

As a second example, let E be an elliptic curve of algebraic rank 4 and $\varepsilon(E) = 1$ (infinite families of such curves are known). Then $L'(E,1) = L'''(E,1) = 0$ because of the functional equation, $r_{an} \geqslant 2$ hence in particular $L(E,1) = 0$ thanks to the corollary, and a numerical computation easily shows that $L''''(E,1) \neq 0$. The BSD conjecture implies that $L''(E,1) = 0$. This can easily be checked numerically to as many decimals as one likes, but nobody has any idea how to prove this. In fact if it could be proved in a single instance, it would be an exceedingly important advance on the subject, certainly worth a million dollars from the Clay prize plus a Fields medal.

From now on we assume that the curve E is given by a Weierstrass equation $y^2z = x^3 + pxz^2 + qz^3$ with $4p^3 + 27q^2 \neq 0$, where we may assume without loss of generality that p and q are in $\mathbb{Z}$. Furthermore we will work in affine coordinates, simply remembering that the point at infinity is the neutral element for the group law, and is the given rational point, so we write our equation as $y^2 = x^3 + px + q$. We would like to determine the group of rational points on this curve. This is extremely difficult to do in complete generality (no algorithm is known), but we can obtain quite a lot of information from different points of view, both rigorous and conjectural. In this section some proofs will be omitted, and we refer to the numerous books on the subject such as [Cas2], [Cre2], [Dar], [Sil1], [Sil2], or [Sil-Tat].

8.1.3 Computing the Torsion Subgroup

There are several algorithms which can be used to compute $E_t(\mathbb{Q})$. The most efficient uses analytic techniques, and will not be described here. We begin with the Nagell–Lutz theorem which is sufficient for small cases.

Theorem 8.1.10 (Nagell, Lutz). *Let E be given by a Weierstrass equation $y^2 = x^3 + ax^2 + bx + c = f(x)$ with a, b, and c in $\mathbb{Z}$. If $T = (x, y) \in E_t(\mathbb{Q}) \setminus \{\mathcal{O}\}$, then either T has order 2, in other words $y = 0$, or x and y are integers such that y^2 divides $D = -(4a^3c - a^2b^2 - 18abc + 4b^3 + 27c^2) = \mathrm{disc}(f)$. In particular if the equation is $y^2 = x^3 + px + q$ then either $y = 0$ or $y^2 \mid D = -(4p^3 + 27q^2)$.*

Proof. The statement concerning points of order 2 is clear, so assume that T is not of order 2. Since the natural map from $E(\mathbb{Q})$ to $E(\mathbb{Q}_p)$ is injective, it follows from Corollary 7.3.30 (3) that $(x, y) \in \mathbb{Z}_p^2$ for all p including $p = 2$, hence that $(x, y) \in \mathbb{Z}^2$. But $2T$ is also a torsion point different from $\mathcal{O}$, so if we write $2T = (x_3, y_3)$ we also have $(x_3, y_3) \in \mathbb{Z}^2$. By the addition formula $x_3 = m^2 - 2x - a$ with $m = (3x^2 + 2ax + b)/(2y)$. Since $x_3 \in \mathbb{Z}$ it follows that m is a rational number which is a root of a monic second degree equation with integral coefficients, hence that $m \in \mathbb{Z}$, so that in particular $y \mid 3x^2 + 2ax + b = f'(x)$. Now we have the identity (see Exercise 2)

$$(27f(x) - (4a^3 - 18ab + 54c))f(x) - (f'(x) - a^2 + 3b)f'(x)^2 = \mathrm{disc}(f) = D\,,$$

and since $y^2 = f(x)$ and $y \mid f'(x)$ it follows that $y^2 \mid D$. □

Note that the same proof shows that if E is given by a general Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with $a_i \in \mathbb{Z}$ and if $T = (x, y)$ is a torsion point of order not dividing 2, then again $(x, y) \in \mathbb{Z}^2$ but with the slightly weaker condition $(2y + a_1x + a_3)^2 \mid 4\,\mathrm{disc}(E)$, see Exercise 3.

The following corollary is important.

Corollary 8.1.11. *If $P = (x, y)$ is a rational point on an elliptic curve given as above (i.e., with integral coefficients), then P is a nontorsion point if and only if there exists k such that $k \cdot P$ has nonintegral coordinates.*

Proof. If $k \cdot P$ has nonintegral coordinates, then it cannot be a torsion point by the above theorem, hence P is also nontorsion. Conversely, if $k \cdot P$ has integral coordinates for all k, these points cannot be distinct otherwise we would have an infinity of integral points, which is impossible by Siegel's Theorem 8.1.2. Thus two of them coincide for distinct values of k, hence P is a torsion point. □

Note that a point satisfying the hypothesis of the Nagell–Lutz theorem is not necessarily a torsion point. For instance the point $P = (-1, 1)$ on

the curve $y^2 = x^3 - 2x$, which satisfies the conditions, is nontorsion since $2 \cdot P = (9/4, -21/8)$ does not have integral coordinates.

A variant of the Nagell–Lutz theorem which is useful in some cases is the following.

Proposition 8.1.12. *Assume that E is given by an equation of the form $y^2 = x^3 + ax^2 + bx$ with a and b integral, in other words that up to translation of the x-coordinate the curve has a rational 2-torsion point. Then if $(x, y) \in E_t(\mathbb{Q})$ with $y \neq 0$ then $x \in \mathbb{Z}$ is such that $x \mid b$ and $x + a + b/x$ is a square.*

Proof. Assume that $T = (x, y) \in E_t(\mathbb{Q})$ with $y \neq 0$. Then $2T \in E_t(\mathbb{Q})$ and $2T \neq \mathcal{O}$. The x-coordinate of $2T$ is equal to $(b - x^2)^2/(4x(x^2 + ax + b))$, and by the Nagell–Lutz theorem this must be an integer. Let $d = \gcd(b, x)$, $b_1 = b/d$, $x_1 = x/d$ so that $\gcd(b_1, x_1) = 1$ and $4x_1(dx_1^2 + ax_1 + b_1) \mid (b_1 - dx_1^2)^2$. In particular $x_1 \mid b_1^2$, and since x_1 and b_1 are coprime we have $x_1 = \pm 1$, in other words $d = \pm x$ so $x \mid b$. Thus $x^2 \mid y^2$, hence writing $y = \pm x y_1$ we deduce that $y_1^2 = x + a + b/x$, hence the latter quantity is a square. □

Another consequence of the Nagell–Lutz theorem which is very useful for computing $E_t(\mathbb{Q})$ is the following.

Proposition 8.1.13. *Let E be given by $y^2 = x^3 + ax^2 + bx + c = f(x)$, and let ℓ be a prime number such that $\ell \nmid \operatorname{disc}(E) = -16D$, where $D = \operatorname{disc}(f)$ is as in Theorem 8.1.10. Then $E_t(\mathbb{Q})$ is isomorphic to a subgroup of $\overline{E}(\mathbb{F}_\ell)$, and in particular $|E_t(\mathbb{Q})|$ divides $|\overline{E}(\mathbb{F}_\ell)|$ for all such ℓ.*

Proof. Since $\ell \neq 2$ and $\ell \nmid \operatorname{disc}(f)$ the reduction $\overline{E}$ of the curve E modulo ℓ is again an elliptic curve. By the Nagell–Lutz theorem all the points of $E_t(\mathbb{Q})$ different from the point at infinity $\mathcal{O}$ have integral coordinates. The map reduction modulo ℓ is thus well defined from $E_t(\mathbb{Q})$ to $\overline{E}(\mathbb{F}_\ell)$ by sending the point at infinity of E to that of $\overline{E}$, and sending $(x, y) \in E_t(\mathbb{Q})$ to $(\overline{x}, \overline{y}) \in \overline{E}(\mathbb{F}_\ell)$. By Proposition 7.3.22 this map is clearly a group homomorphism with trivial kernel, hence is injective, proving the proposition. □

Thus for instance if we find two suitable values of ℓ for which the cardinalities $|\overline{E}(\mathbb{F}_\ell)|$ are coprime, we immediately know that $E_t(\mathbb{Q})$ is reduced to the point at infinity. As an application we give the following classical result.

Proposition 8.1.14. *Let d be a nonzero integer.*

(1) *Let E be given by $y^2 = x^3 - dx$. Then $E_t(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if and only if d has the form $d = m^2$, $E_t(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ if and only if d has the form $d = -4m^4$, and otherwise $E_t(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$.*

(2) *Let E be given by $y^2 = x^3 - d$. We have $E_t(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ if and only if d is a cube not of the form $-m^6$, $E_t(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$ if and only if d is either of the form $432m^6$ or of the form $-m^2$ and not of the form $-m^6$, $E_t(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$ if and only if d has the form $-m^6$, and otherwise $E_t(\mathbb{Q})$ is trivial.*

Proof. The proof of both statements relies on the essential fact that the two types of curves under consideration have complex multiplication by $\mathbb{Z}[i]$ and $\mathbb{Z}[\rho]$ respectively, where $i^2+1=0$ and $\rho^2+\rho+1=0$, but there is no need to know the theory of CM to understand the very simple proof.

(1). We note that the discriminant of E is equal to $-64d^3$. Let ℓ be a prime not dividing d and congruent to 3 modulo 4. Since $\left(\frac{-1}{\ell}\right)=-1$, it follows that for each $x\in\mathbb{F}_\ell$ either $x^3-dx=0$, or exactly one of x^3-dx and $(-x)^3-d(-x)=-(x^3-dx)$ is a quadratic residue modulo ℓ. If k denotes the number of roots of $x^3-dx=0$ in $\mathbb{F}_\ell$, it follows that counting the point at infinity we have $|\overline{E}(\mathbb{F}_\ell)|=1+k+\ell-k=\ell+1$. As mentioned above, this reflects the fact that a prime congruent to 3 modulo 4 is inert in the complex multiplication field $\mathbb{Q}(i)$.

When ℓ varies among all primes congruent to 3 modulo 4 and not dividing d, it is easy to see that the GCD of $\ell+1$ is equal to 4. Indeed, assume the contrary, and let p be a common prime divisor of all such $(\ell+1)/4$. Assume first that $p\neq 3$. By Dirichlet's theorem on primes in arithmetic progression (Theorem 10.5.29), since $\gcd(4p,3)=1$ we can find an infinity of primes ℓ such that $\ell=4kp+3$, and in particular one such that $\ell>d$, hence which does not divide d. But then $(\ell+1)/4=kp+1$ must be divisible by p, which is absurd. If now $p=3$, we consider instead the arithmetic progression $4kp-5$, and we obtain again a contradiction.

It thus follows from Proposition 8.1.13 that $|E_t(\mathbb{Q})|\mid 4$. Since $(0,0)$ is evidently a point of order 2 in $E(\mathbb{Q})$, we have $E_t(\mathbb{Q})\simeq\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, or $\mathbb{Z}/4\mathbb{Z}$. Since points of order 2 other than the point at infinity are those of the form $(x,0)$, it follows that $E_t(\mathbb{Q})\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ if and only if $x^2-d=0$ has two rational roots, hence if and only if d is a square. On the other hand P is a point of order 4 if and only if $2P$ has zero y-coordinate. If $P=(x,y)$, a short computation shows that this happens if and only if $x^2+d=0$ or $x^4-6dx^2+d^2=0$. This last case cannot occur since it would imply that the equation $X^2-6X+1=0$ has the rational root x^2/d. Thus $d=-x^2$, hence x and y are in $\mathbb{Z}$, and $y^2=x^3-dx=2x^3$, so $(2x)^3=(2y)^2$, hence $2x$ is a square, hence $x=2m^2$ for some m, hence $d=-4m^4$ as claimed, and in that case the point $(2m^2,4m^3)$ has order 4.

(2). This case is completely similar. The discriminant of E is equal to $-432d^2$, and we choose primes ℓ not dividing d and congruent to 5 modulo 6. Since $3\nmid(\ell-1)$, for such primes the map $x\mapsto x^3$ from $\mathbb{F}_\ell$ to itself is a bijection, hence for each $y\in\mathbb{F}_\ell$ there exists exactly one $x\in\mathbb{F}_\ell$ such that $x^3=y^2+d$, and it follows once again that $|\overline{E}(\mathbb{F}_\ell)|=\ell+1$, and this time it is because a prime congruent to 5 modulo 6 is inert in the complex multiplication field $\mathbb{Q}(\rho)$. A reasoning exactly similar to the one made for (1) shows that this implies that $|E_t(\mathbb{Q})|$ divides 6.

Clearly $|E_t(\mathbb{Q})|$ is even if and only if there exists a rational point of order 2, hence if and only if d is a cube. On the other hand there exists a point $P=(x,y)$ which has order 3 if and only if $2P=-P=(x,-y)$. a point of 3

torsion. It is immediately checked that this occurs if and only if $x(x^3-4d)=0$, hence either $x=0$, so $d=-y^2$ has the form $-m^2$, or if $x^3=4d$. But then $x=2x_1$ hence $d=2x_1^3$ and $y^2=x^3-d=6x_1^3$, so $(6x_1)^3=(6y)^2$, hence $6x_1$ is a square, so $x_1=6m^2$ for some m, hence $d=432m^6$, and in that case the point $(12m^2,36m^3)$ has order 3, proving (2). □

Corollary 8.1.15. *Let a, b, c be nonzero rational numbers, and assume that there exists a (projective) rational point $(x_0:y_0:z_0)$ on the cubic $ax^3+by^3+cz^3=0$.*

(1) *If there are only a finite number of such points then either b/a, c/a, or c/b is the cube of a rational number.*
(2) *Let T be the group of torsion points of the projective cubic, considered as an elliptic curve. We have $T\simeq\mathbb{Z}/3\mathbb{Z}$ if and only if b/a, c/a, and c/b are all cubes, $T\simeq\mathbb{Z}/2\mathbb{Z}$ if and only if up to permutation of a, b, and c we have that b/a and $c/(2a)$ are cubes, or $a/(2b)$ and $a/(2c)$ are cubes, otherwise T is trivial.*

Proof. By Proposition 7.2.4 we know that the cubic is birationally equivalent to the elliptic curve E whose affine Weierstrass equation is $Y^2=X^3-432(abc)^2$. It follows that if there are k projective points on our cubic, the curve E has rank 0 and $|E_t(\mathbb{Q})|=k$. We consider two cases.

Case 1: abc is not a cube or twice a cube. It follows from the proposition that $E_t(\mathbb{Q})$ is trivial, hence $k=1$, so the cubic must have a single projective rational point. However if we compute the intersection of the tangent to the cubic at $(x_0:y_0:z_0)$ with the cubic we find that

$$(x_1:y_1:z_1)=(x_0(by_0^3-cz_0^3):y_0(cz_0^3-ax_0^3):z_0(ax_0^3-by_0^3))$$

is another projective point on the cubic. Note that it is well defined (i.e., $(x_1,y_1,z_1)\neq(0,0,0)$): indeed otherwise, by symmetry assume that $x_0\neq0$. Then $by_0^3=cz_0^3$, hence $y_0\neq0$ (otherwise $z_0=0$, so $x_0=0$ since $ax_0^3+by_0^3+cz_0^3=0$), hence $ax_0^3=by_0^3=cz_0^3$, which implies that $0=ax_0^3+by_0^3+cz_0^3=3ax_0^3$ so $x_0=0$, again absurd and proving my claim.

Since $k=1$ we must have $(x_1:y_1:z_1)=(x_0:y_0:z_0)$. Since we cannot have $ax_0^3=by_0^3=cz_0^3$, once again by symmetry we may assume that $by_0^3\neq cz_0^3$. If we had the equality

$$by_0^3-cz_0^3=cz_0^3-ax_0^3=ax_0^3-by_0^3\ ,$$

then by adding these three quantities we would obtain $0=3(by_0^3-cz_0^3)$ contradicting our assumption that $by_0^3\neq cz_0^3$. It follows that for instance $cz_0^3-ax_0^3\neq by_0^3-cz_0^3$, and since $(x_1:y_1:z_1)=(x_0:y_0:z_0)$ this implies that $y_0=0$. But then $z_0\neq0$ and $ax_0^3+cz_0^3=0$, so $c/a=(-x_0/z_0)^3$ is a cube, as claimed.

Case 2: abc is a cube or twice a cube. By elementary manipulations that we have already explained in Section 6.4.4, without loss of generality

we may assume that $a = 1$ and that b and c are cubefree integers, and these manipulations only modify the ratios b/a, c/a, and c/b by cubes. Assume first that $abc = bc = m^3$, and let p be a prime divisor of m. We have $v_p(b)+v_p(c) \equiv 0 \pmod 3$ and $v_p(b) + v_p(c) \neq 0$, hence $v_p(b) \equiv 1 \pmod 3$ and $v_p(c) \equiv 2 \pmod 3$ or the reverse. But this is absurd since then $v_p(ax^3) = v_p(x^3) \equiv 0 \pmod 3$, $v_p(by^3) \equiv 1 \pmod 3$ and $v_p(cz^3) \equiv 2 \pmod 3$, although these three quantities sum to zero. Thus p cannot exist, hence $m = \pm 1$, and since b and c are integers $b = \pm c = \pm 1$, so for instance b is a cube. If $abc = bc = 2m^3$, the same reasoning shows that the only possible prime divisor of m is $p = 2$, so $b = \pm 2^{j_1}$ and $c = \pm 2^{j_2}$ with $j_1 + j_2 \equiv 1 \pmod 3$. It follows that $(j_1, j_2) \equiv (0,1)$, $(1,0)$, or $(2,2)$ modulo 3, hence either b, c, or c/b is a cube, as claimed. We leave the proof of (2) to the reader (Exercise 5). □

Although the determination of $E_t(\mathbb{Q})$ is very easy, the following deep theorem of B. Mazur can also be useful.

Theorem 8.1.16 (Mazur). *The group $E_t(\mathbb{Q})$ is isomorphic either to $\mathbb{Z}/N\mathbb{Z}$ with $1 \leqslant N \leqslant 10$ or $N = 12$, or to $(\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ with $N = 2$, 4, 6, or 8.*

For instance, if we find a point of order 7 in $E_t(\mathbb{Q})$, it is not necessary to go any further ($E_t(\mathbb{Q})$ has order 7). If we find a point of order 5, then since it is trivial to check if there exists a point of order 2 (the points with $y = 0$), we can immediately determine that $E_t(\mathbb{Q})$ is cyclic of order 5 or 10. Note that it is easy to show that there are an infinity of nonisomorphic elliptic curves E such that $E_t(\mathbb{Q})$ is isomorphic to one of the 15 groups given above, and they can also be rationally *parametrized*.

8.1.4 Computing the Mordell–Weil Group

Now that we have seen that $E_t(\mathbb{Q})$ is easily accessible, we consider the nontorsion part. There are essentially three different methods to attack the problem. The first and historically the oldest (initiated by Fermat) is the method of 2-descent. The second method is that of Heegner points, initiated in principle by Heegner in 1954, but really developed by Stark, Birch and others starting in 1967. The third method is partly conjectural since it is based on the Birch–Swinnerton-Dyer (BSD) conjecture which is proved (up to constants) only in rank 0 and 1, but at least says what to expect.

The 2-descent method is most useful when $r = 0$, i.e., when there are no points of infinite order. It is then often (but not always) possible to prove this in an elementary way, as we shall see below. However, even when $r > 0$ it gives very useful information, and in many favorable cases allows the rigorous computation of r and the P_i.

The Heegner point method is applicable if and only if $r = 1$. This may seem like a severe restriction, but tables and heuristics seem to show that curves with $r > 1$ form a small proportion of all elliptic curves and that

the others are equally divided between $r = 0$ and $r = 1$. It is even possible that the density of curves with $r > 1$ is equal to 0. Thus the Heegner point construction should be applicable to almost half of all elliptic curves.

Finally the third method (which appears in several guises, for instance Manin's conditional algorithm) is based on the BSD conjecture stating among other things that the algebraic rank r should be equal to the analytic rank, which is the order of vanishing at $s = 1$ of the Dirichlet series $L(E, s)$ attached to the elliptic curve E. Even that order is not easy to compute rigorously (in fact nobody has any idea how to prove that $L(E, s)$ vanishes to order greater or equal to 4 when it should), but at least we can use numerical approximations to guess its exact value. This then gives strong guidelines on how to use the rigorous methods.

In the next sections we will describe the three methods described above. Since the 2-descent method is the closest in spirit to the rest of this book we will describe it in more detail than the two others.

8.1.5 The Naïve and Canonical Heights

Before studying practical methods for computing the rank and if possible, also generators, an important point must be settled, which in fact is essential for the completion of the proof of the Mordell–Weil theorem. Consider the following problem. Let E be an elliptic curve defined over $\mathbb{Q}$. If we are given a point $P \in E(\mathbb{Q})$, it is easy to determine whether P has infinite order, for instance by using Corollary 8.1.11. But now assume that P and Q are two points in $E(\mathbb{Q})$, and for instance that there is no torsion. How do we check that P and Q are independent points in $E(\mathbb{Q})$, in other words that $mP + nQ \neq \mathcal{O}$ for all $(m, n) \neq (0, 0)$? The answer is not as simple as one could think, but luckily there *is* a very nice answer, given by the notion of *canonical height*.

Let us begin by defining the (naïve) height of a nonzero rational number x. Writing $x = n/d$ with $\gcd(n, d) = 1$ we define $h(x) = \max(\log(|n|), \log(|d|))$. This is also natural if we view x as an element of $\mathbb{P}^1(\mathbb{Q})$ with coordinates $(n : d)$. Thus more generally if $P \in \mathbb{P}^n(\mathbb{Q})$ we can write (uniquely up to a sign change) $P = (x_0 : x_1, \cdots : x_n)$ where $x_i \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_n) = 1$, and we define $h(P) = \max_i \log(|x_i|)$, where by convention $\log(0) = -\infty$.

Now assume for simplicity that the elliptic curve E is given by a single equation, hence defined as a curve in $\mathbb{P}^2$, and let $P \in E(\mathbb{Q}) \subset \mathbb{P}^2(\mathbb{Q})$. We could define the height of P as a point in $\mathbb{P}^2(\mathbb{Q})$. However for several reasons we prefer to define the (naïve) height of P as the height of its x-coordinate. In other words, thanks to Proposition 7.3.1, we can write the affine coordinates of P as $(m/d^2, n/d^3)$ with $\gcd(m, d) = \gcd(n, d) = 1$, and we define the height as $h(P) = \max(\log(|m|), \log(d^2))$, called again the *naïve height* of the point P. Note that because of the equation of the curve, when $h(P)$ is large then $\log(|n|)$ is comparable to $3h(P)$, so $h(P)$ does take into account the y-coordinate.

Please note that the function $h(P)$ is only defined on $E(\mathbb{Q})$ (or more generally on number fields), but not on $E(\mathbb{C})$. Although it has some nice properties, we also need a more regular function of P, called the *canonical height* of P, and defined as follows. First note that when experimentally computing $h(kP)$ for increasing values of k, we find immediately that it has the appearance of a parabola, which in fact is approximately true. For instance if E is the curve $y^2 = x^3 - 2x$ and $P = (-1, 1)$, then the first values of the integers $\exp(h(kP))$ are

```
1
9
169
12769
2325625
3263037129
5627138321281
68970122119586689
179966451590701691496 1
19797089376549862813859540 1
58648738806449243564537197828441
11343087863147146490729582249511602812 9
32398460974000521187196405196075267458328192 1
57163008369984740944839327879387136420685658888480 09
20430899634623811551503927405896084479142073252182576543062 5
```

which is visually a parabola. We thus define the canonical height by the formula

$$\widehat{h}(P) = \lim_{k\to\infty} \frac{h(kP)}{k^2} .$$

Note that we evidently have $h(P) \geqslant 0$, hence $\widehat{h}(P) \geqslant 0$ for all P. The following theorem summarizes the main properties of the canonical height.

Theorem 8.1.17. *The above limit exists, and defines a nonnegative function $\widehat{h}(P)$ on $E(\mathbb{Q})$ with the following properties.*

(1) (*Quadratic form.*) *The function $\widehat{h}(P)$ is a quadratic form on $E(\mathbb{Q})$, in other words if we define $\langle P, Q\rangle$ by the formula*

$$\langle P, Q\rangle = (\widehat{h}(P+Q) - \widehat{h}(P) - \widehat{h}(Q))/2$$

then $\langle P, Q\rangle$ is a symmetric bilinear form on $E(\mathbb{Q})$ such that $\langle P, P\rangle = \widehat{h}(P)$, hence $\widehat{h}(kP) = k^2\widehat{h}(P)$.

(2) (*Nondegeneracy.*) *We have $\widehat{h}(P) = 0$ if and only if $P \in E_t(\mathbb{Q})$, hence $\widehat{h}$ induces a positive definite quadratic form on the finitely generated free abelian group $E(\mathbb{Q})/E_t(\mathbb{Q})$.*

(3) (*Independence.*) *Points* $(P_i)_{1\leqslant i\leqslant n}$ *in* $E(\mathbb{Q})$ *are linearly independent in* $E(\mathbb{Q})/E_t(\mathbb{Q})$ *if and only if the determinant of the so-called* height pairing matrix $M = ((\langle P_i, P_j\rangle))_{1\leqslant i,j\leqslant n}$ *is not equal to* 0. *More precisely* $\sum_{1\leqslant j\leqslant n} b_j P_j$ *is a torsion point if and only if* $\sum_{1\leqslant j\leqslant n} b_j M_j = 0$, *where* M_j *is the* j*th column of* M.

(4) (*Bound.*) *There exists an explicitly computable constant* $C(E)$ *depending only on* E *such that for all* $P \in E(\mathbb{Q})$ *we have* $|\widehat{h}(P) - h(P)| \leqslant C(E)$ (*see below for a more precise estimate*).

(5) (*Finiteness.*) *For any* $B > 0$ *there exist only a finite number of points* $P \in E(\mathbb{Q})$ *such that* $\widehat{h}(P) \leqslant B$ (*or, equivalently,* $h(P) \leqslant B$).

We refer to [Sil-Tat] for proofs of the above properties, which are not difficult.

Note that in practice, to check that points are independent (or dependent) modulo the torsion subgroup one must use some care, since the determinant of the matrix M is an inexact real number. If this determinant seems to be nonzero, then one should give an error bound on the computation of the determinant so as to *prove* rigorously that the determinant is nonzero. On the other hand if the determinant seems to be equal to 0, one must then find a nonzero element of the kernel of the matrix M, which must exist and have entries very close to an integer after multiplying by a suitable denominator. Although it is usually impossible to prove rigorously that a real number is exactly equal to 0, here it is possible because one simply checks that the (integral) entries of the given element of the kernel produce a linear combination of the generators which is in the torsion subgroup. If this is the case all is well, we have shown that the points are dependent modulo torsion, otherwise it shows that the determinant computation has not been accurate enough, and it should be redone with a higher accuracy.

Because of the above theorem and remarks, it is thus essential to be able to compute heights numerically. The definition can be used, but is not very well suited to accurate computation. A much better algorithm is given for instance in Chapter 7 of [Coh0]. This is implemented in `GP` as the function `2*ellheight(P)`. Note that in versions up to 2.3 it is important to multiply by 2 the result given by `ellheight(P)`, since it corresponds to a different normalization (this may change in future releases of the package).

If we had taken a slightly different definition of the naïve height, such as for instance $\max(\log(|md|), \log(|n|), \log(d^3))$, which is the naïve height on the projective plane, using the same definition it can be shown that we would obtain a canonical height *equal to* (up to a constant multiple) the canonical height defined above.

For practical applications, it is essential to give explicit bounds for the difference between the naïve and canonical heights. Such a bound is the following (see [Sil3], and see [Cre-Pri-Sik] for much better bounds).

Theorem 8.1.18. *Let E be an elliptic curve defined over $\mathbb{Q}$ by a generalized Weierstrass equation. With the usual notation, set*

$$\mu(E) = \frac{\log(|\operatorname{disc}(E)|) + \log^+(j(E))}{6} + \log^+(b_2/12) + \log(2^*)\,,$$

where $\log^+(x) = \max(1, \log(|x|))$ *and* $2^* = 2$ *if* $b_2 \neq 0$ *and* $2^* = 1$ *otherwise. Then for* $P \in E(\mathbb{Q})$ *we have*

$$-\frac{h(j(E))}{12} - \mu(E) - 1.946 \leqslant \widehat{h}(P) - h(P) \leqslant \mu(E) + 2.14$$

(*recall that if* $\gcd(n,d) = 1$ *then* $h(n/d) = \max(\log(|n|), \log(|d|))$).

As a direct application, we see that in the computation of the torsion subgroup for instance using Theorem 8.1.10, then if $P = (x,y) \in E_t(\mathbb{Q})$ we have $\widehat{h}(P) = 0$ hence $h(P) = h(x) \leqslant h(j(E))/12 + \mu(E) + 1.946$, and since we know that $x \in \mathbb{Z}$, this gives a (usually small) upper bound for $|x|$.

8.2 Description of 2-Descent with Rational 2-Torsion

I emphasize from the start that my purpose is not to give the most efficient algorithms, which are in fact in constant progress, but to describe a simple version of the method which is already useful to treat many small cases. We closely follow [Sil-Tat].

8.2.1 The Fundamental 2-Isogeny

As above, in this section we fix an elliptic curve E given by a not necessarily reduced Weierstrass equation $y^2 = x^3 + ax^2 + bx + c$ with integers a, b and c and nonzero discriminant. We denote by $\mathcal{O}$ its point at infinity, which is the neutral element for the group law. In this section we make the crucial simplifying assumption that there exists a rational point of order 2 different from $\mathcal{O}$, i.e., that there exists $x_0 \in \mathbb{Q}$ (hence in $\mathbb{Z}$) such that $x_0^3 + ax_0^2 + bx_0 + c = 0$. We will explain in Section 8.3 what must be done if this assumption is not satisfied.

By setting $x = X + x_0$, we can send the point $(x_0, 0)$ to the origin $T = (0,0)$ which is therefore a point of order 2, and our equation will now have the form $y^2 = x^3 + ax^2 + bx$ for some other integers a and b. We will work with equations of this form. It is easy to see that the discriminant of the third degree polynomial is given by the formula $D = b^2(a^2 - 4b)$, hence $\operatorname{disc}(E) = 16b^2(a^2 - 4b)$.

In this section we will work with a pair of elliptic curves, one being E and the other which we will denote by $\widehat{E}$. All quantities and variables relative to $\widehat{E}$ will be denoted with a $\widehat{\ }$, and this will not cause any confusion with a reduction

homomorphism, which will not be used in this section. The curve $\widehat{E}$ is defined by the equation $y^2 = x^3 + \widehat{a}x^2 + \widehat{b}x$ with $\widehat{a} = -2a$ and $\widehat{b} = a^2 - 4b$. Note that $\widehat{\widehat{a}} = 4a$ and $\widehat{\widehat{b}} = 16b$, hence the curve $\widehat{\widehat{E}}$ is the curve $y^2 = x^3 + 4ax^2 + 16bx$, which is trivially isomorphic to E by replacing x by $4x$ and y by $8y$.

Proposition 8.2.1. *For any $P = (x, y) \in E$ set*

$$\phi(P) = (\widehat{x}, \widehat{y}) = \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2}\right)$$

for P not equal to T or $\mathcal{O}$, and set $\phi(T) = \phi(\mathcal{O}) = \widehat{\mathcal{O}}$. Then ϕ is a group homomorphism from E to $\widehat{E}$, whose kernel is equal to $\{\mathcal{O}, T\}$. Applying the same process to $\widehat{E}$ gives a map $\widehat{\phi_1}$ from $\widehat{E}$ to $\widehat{\widehat{E}}$, and $\widehat{\widehat{E}}$ is isomorphic to E via the map $(x, y) \mapsto (x/4, y/8)$. Thus there is a homomorphism $\widehat{\phi}$ from $\widehat{E}$ to E defined for $\widehat{P} = (\widehat{x}, \widehat{y})$ different from $\widehat{T}$ and $\widehat{\mathcal{O}}$ by

$$\widehat{\phi}(\widehat{P}) = (x, y) = \left(\frac{\widehat{y}^2}{4\widehat{x}^2}, \frac{\widehat{y}(\widehat{x}^2 - \widehat{b})}{8\widehat{x}^2}\right)$$

and by $\widehat{\phi}(\widehat{T}) = \widehat{\phi}(\widehat{\mathcal{O}}) = \mathcal{O}$. Furthermore for all $P \in E$ we have $\widehat{\phi} \circ \phi(P) = 2P$, and for all $\widehat{P} \in \widehat{E}$ we have $\phi \circ \widehat{\phi}(\widehat{P}) = 2\widehat{P}$.

Proof. The proof consists in a series of explicit verifications, where in each case we must separate the points $\mathcal{O}$ and T from the other points. It is done with utmost detail in [Sil-Tat] to which we refer. We will simply show that ϕ maps E to $\widehat{E}$, and that it maps three collinear points of E to three collinear points of $\widehat{E}$. This is the essential part of the proof. Also, to simplify we will assume that all the points that occur are distinct and different from $\mathcal{O}$, T, $\widehat{\mathcal{O}}$ and $\widehat{T}$.

Let (x, y) be a point on E, and $(\widehat{x}, \widehat{y}) = \phi(x, y)$. We compute that

$$\begin{aligned}\widehat{x}^3 + \widehat{a}\widehat{x}^2 + \widehat{b}\widehat{x} &= \frac{y^2}{x^2}\left(\frac{y^4}{x^4} - 2a\frac{y^2}{x^2} + a^2 - 4b\right) = \frac{y^2}{x^6}((y^2 - ax^2)^2 - 4bx^4) \\ &= \frac{y^2}{x^6}((x^3 + bx)^2 - 4bx^4) = \left(\frac{y(x^2 - b)}{x^2}\right)^2 = \widehat{y}^2\ ,\end{aligned}$$

proving that $(\widehat{x}, \widehat{y})$ is on the curve $\widehat{E}$.

Now for $i = 1$, 2 and 3 let $P_i = (x_i, y_i)$ be three collinear points on E (so that $P_1 + P_2 + P_3 = \mathcal{O}$ by definition of the group law). We will show that the points $\phi(P_i) = (\widehat{x_i}, \widehat{y_i})$ are collinear. Let $y = mx + n$ be the equation of the line through the points P_i. We have $n \neq 0$ since otherwise one of the points would be equal to $T = (0, 0)$, which we have excluded. I claim that the points $\phi(P_i)$ are on the line $y = \widehat{m}x + \widehat{n}$, with

$$\widehat{m} = \frac{nm - b}{n} \quad \text{and} \quad \widehat{n} = \frac{n^2 - anm + bm^2}{n} .$$

Using the equation of the curve and the relations $y_i = mx_i + n$ we compute that

$$\begin{aligned}
\widehat{m}\widehat{x}_i + \widehat{n} &= \frac{(nm-b)y_i^2 + (n^2 - anm + bm^2)x_i^2}{nx_i^2} \\
&= \frac{nm(y_i^2 - ax_i^2) - b(y_i - mx_i)(y_i + mx_i) + n^2x_i^2}{nx_i^2} \\
&= \frac{m(x_i^3 + bx_i) - b(y_i + mx_i) + nx_i^2}{x_i^2} \\
&= \frac{x_i^2(mx_i + n) - by_i}{x_i^2} = \frac{y_i(x_i^2 - b)}{x_i^2} = \widehat{y}_i ,
\end{aligned}$$

proving my claim. The rest of the verifications are simpler and left to the reader.

The proofs of the formulas for $\widehat{\phi}$ and that $\widehat{\phi}\circ\phi(P) = 2P$ and $\phi\circ\widehat{\phi}(\widehat{P}) = 2\widehat{P}$ are also verifications left to the reader. □

It follows from Definition 7.1.6 that ϕ is an isogeny from E to $\widehat{E}$, and that $\widehat{\phi}$ is its dual isogeny. Furthermore since we are in characteristic zero and the kernels (over $\overline{\mathbb{Q}}$) have two elements, these maps are 2-isogenies. This is why this method is called 2-descent via 2-isogenies (we will study general 2-descent in Section 8.3 below).

8.2.2 Description of the Image of ϕ

Although we know by Theorem 7.1.7 that ϕ is surjective over $\overline{\mathbb{Q}}$, we now restrict to *rational* points, and we want to determine the image of ϕ on rational points (since T is assumed to be a rational point, here in fact $(0,0)$, the kernel of ϕ is of course still equal to $\{\mathcal{O}, T\}$). This is given by the following result.

Proposition 8.2.2. *Denote by $I = \phi(E(\mathbb{Q}))$ the image of the rational points of E in $\widehat{E}(\mathbb{Q})$. Then*

(1) *$\widehat{\mathcal{O}} \in I$, and $\widehat{T} \in I$ if and only if* $\mathrm{disc}(E)$ *is a square in $\mathbb{Q}^*$ or, equivalently, if $\widehat{b} = a^2 - 4b$ is a square in $\mathbb{Q}^*$.*

(2) *Otherwise, a general point $\widehat{P} = (\widehat{x}, \widehat{y}) \in \widehat{E}(\mathbb{Q})$ with $\widehat{x} \neq 0$ belongs to I if and only if $\widehat{x}$ is a square in $\mathbb{Q}$.*

Proof. Since $\phi(\mathcal{O}) = \widehat{\mathcal{O}}$ the first statement is trivial. Since $x = 0$ implies $y = 0$, hence $(x, y) = T$ so $\phi((x, y)) = \widehat{\mathcal{O}}$, for the other statements we may assume $x \neq 0$. Then $\widehat{T} \in I$ if and only if there exists $x \neq 0$ such that

$y^2/x^2 = 0$, hence $y^2 = x(x^2 + ax + b) = 0$, hence x is a root of $x^2 + ax + b$. Thus x exists if and only if the discriminant $a^2 - 4b$ of this quadratic is a square, proving (1).

For (2), the definition of ϕ shows that $\widehat{x}$ is a square. Conversely, assume that $(\widehat{x}, \widehat{y}) \in \widehat{E}(\mathbb{Q})$ with $\widehat{x} \neq 0$ and $\widehat{x} = u^2$, and for $\varepsilon = \pm 1$ set

$$x_\varepsilon = \frac{u^2 - a + \varepsilon\widehat{y}/u}{2}, \quad y_\varepsilon = \varepsilon x_\varepsilon u \ .$$

I claim that both points $(x_\varepsilon, y_\varepsilon)$ are in $E(\mathbb{Q})$ and that $\phi(x_\varepsilon, y_\varepsilon) = (\widehat{x}, \widehat{y})$ (since the kernel of ϕ has order 2, we must indeed have two preimages). To prove that they are in $E(\mathbb{Q})$, using the equation of $\widehat{E}$ we compute that

$$x_1 x_{-1} = \frac{(\widehat{x} - a)^2 - \widehat{y}^2/\widehat{x}}{4} = \frac{\widehat{x}^3 - 2a\widehat{x}^2 + a^2\widehat{x} - \widehat{y}^2}{4\widehat{x}} = b \ .$$

Thus

$$x_\varepsilon + a + \frac{b}{x_\varepsilon} = x_\varepsilon + x_{-\varepsilon} + a = u^2 \ ,$$

hence

$$x_\varepsilon^3 + a x_\varepsilon^2 + b x_\varepsilon = (u x_\varepsilon)^2 = y_\varepsilon^2 \ ,$$

proving that both points are on E, and of course with rational coordinates.

Furthermore we have $\phi(x_\varepsilon, y_\varepsilon) = (x', y')$ with

$$x' = \frac{y_\varepsilon^2}{x_\varepsilon^2} = u^2 = \widehat{x} \ ,$$

and using once again the equality $b = x_\varepsilon x_{-\varepsilon}$

$$y' = \frac{y_\varepsilon(x_\varepsilon^2 - b)}{x_\varepsilon^2} = \varepsilon u(x_\varepsilon - x_{-\varepsilon}) = \varepsilon u(\varepsilon\widehat{y}/u) = \widehat{y}$$

as claimed. □

8.2.3 The Fundamental 2-Descent Map

The fact that the image of ϕ consists essentially of points $(\widehat{x}, \widehat{y})$ for which $\widehat{x}$ is a square is quite remarkable and will now be exploited in full.

Definition 8.2.3. *We define the* 2-descent map α *from the group* $E(\mathbb{Q})$ *to the multiplicative group* $\mathbb{Q}^*/\mathbb{Q}^{*2}$ *as follows.*

(1) $\alpha(\mathcal{O}) = 1$, $\alpha(T) = b$.
(2) *When* $x \neq 0$ *and* $(x, y) \in E(\mathbb{Q})$ *then* $\alpha((x, y)) = x$.

In the above, all the values are of course understood modulo the multiplicative action of $\mathbb{Q}^{*2}$.

The main result is the following.

Proposition 8.2.4. (1) *The 2-descent map α is a group homomorphism.*
(2) *The kernel of α is equal to $\widehat{\phi}(\widehat{E}(\mathbb{Q}))$, hence α induces an injective group homomorphism from $E(\mathbb{Q})/\widehat{\phi}(\widehat{E}(\mathbb{Q}))$ to $\mathbb{Q}^*/\mathbb{Q}^{*2}$.*
(3) *Let p_i for $1 \leqslant i \leqslant t$ be the distinct primes dividing b. The image of α is contained in the subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ generated by the classes modulo squares of -1 and the p_i.*
(4) *The index $[E(\mathbb{Q}) : \widehat{\phi}(\widehat{E}(\mathbb{Q}))]$ divides 2^{t+1}.*

Proof. (1) Clearly if $P = (x, y) \neq T$ then $\alpha(-P) = \alpha((x, -y)) = x$, hence $\alpha(P)\alpha(-P) = x^2 \in \mathbb{Q}^{*2}$, and $\alpha(T)\alpha(-T) = \alpha(T)^2 = b^2 \in \mathbb{Q}^{*2}$, so α sends inverses to inverses. Thus to prove (1) we must prove that if $P_1 + P_2 + P_3 = \mathcal{O}$ then $\alpha(P_1)\alpha(P_2)\alpha(P_3) \in \mathbb{Q}^{*2}$. If one of the P_i is equal to $\mathcal{O}$, we are in the case we have just treated. Let us first assume that none of the P_i is equal to T. As usual, let $y = mx + n$ be the equation of the line passing through the three points (the only other possible lines $x = n$ are excluded since none of the P_i is equal to $\mathcal{O}$). Writing the intersection of the line with the cubic equation, we see that the three abscissas x_i of the points P_i are the three roots of the equation

$$x^3 + (a - m^2)x^2 + (b - 2mn)x - n^2 = 0$$

(this is of course how the algebraic formula for the group law is obtained in the first place). In particular $x_1x_2x_3 = n^2 \in \mathbb{Q}^{*2}$, proving (1) when none of the P_i is equal to T. If one of the P_i is equal to T (and only one since otherwise the third point is equal to $\mathcal{O}$), we may assume for instance that $P_1 = T$. The three abscissas are now $x_1 = 0$, x_2, and x_3, and a line going through $P_1 = T = (0, 0)$ has equation $y = mx$, hence $n = 0$. It follows that the x_i are the roots of $x^3 + (a - m^2)x^2 + bx = 0$, hence x_2 and x_3 are the two roots of $x^2 + (a - m^2)x + b = 0$. Thus $x_2x_3 = b$ hence $\alpha(P_1)\alpha(P_2)\alpha(P_3) = b^2 \in \mathbb{Q}^{*2}$, finishing the proof of (1) and explaining why we must choose $\alpha(T) = b$.

(2) Applying Proposition 8.2.2 with $\widehat{E}$ instead of E and $\widehat{\phi}$ instead of ϕ, we see that α has in fact been constructed so that its kernel is exactly equal to $\widehat{\phi}(\widehat{E})(\mathbb{Q})$ (note that $\widehat{a}^2 - 4\widehat{b} = 16b \equiv b \pmod{\mathbb{Q}^{*2}}$).

(3) Let $P = (x, y) \in E(\mathbb{Q})$. We want to find conditions on $x = \alpha(P)$ modulo squares. By Proposition 7.3.1 we know that there exist integers m, n and d such that $x = m/d^2$, $y = n/d^3$ and $\gcd(m, d) = \gcd(n, d) = 1$. Replacing in the equation of E and clearing denominators gives

$$n^2 = m^3 + am^2d^2 + bmd^4 = m(m^2 + amd^2 + bd^4) .$$

This is the key to the proposition: we have a product of two integers equal to a square, so that as we have so often done in the study of Diophantine equations, both are close to squares. To see how close, we must compute the GCD of both factors. Assume first that $x \neq 0$. Since $\gcd(m, d) = 1$, we

see that the GCD of the factors is equal to $\gcd(m,b)$, and in particular is a divisor of b. Thus if $p \nmid b$, $v_p(m)$ is even. This means that m, hence x, is up to a multiplicative square in the group generated by ± 1 and the p_i, as claimed. If $x = 0$, then $P = T$ and $\alpha(P) = b$, which of course belongs to the group generated by its prime divisors and by -1.

(4) The subgroup described in (3) is the group of classes of the distinct representatives $\prod_{0 \leqslant i \leqslant t} p_i^{e_i}$ with $p_0 = -1$ and $e_i = 0$ or 1, which has 2^{t+1} elements. Thus (4) follows from (2) and (3). □

Although the aim of the above results is to describe an explicit method for computing the Mordell–Weil group in practice, it is to be noted that they comprise a large part of the Mordell–Weil theorem itself, at least for the type of curve that we are considering (having a rational torsion point of order 2).

Now note the following purely abelian group-theoretic lemma.

Lemma 8.2.5. *Let A and B be abelian groups written additively, and let ϕ from A to B and $\widehat{\phi}$ from B to A be two group homomorphisms. Assume that the indexes $[B : \phi(A)]$ and $[A : \widehat{\phi}(B)]$ are finite. Then the index $[A : \widehat{\phi} \circ \phi(A)]$ is also finite, and more precisely we have*

$$[A : \widehat{\phi} \circ \phi(A)] \mid [A : \widehat{\phi}(B)][B : \phi(A)] .$$

Proof. We have

$$[A : \widehat{\phi} \circ \phi(A)] = [A : \widehat{\phi}(B)][\widehat{\phi}(B) : \widehat{\phi}(\phi(A))] .$$

On the other hand it is clear that the map $\widehat{\phi}$ induces a surjective map from $B/\phi(A)$ to $\widehat{\phi}(B)/\widehat{\phi}(\phi(A))$, hence the cardinality of the latter quotient divides that of the former, proving the lemma. □

We now immediately deduce what is commonly called the *weak Mordell–Weil theorem*, since it easily implies the full theorem.

Corollary 8.2.6. *The group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. More precisely, its cardinality divides 2^{s+t+2}, where t is the number of distinct prime divisors of b and s is the number of distinct prime divisors of $a^2 - 4b$.*

Proof. By Proposition 8.2.4, we have $[E(\mathbb{Q}) : \widehat{\phi}(\widehat{E}(\mathbb{Q}))] \mid 2^{t+1}$. Applying the proposition to $\widehat{E}$ and ϕ, we have $[\widehat{E}(\mathbb{Q}) : \phi(E(\mathbb{Q}))] \mid 2^{s+1}$. The result thus follows from the lemma, since $\widehat{\phi} \circ \phi$ is the multiplication by 2 map. □

We can now prove the strong form of Mordell's theorem.

Theorem 8.2.7 (Mordell). *Let E be an elliptic curve defined over $\mathbb{Q}$, and assume known that for some $m \geqslant 2$ we know that $E(\mathbb{Q})/mE(\mathbb{Q})$ is finite (by the above corollary this is true for $m = 2$ when E has a rational 2-torsion*

point). Then $E(\mathbb{Q})$ is a finitely generated abelian group. More precisely if B is the largest canonical height of a system of representatives of $E(\mathbb{Q})$ modulo $mE(\mathbb{Q})$, then the (finite) set S of rational points $P \in E(\mathbb{Q})$ such that $\widehat{h}(P) \leqslant B$ generates $E(\mathbb{Q})$.

Proof. Assume by contradiction that the subgroup H of $E(\mathbb{Q})$ generated by S is not equal to $E(\mathbb{Q})$, and let $Q_1 \in E(\mathbb{Q})\backslash H$. The set of points in $E(\mathbb{Q})\backslash H$ of height less than or equal to that of Q_1 is finite, hence let $Q \in E(\mathbb{Q}) \setminus H$ be of minimal height. By assumption there exists $P \in S$ (in fact in our chosen system of representatives modulo $mE(\mathbb{Q})$) and $R \in E(\mathbb{Q})$ such that $Q = P + mR$. Since $P \in S \subset H$ and $Q \notin H$ we have $R \notin H$, hence $\widehat{h}(R) \geqslant \widehat{h}(Q)$ by our minimality assumption. Thus, since $\widehat{h}$ is a nonnegative quadratic form we obtain

$$\begin{aligned}\widehat{h}(P) &= \frac{1}{2}(\widehat{h}(Q+P) + \widehat{h}(Q-P)) - \widehat{h}(Q) \geqslant \frac{1}{2}\widehat{h}(mR) - \widehat{h}(Q) \\ &\geqslant \frac{m^2}{2}\widehat{h}(R) - \widehat{h}(Q) \geqslant 2\widehat{h}(R) - \widehat{h}(Q) \geqslant \widehat{h}(Q) > B\end{aligned}$$

since $Q \notin H$, and a fortiori $Q \notin S$. This is a contradiction since $P \in S$ hence $\widehat{h}(P) \leqslant B$. □

An important consequence of the proof of this theorem is that once $E(\mathbb{Q})/mE(\mathbb{Q})$ is known for some m (for instance for $m = 2$), obtaining a system of generators for $E(\mathbb{Q})$ is completely algorithmic. Thus the only obstruction to the existence of an algorithm to compute $E(\mathbb{Q})$ lies in the computation of the finite group $E(\mathbb{Q})/mE(\mathbb{Q})$ for some m. In practice however, better algorithms are used than the one implicit in the proof of the theorem.

8.2.4 Practical Use of 2-Descent with 2-Isogenies

Now that we have seen how to use 2-descent for theoretical purposes, we will show how it can be used in practice to bound the rank of an elliptic curve, and sometimes to compute it exactly. For this, we must analyze more precisely the images of the 2-descent maps.

We will denote by r the algebraic rank of the group $E(\mathbb{Q})$. Since E and $\widehat{E}$ are isogenous through the maps ϕ and $\widehat{\phi}$, it is clear that r is also the rank of $\widehat{E}$. We naturally denote by $\widehat{\alpha}$ the 2-descent map from $\widehat{E}(\mathbb{Q})$ to $\mathbb{Q}^*/\mathbb{Q}^{*2}$. We begin by the following proposition.

Proposition 8.2.8. *We have the equality*

$$|\alpha(E(\mathbb{Q}))||\widehat{\alpha}(\widehat{E}(\mathbb{Q}))| = 2^{r+2}\ .$$

Proof. As an abstract abelian group, we have $E(\mathbb{Q}) \simeq E_t(\mathbb{Q}) \oplus \mathbb{Z}^r$, hence

$$E(\mathbb{Q})/2E(\mathbb{Q}) \simeq E_t(\mathbb{Q})/2E_t(\mathbb{Q}) \oplus (\mathbb{Z}/2\mathbb{Z})^r\ .$$

Furthermore, for any finite abelian group A, the exact sequence

$$0 \longrightarrow A[2] \longrightarrow A \longrightarrow A \longrightarrow A/2A \longrightarrow 1 ,$$

where the middle map is multiplication by 2 and $A[2]$ is the kernel of that map, shows that $|A/2A| = |A[2]|$ (in fact $A/2A$ is noncanonically isomorphic to $A[2]$). In our case with $A = E_t(\mathbb{Q})$ the points of order 2 are exactly $\mathcal{O}$ and those with $y = 0$, hence $x = 0$ plus the two points corresponding to the roots of $x^2 + ax + b = 0$ if $a^2 - 4b$ is a square. Thus

$$|E(\mathbb{Q})/2E(\mathbb{Q})| = 2^{r+1+\delta} ,$$

where $\delta = 1$ or 0 according to whether $a^2 - 4b$ is a square or not.

On the other hand, let us consider our 2-isogenies ϕ and $\widehat{\phi}$. Since $\widehat{\phi} \circ \phi$ is the multiplication by 2 map, we evidently have

$$|E(\mathbb{Q})/2E(\mathbb{Q})| = [E(\mathbb{Q}) : \widehat{\phi}(\widehat{E}(\mathbb{Q}))][\widehat{\phi}(\widehat{E}(\mathbb{Q})) : \widehat{\phi}(\phi(E(\mathbb{Q})))] .$$

Now for any group homomorphism $\widehat{\phi}$ and subgroup B of finite index in an abelian group A we evidently have

$$\frac{\widehat{\phi}(A)}{\widehat{\phi}(B)} \simeq \frac{A}{B + \mathrm{Ker}(\widehat{\phi})} \simeq \frac{A/B}{(B + \mathrm{Ker}(\widehat{\phi}))/B} \simeq \frac{A/B}{\mathrm{Ker}(\widehat{\phi})/(\mathrm{Ker}(\widehat{\phi}) \cap B)} .$$

Thus

$$[\widehat{\phi}(A) : \widehat{\phi}(B)] = \frac{[A : B]}{[\mathrm{Ker}(\widehat{\phi}) : \mathrm{Ker}(\widehat{\phi}) \cap B]} .$$

We are going to use this formula with $A = \widehat{E}(\mathbb{Q})$ and $B = \phi(E(\mathbb{Q}))$. We know that $\mathrm{Ker}(\widehat{\phi})$ has two elements $\widehat{\mathcal{O}}$ and $\widehat{T}$, and we have shown in Proposition 8.2.2 that $\widehat{T} \in \phi(E(\mathbb{Q}))$ if and only if $a^2 - 4b$ is a square. Using the δ-notation above, it follows that

$$[\widehat{\phi}(\widehat{E}(\mathbb{Q})) : \widehat{\phi}(\phi(E(\mathbb{Q})))] = \frac{[\widehat{E}(\mathbb{Q}) : \phi(E(\mathbb{Q}))]}{2^{1-\delta}} .$$

Putting everything together we obtain

$$2^{r+2} = [E(\mathbb{Q}) : \widehat{\phi}(\widehat{E}(\mathbb{Q}))][\widehat{E}(\mathbb{Q}) : \phi(E(\mathbb{Q}))] ,$$

proving the proposition thanks to Proposition 8.2.4 (2). □

It remains to give a reasonably practical method to compute $|\alpha(E(\mathbb{Q}))|$ (which we will of course also use for $\widehat{\alpha}(\widehat{E}(\mathbb{Q}))$). We have seen in Proposition 8.2.4 (3) and (4) how $\alpha(E(\mathbb{Q}))$ can be determined in principle by looking at the factorization of b. We make this more precise in the following theorem.

Theorem 8.2.9. *The group $\alpha(E(\mathbb{Q}))$ is equal to the classes modulo squares of 1, b and of the positive and negative divisors b_1 of b such that the quartic equation*

$$Y^2 = b_1X^4 + aX^2Z^2 + (b/b_1)Z^4$$

has a solution with X, Y, Z pairwise coprime integers such that $XZ \neq 0$. If (X,Y,Z) is such a solution we will have $\gcd(b/b_1, X) = \gcd(b_1, Z) = 1$ and the point $P = (b_1X^2/Z^2, b_1XY/Z^3)$ is in $E(\mathbb{Q})$ and such that $\alpha(P) = b_1$.

Proof. Clearly $1 \in \alpha(E(\mathbb{Q}))$ hence we can forget the point at infinity. Let $(x,y) \in E(\mathbb{Q})$, and assume for the moment that $y \neq 0$, hence $x \neq 0$. We have seen in the proof of Proposition 8.2.4 that we can write $x = m/d^2$, $y = n/d^3$ with $d \neq 0$, $\gcd(m,d) = \gcd(n,d) = 1$ and the equation $n^2 = m(m^2 + amd^2 + bd^4)$. Let us now go further. Set $b_1 = \mathrm{sign}(m)\gcd(m,b)$. We can thus write $m = b_1m_1$, $b = b_1b_2$ with $m_1 > 0$ and $\gcd(m_1, b_2) = 1$. Substituting, we obtain $n^2 = b_1^2m_1(b_1m_1^2 + am_1d^2 + b_2d^4)$. It follows that $b_1 \mid n$, so we write $n = b_1n_1$, hence $n_1^2 = m_1(b_1m_1^2 + am_1d^2 + b_2d^4)$. Since $\gcd(m_1, b_2) = 1$ and $\gcd(m_1, d) \mid \gcd(m,d) = 1$ it follows that both factors are relatively prime so each of them is a square (since $m_1 > 0$). Thus there exist coprime integers X and Y such that $m_1 = X^2$, $b_1m_1^2 + am_1d^2 + b_2d^4 = Y^2$ and $n_1 = XY$. Setting $Z = d$ this gives the desired quartic $Y^2 = b_1X^4 + aX^2Z^2 + b_2Z^4$, and coming back to the initial point we have $x = m/Z^2 = b_1X^2/Z^2$ and $y = n/Z^3 = b_1XY/Z^3$. Thus given a point on the quartic we can come back to a point on $E(\mathbb{Q})$, proving that we have exactly described $\alpha(E(\mathbb{Q}))$ outside of the image of the points for which $y = 0$. Since $\gcd(m,d) = \gcd(n,d) = 1$ we deduce that $\gcd(X,Z) = \gcd(Y,Z) = 1$, so that X, Y and Z are pairwise coprime. Finally the points with $y = 0$ are either the point $T = (0,0)$, which is such that $\alpha(T) = b$ which is taken into account, or when $a^2 - 4b = e^2$ is a square the points with $x = (-a \pm e)/2$. But in that case $((-a-e)/2)((-a+e)/2) = (a^2-e^2)/4 = b$, so we can choose $b_1 = (-a \pm e)/2$, and clearly the point $(X,Y,Z) = (1,0,1)$ is on the corresponding quartic $Y^2 = b_1X^4 + aX^2Z^2 + (b/b_1)Z^4$, so these points will be included in the count. Note that $Z = d \neq 0$, and that in every case $X \neq 0$. Finally a simple inspection of the quartic equation shows that if X, Y and Z are pairwise coprime then $\gcd(b/b_1, X) = \gcd(b_1, Z) = 1$. □

To use this theorem in practice it is useful to have some additional results.

Definition 8.2.10. *For any nonzero integer $N \in \mathbb{Z}$, denote by $s(N)$ the* squarefree part *of N, i.e., the unique squarefree integer such that there exists an integer f with $N = s(N)f^2$.*

Proposition 8.2.11. *A divisor b_1 of b is such that the quartic $Y^2 = b_1X^4 + aZ^2X^2 + (b/b_1)Z^4$ is solvable with pairwise coprime X, Y and Z with $XZ \neq 0$ if and only if the quartic $Y^2 = s(b_1)X^4 + aZ^2X^2 + (b/s(b_1))Z^4$ is solvable with $\gcd(X,Z) = 1$ and $XZ \neq 0$.*

Proof. Assume that b_1 is such that the quartic $Y^2 = b_1X^4 + aZ^2X^2 + (b/b_1)Z^4$ is solvable with pairwise coprime X, Y and Z with $XZ \neq 0$ and write $b_1 = s(b_1)f^2$. Then

$$(Yf)^2 = s(b_1)(Xf)^4 + aZ^2(Xf)^2 + (b/s(b_1))Z^4 ,$$

so that if we set $Y_1 = Yf$, $X_1 = Xf$, the coprimality conditions of the theorem imply that X and $f \mid b_1$ are coprime to Z, hence X_1 also.

Conversely, assume that $Y^2 = s(b_1)X^4 + aZ^2X^2 + (b/s(b_1))Z^4$ is solvable with $XZ \neq 0$ and $\gcd(X, Z) = 1$, and set $f = \gcd(X, Y)$, which is coprime to Z since it divides X. Thus f^2 divides $(b/s(b_1))Z^4$, hence $b/s(b_1)$ so we can write

$$(Y/f)^2 = s(b_1)f^2(X/f)^4 + aZ^2(X/f)^2 + (b/(s(b_1)f^2))Z^4 .$$

It follows that $(X/f, Y/f, Z)$ is a solution to the quartic with $s(b_1)f^2$ (still dividing b) instead of b_1, but now with $\gcd(X/f, Y/f) = 1$. Next we have evidently $\gcd(X/f, Z) = 1$, and if p is a prime dividing $\gcd(Y, Z)$, then $p^2 \mid s(b_1)X^4$, hence since $s(b_1)$ is squarefree $p \mid X$, a contradiction since $p \mid Z$ and $\gcd(X, Z) = 1$. Thus $\gcd(Y, Z) = \gcd(Y/f, Z) = 1$. By Theorem 8.2.9, the pairwise coprimality of X/f, Y/f and Z imply the two other coprimality conditions. □

Corollary 8.2.12. *Let b_1 be a divisor of b such that both b_1 and b/b_1 are squarefree (which is in particular the case if b is squarefree). If (X, Y, Z) satisfies $Y^2 = b_1X^4 + aZ^2X^2 + (b/b_1)Z^4$ with $XZ \neq 0$ and $\gcd(X, Z) = 1$, then X, Y and Z are pairwise coprime.*

Proof. Note that $b_1 = s(b_1)$. Thus from the proof of the above proposition we see that if we set $f = \gcd(X, Y)$ then $f^2 \mid b/b_1$, hence $f = 1$ since we assume b/b_1 squarefree. As in the above proof we also deduce that $\gcd(Y, Z) = 1$. □

Corollary 8.2.13. *The group $\alpha(E(\mathbb{Q}))$ is equal to the set of classes modulo squares of 1, of $s(b)$, and of b_1 and b/b_1 for all positive and negative divisors b_1 of b such that b_1 is squarefree, $|b_1| \leqslant |b|^{1/2}$, such that the quartic equation*

$$Y^2 = b_1X^4 + aZ^2X^2 + (b/b_1)Z^4$$

has a solution with X, Y, Z integral, $XZ \neq 0$ and $\gcd(X, Z) = 1$.

Proof. Denote by G the set of classes modulo squares of the elements described in this corollary. Clearly the classes of 1 and the squarefree part of b belong to $\alpha(E(\mathbb{Q}))$. If b_1 is squarefree we have $s(b_1) = b_1$, hence the proposition and the theorem imply that the class of b_1 is in $\alpha(E(\mathbb{Q}))$, hence the class of b/b_1 also since $\alpha(E(\mathbb{Q}))$ is a group. We have thus shown that $G \subset \alpha(E(\mathbb{Q}))$. Conversely, let b_1 be an arbitrary divisor of b such that there

exist pairwise coprime integers X, Y and Z with $XZ \neq 0$ such that $Y^2 = b_1X^4 + aZ^2X^2 + (b/b_1)Z^4$. By the proposition, the class of $s(b_1)$, which is equal to that of b_1, is such that the corresponding quartic is solvable with $XZ \neq 0$ and $\gcd(X,Z) = 1$. If $|b_1| \leqslant |b|^{1/2}$, hence $|s(b_1)| \leqslant |b|^{1/2}$, this implies that the class of b_1 is in G. If $|b_1| > |b|^{1/2}$ then $|b/b_1| < |b|^{1/2}$, we have $Y^2 = (b/b_1)Z^4 + aZ^2X^2 + (b/(b/b_1))X^4$ so the quartic is solvable with X and Z interchanged, $XZ \neq 0$, and X, Y, Z pairwise coprime. By the proposition we deduce that the class of $s(b/b_1)$, hence of b/b_1 is in G, hence that of $b_1 = b/(b/b_1)$ also by definition of G. It follows that $G = \alpha(E(\mathbb{Q}))$, as claimed. □

Remark. In the above results we have used in part the fact that $\alpha(E(\mathbb{Q}))$ is a group. In practice, this fact must be used to its maximum extent.

8.2.5 Examples of 2-Descent with 2-Isogenies

Let us consider several simple examples of 2-descent when the curve has a rational 2-torsion point.

Proposition 8.2.14. (1) *The curve* $y^2 = x^3 - 1$ *has rank* 0 *and torsion group of order* 2.
(2) *The curve* $y^2 = x^3 + 1$ *has rank* 0 *and torsion group of order* 6.

Note that we have already proved this result in Corollary 6.5.8, also using 2-descent.

Proof. We treat both curves simultaneously. The point $\mathcal{O}$ together with $(1,0)$ for the first curve and $(-1,0)$ for the second clearly are the only points of order dividing 2. By the Nagell–Lutz Theorem 8.1.10 any other torsion point is such that y is integral and $y^2 \mid 27$, hence $y^2 = 1$ or 9. For the first curve this does not correspond to rational values of x, and for the second curve it gives the points $(0, \pm 1)$ and $(2, \pm 3)$, which one can check are torsion points, the torsion group being of order 6 generated by the point $(2,3)$.

Let us now compute the rank using 2-descent. Let $y^2 = x^3 - \varepsilon$ be the equation of our curve, with $\varepsilon = \pm 1$. We first set $x = x_1 + \varepsilon$ to put the curve in the form that we have treated $y^2 = x_1^3 + 3\varepsilon x_1^2 + 3x_1$. Thus $a = 3\varepsilon$ and $b = 3$. The group $\alpha(E(\mathbb{Q}))$ contains 1 and 3. The divisors of b are ± 1 and ± 3, hence it is sufficient to check whether $b_1 = -1$ gives a solvable quartic with $X \neq 0$. The quartic equation is $Y^2 = -X^4 + 3\varepsilon X^2Z^2 - 3Z^4$. Since the discriminant of the quadratic $-u^2 + 3\varepsilon u - 3$ is negative, the quadratic is always negative, hence our quartic does not even have real solutions. Thus $|\alpha(E(\mathbb{Q}))| = 2$.

We must now compute $|\widehat{\alpha}(\widehat{E}(\mathbb{Q}))|$. The equation of $\widehat{E}$ is $y^2 = x_1^3 - 6\varepsilon x_1^2 - 3x_1$. Thus $b = -3$, and the group $\widehat{\alpha}(\widehat{E}(\mathbb{Q}))$ contains 1 and -3. Once again it is sufficient to check whether $b_1 = -1$ gives a solvable quartic with $X \neq 0$. The quartic equation is $Y^2 = -X^4 - 6\varepsilon X^2Z^2 + 3Z^4$. There exist real solutions to this quartic, so we cannot get away with that. On the other hand there are

no solutions modulo 3 since $Y^2 \equiv -(X^2)^2 \pmod 3$ implies that $3 \mid X$ and $3 \mid Y$ hence $9 \mid 3Z^4$ hence $3 \mid \gcd(X, Z)$, a contradiction since $\gcd(X, Z) = 1$. Thus once again $|\widehat{\alpha}(\widehat{E}(\mathbb{Q}))| = 2$, and we deduce from Proposition 8.2.8 that $r = 0$. □

Proposition 8.2.15. *Let p be a positive or negative prime number, and let E_p be the elliptic curve with equation $y^2 = x^3 - px$. The torsion group of E_p has order 2, and if r_p is the rank of $E_p(\mathbb{Q})$ we have the following results:*

(1) *When $p > 0$ and $p \equiv 3$, 11 or 13 modulo 16 or if $p < 0$ and $p = -2$ or $p \equiv 5$ or 9 modulo 16 we have $r_p = 0$.*
(2) *When $p > 0$ and $p = 2$ or $p \equiv 5$, 7, 9 or 15 modulo 16, or if $p < 0$ and $p \equiv 1$, 3, 11 or 13 modulo 16 we have $r_p = 0$ or 1 (and $r_2 = 1$).*
(3) *When $p > 0$ and $p \equiv 1 \pmod{16}$ or $p < 0$ and $p \equiv -1 \pmod 8$ we have $r_p = 0$, 1 or 2.*

Proof. The points $\mathcal{O}$ and $(0, 0)$ are clearly the only points of order dividing 2. By the Nagell–Lutz Theorem 8.1.10 and its refinement Proposition 8.1.12, any other torsion point has integral x and y with $x \mid p$ and $y^2 \mid 4p^3$, in other words $y^2 \mid 4p^2$. This clearly implies that $x = -\operatorname{sign}(p)$ with $|p - 1|$ a square dividing $4p^2$, hence dividing 4 since it is coprime to p, or $x = \operatorname{sign}(p)p = |p|$ with $p^2|p - 1|$ a square dividing $4p^2$, hence $|p - 1|$ a square dividing 4, as before. However Proposition 8.1.12 also implies that $x + p/x$ is a square, so here that $|p + 1|$ is a square. Since two squares cannot differ by 2, this is impossible, proving the statement concerning the torsion subgroup (we could also look at the finite number of remaining possibilities).

Let us now apply 2-descent. With the notation used in that context we have $a = 0$ and $b = -p$. Thus $\alpha(E(\mathbb{Q}))$ contains the classes of 1 and of $-p$. The only other divisors of b are -1 and p, and they will both be in $\alpha(E(\mathbb{Q}))$ if and only if $b_1 = -1$ is, hence if the quartic $Y^2 = -X^4 + pZ^4$ has a solution with $XZ \neq 0$. If $p < 0$ this quartic has no real solution, hence in that case $|\alpha(E(\mathbb{Q}))| = 2$. On the other hand if $p > 0$ there are cases when there exist solutions, and others where there are none. For $p = 2$ we have the trivial solution $(X, Y, Z) = (1, 1, 1)$ so $|\alpha(E(\mathbb{Q}))| = 4$, hence we exclude that case, so p is odd. Recall that by Theorem 8.2.9 we have $\gcd(X, Z) = \gcd(Y, Z) = \gcd(p, X) = \gcd(X, Y) = 1$. Since $p \nmid X$, Y/X^2 is a square root of -1 modulo p, hence when $p \equiv 3 \pmod 4$ once again we obtain that $|\alpha(E(\mathbb{Q}))| = 2$. We may thus assume that $p > 0$ with $p \equiv 1 \pmod 4$. If Z is even then X must be odd, hence Y also, which is impossible if $Y^2 \equiv -X^4 \pmod{16}$. Thus Z is odd hence $Z^4 \equiv 1 \pmod{16}$. If X is even, we have $1 \equiv Y^2 \equiv p \pmod 8$. If X is odd we have $X^4 \equiv 1 \pmod{16}$ and Y is even, hence we have $Y^2 \equiv 0$ or 4 modulo 16, so $p \equiv 1$ or 5 modulo 16. Thus if $p \equiv 13 \pmod{16}$ we see once again that $|\alpha(E(\mathbb{Q}))| = 2$. On the other hand for $p \equiv 1$, 5 and 9 modulo 13 there are no 2-adic conditions, and a short computer search shows that the quartic is often (but not always) solvable

(the only exceptions for $p \leqslant 500$ and a search up to $d = 1000$ are $p = 113$, 193 and 353, out of 33 possible primes; of course this does not imply that the quartic has no solutions for these values of p).

To summarize, if $p < 0$ or $p \equiv 3 \pmod 4$ or $p \equiv 13 \pmod{16}$ we have $|\alpha(E(\mathbb{Q}))| = 2$, if $p = 2$ we have $|\alpha(E(\mathbb{Q}))| = 4$, and otherwise (i.e., if $p > 0$ and $p \equiv 1$, 5 or 9 modulo 16) we have $|\alpha(E(\mathbb{Q}))| = 2$ or 4.

Let us now consider $\widehat{\alpha}(\widehat{E})(\mathbb{Q})$. The equation of $\widehat{E}$ is $y^2 = x^3 + 4px$, hence $a = 0$ and $b = 4p$, and we will apply Corollary 8.2.13 since b is not squarefree. The classes of 1 and p belong to $\widehat{\alpha}(\widehat{E})(\mathbb{Q})$, and otherwise the quartic to be considered is $Y^2 = b_1X^4 + (4p/b_1)Z^4$. The possible squarefree values of b_1 less than $|b|^{1/2}$ in absolute value are ± 1 and ± 2, except if $p = \pm 3$ for which we also have ± 3. When $b_1 = -1$ the quartic is $Y^2 = -X^4 - 4pZ^4$, hence has no real solutions when $p > 0$. When $p < 0$ we cannot have X odd, otherwise Y is also odd, which is impossible modulo 4. Thus X and Y are both even, and writing $Y = 2Y_1$, $X = 2X_1$ we obtain $Y_1^2 = -4X_1^4 - pZ^4$. Since $\gcd(X, Z) = 1$, Z is odd, and $p \neq -2$ otherwise Y_1 is even hence $4 \mid pZ^4$, so p is also odd. Thus Y_1 is odd, so $1 + p \equiv 0 \pmod 4$ hence $p \equiv 3 \pmod 4$. To summarize, if either $p > 0$ or $p < 0$ and $p \not\equiv 3 \mod 4$ then we cannot take $b_1 = -1$ in Corollary 8.2.13.

When $b_1 = \pm 2$ the quartic is $Y^2 = \pm(2X^4 + 2pZ^4)$. If $b_1 = -2$ we must have $p < 0$ otherwise there are no real solutions. Writing $Y = 2Y_1$, we have $2Y_1^2 = \pm(X^4 + pZ^4)$. If p is odd, X must be odd otherwise Z is even and $2 \mid \gcd(X, Z)$. Thus Z is also odd so we deduce that $p + 1 \equiv 0$, ± 2 or 8 modulo 16, hence $p \equiv 1$, 7, 13, or 15 modulo 16. When $p = 2\varepsilon$ with $\varepsilon = \pm 1$, X must be even, hence Z must be odd, and writing $X = 2X_1$ we have $Y_1^2 = \pm(8X_1^4 + \varepsilon Z^4)$. It follows that we must have $\varepsilon = \pm = \operatorname{sign}(b_1)$, otherwise we have a contradiction modulo 4, and for $\varepsilon = \pm$ we have the solution $(X_1, Y_1, Z) = (1, 3, 1)$ when $b_1 = p = 2$ and $(X_1, Y_1, Z) = (1, 1, 3)$ when $b_1 = p = -2$. To summarize, if $p \neq b_1$ or p odd and $p \not\equiv \pm 2 - 1$, 7 or 15 modulo 16 we cannot take $b_1 = \pm 2$, while for $p = b_1$ we can, but we already have p in our list.

Assume now that $p = 3\varepsilon$ with $\varepsilon = \pm 1$, so that we must also consider $b_1 = \pm 3$. Since the class of p already belongs to $\widehat{\alpha}(\widehat{E})(\mathbb{Q})$, it is thus sufficient to consider $b_1 = -p$, hence the quartic is $Y^2 = -3\varepsilon X^4 - 4Z^4$. This has no real solution if $\varepsilon = 1$. If $\varepsilon = -1$, i.e., $p = -3$, it has no solution modulo 4 with X odd. Thus X, hence Y is even, hence Z is odd since $\gcd(X, Z) = 1$, and writing $X = 2X_1$ and $Y = 2Y_1$ we obtain $Y_1^2 = 12X_1^4 - Z^4$ which has also no solution modulo 4. Thus in all cases we do not obtain any extra element of our group when $b_1 = \pm 3$.

Using Corollary 8.2.13, we finally have the following cases.

- If $p = \pm 2$, $\widehat{\alpha}(\widehat{E})(\mathbb{Q})$ is equal to the classes of 1 and p, hence has 2 elements.
- If $p > 0$ and $p \equiv 3$, 5, 9, 11 or 13 modulo 16, then $\widehat{\alpha}(\widehat{E})(\mathbb{Q})$ is equal to the classes of 1 and p, hence has 2 elements.

• If $p > 0$ and $p = 2$ or $p \equiv 1$, 7 or 15 modulo 16, then $\widehat{\alpha}(\widehat{E})(\mathbb{Q})$ may have 2 or 4 elements (when the class of $b_1 = 2$ belongs to it). Both cases can occur.

• If $p < 0$ and $p \equiv 5$ or 9 modulo 16 then $\widehat{\alpha}(\widehat{E})(\mathbb{Q})$ is equal to the classes of 1 and p, hence has 2 elements.

• If $p < 0$ and $p \equiv 1 \pmod{16}$, then $\widehat{\alpha}(\widehat{E})(\mathbb{Q})$ may have 2 or 4 elements (when the class of $b_1 = 2$ belongs to it). Both cases can occur.

• If $p < 0$ and $p \equiv 13 \pmod{16}$, then $\widehat{\alpha}(\widehat{E})(\mathbb{Q})$ may have 2 or 4 elements (when the class of $b_1 = -2$ belongs to it). Both cases can occur.

• If $p < 0$ and $p \equiv 3$ or 11 modulo 16, then $\widehat{\alpha}(\widehat{E})(\mathbb{Q})$ may have 2 or 4 elements (when the class of $b_1 = -1$ belongs to it). Both cases can occur.

• If $p < 0$ and $p \equiv 7$ or 15 modulo 16, then $\widehat{\alpha}(\widehat{E})(\mathbb{Q})$ may have 2, 4 or 8 elements (depending on the classes of $b_1 = -1$ and $b_1 = \pm 2$).

Putting together the results on both groups, we obtain the results of the proposition. □

Remark. Assuming a very weak form of the Birch–Swinnerton-Dyer conjecture, in case (2) of the proposition we always have $r = 1$ and in case (3) we always have $r = 0$ or 2, and both cases can occur. We give here an example where $r = 2$, and will give an example where $r = 0$ in the next section.

Proposition 8.2.16. *For $p = -73$ we have $r_p = 2$, generators of $E(\mathbb{Q})$ modulo torsion being $(9/16, 411/64)$ and $(4/9, 154/27)$.*

Proof. Since $p < 0$ we already know that $|\alpha(E(\mathbb{Q}))| = 2$, so we consider only $\widehat{E}$ whose equation is $y^2 = x^3 - 292x$. The squarefree divisors b_1 of $b = -292 = -2^2 \cdot 73$ less than $|b|^{1/2}$ are $b_1 = \pm 1$ and ± 2. The corresponding quartics are $Y^2 = b_1 X^4 - (292/b_1)Z^4$, and for $b_1 = -1$, 2 and -2 we find $(X, Y, Z) = (4, 6, 1)$, $(3, 4, 1)$ and $(1, 12, 1)$ respectively as solutions. It follows that $|\widehat{\alpha}(\widehat{E}(\mathbb{Q}))| = 8$, hence $r_p = 2$ as claimed. To find the corresponding points on E, we proceed as follows. By Theorem 8.2.9, we find the points $(-16, -24)$, $(18, 24)$ on the curve $\widehat{E}$. We do not need the third point corresponding to $b_1 = -2 = -1 \cdot 2$ since it will be the sum or difference of the first two (in fact it is the difference), and we do not need the points corresponding to b/b_1 which will be the opposites. We now apply the map $\widehat{\phi}$ from $\widehat{E}$ to E, thus obtaining the two points $(9/16, -411/64)$ and $(4/9, 154/27)$. These points are necessarily independent, and one can prove that they generate $E(\mathbb{Q})$ modulo torsion. □

8.2.6 An Example of Second Descent

We now give an example showing how descent can be pushed one step further, and also showing that the case $r_p = 0$ can also occur in case (3) of Proposition 8.2.15.

Proposition 8.2.17. *For $p = -17$, we have $r_p = 0$.*

Proof. As above, we note that since $p < 0$ we already know that $|\alpha(E(\mathbb{Q}))| = 2$, so we consider only $\widehat{E}$ whose equation is $y^2 = x^3 - 68x$. The squarefree divisors b_1 of $b = -68 = -2^2 \cdot 17$ less than $|b|^{1/2}$ are $b_1 = \pm 1$ and ± 2, so we must consider the quartics $Y^2 = -X^4 + 68Z^4$ and $Y^2 = \varepsilon(2X^4 - 34Z^4)$ for $\varepsilon = \pm 1$. It is not difficult to see that these quartics are everywhere locally soluble. On the other hand a quick search does not produce any solutions. We thus must work some more to show that they indeed have no solutions.

Consider the first quartic. Dividing through by Z^4 gives the conic $y^2 = -x^2 + 68$ with $y = Y/Z^2$ and $x = X^2/Z^2$. Conversely, if we have a rational point (x, y) on that conic with $x \in \mathbb{Q}^{*2}$, we can write $x = X^2/Z^2$ with $\gcd(X, Z) = 1$ and set $Y = yZ^2$, hence we will have a suitable integer point on our quartic. Now $(x, y) = (2, 8)$ is an evident point on our conic, so to parametrize it we set $y - 8 = t(x - 2)$ and intersect with the conic. An easy computation gives the parametrization $x = 2(t^2 - 8t - 1)/(t^2 + 1)$, $y = -4(2t^2 + t - 2)/(t^2 + 1)$. Thus, writing $t = u/v$ with $\gcd(u, v) = 1$ we are looking for such pairs (u, v) with $2(u^2 - 8uv - v^2)/(u^2 + v^2) \in \mathbb{Q}^{*2}$.

This is equivalent to the equation $z^2 = 2(u^2 - 8uv - v^2)(u^2 + v^2)$, which is a new quartic, and we could hope to show that this quartic is not locally soluble. However it is simpler to proceed as follows. Writing $2(u^2 - 8uv - v^2)/(u^2 + v^2) = a^2/b^2$ with $\gcd(a, b) = 1$, we see that there exists $\lambda \in \mathbb{Z}$ (which we may assume squarefree if we forget the condition $\gcd(a, b) = 1$) such that $2(u^2 - 8uv - v^2) = \lambda a^2$ and $u^2 + v^2 = \lambda b^2$. Now note that

$$(-8u + 66v)(u^2 + v^2) + (4u - v)(2(u^2 - 8uv - v^2)) = 68v^3$$

hence (exchanging u and v and v into $-v$)

$$(8v + 66u)(u^2 + v^2) + (4v + u)(2(u^2 - 8uv - v^2)) = 68u^3$$

so that $\lambda \mid 68$ since $\gcd(u, v) = 1$. Since $\lambda = (u^2 + v^2)/b^2 > 0$ and is squarefree, it follows that $\lambda = 1$, 2, 17 or 34.

Assume first that λ is odd. Then $u^2 + v^2 = \lambda b^2$, so u and v have opposite parities otherwise they are both odd, hence $\lambda b^2 \equiv 2 \pmod 8$, so $2 \mid b$ which is absurd. But then $u^2 - 8uv - v^2$ is odd, hence $\lambda a^2 \equiv 2 \pmod 4$ which again is impossible since it implies $2 \mid a$. Thus λ must be even, i.e., $\lambda = 2$ or 34, so that $\lambda \equiv 2 \pmod{32}$. Then $u^2 + v^2 = \lambda b^2$ and $\gcd(u, v) = 1$ imply that u and v are both odd. We thus have

$$a^2 \equiv (\lambda/2)a^2 = u^2 - 8uv - v^2 = 2((\lambda/2)b^2 - v^2 - 4uv) \equiv 2(b^2 + 3) \pmod{16},$$

hence $a^2 \equiv 6$, 8 or 14 modulo 16, which is impossible. Thus all four values of λ are excluded, showing that our quartic $Y^2 = -X^4 + 68Z^4$ has no solutions.

We proceed similarly for the quartics $Y^2 = \varepsilon(2X^4 - 34Z^4)$ with $\varepsilon = \pm 1$. We want to look for rational points on the conic $y^2 = \varepsilon(2x^2 - 34)$ for which

x is a rational square. Clearly $(x,y) = (4+\varepsilon, 4)$ is on the conic, so we set $y - 4 = t(x - 4 - \varepsilon)$. An easy computation gives the parametrization

$$x = \frac{t^2(4+\varepsilon) - 8t + 8\varepsilon + 2}{t^2 - 2\varepsilon}, \quad y = \frac{-4t^2 + 4t(4\varepsilon+1) - 8\varepsilon}{t^2 - 2\varepsilon} .$$

As above, we write $t = u/v$ with $\gcd(u,v) = 1$ and $x = a^2/b^2$ hence we deduce as above that there exists a squarefree integer λ such that

$$u^2(4+\varepsilon) - 8uv + (8\varepsilon+2)v^2 = \lambda a^2 \quad \text{and} \quad u^2 - 2\varepsilon v^2 = \lambda b^2 ,$$

and since

$$(-10u - 9v)(u^2 - 2v^2) + (2u + 5v)(5u^2 - 8uv + 10v^2) = 68v^3$$

and

$$(-6u + 25v)(u^2 + 2v^2) + (2u - 3v)(3u^2 - 8uv - 6v^2) = 68v^3$$

and similar identities with $68u^3$ on the right hand side, we deduce as above that $\lambda \mid 68$ hence that $\lambda = \pm 1, \pm 2, \pm 17$, or ± 34.

When $\varepsilon = 1$, the quadratic $5u^2 - 8uv + 10v^2$ has negative discriminant hence is always positive, so we must have $\lambda > 0$. When $\varepsilon = -1$, $u^2 + 2v^2 > 0$ so once again $\lambda > 0$. Thus in both cases we must have $\lambda = 1$, 2, 17 or 34.

Assume first that λ is odd, hence $\lambda \equiv 1 \pmod 8$. From $u^2 - 2\varepsilon v^2 = \lambda b^2$ we deduce that b is odd, otherwise $4 \mid \lambda b^2$ hence $4 \mid u^2$ hence $2 \mid v^2$ contradicting $\gcd(u,v) = 1$. Thus u is odd. It follows that

$$u^2(4+\varepsilon) - 8uv + 8\varepsilon v^2 + 2v^2 \equiv 4 + 2\varepsilon - \varepsilon\lambda \pmod 8$$

is odd, hence a is odd so that $3 + \varepsilon \equiv 0 \pmod 8$, which is absurd.

Assume now that λ is even, hence $\lambda/2 \equiv 1 \pmod 8$. Then u is even, hence v is odd. We thus have

$$2(u/2)^2(4+\varepsilon) - 8(u/2)v + (4\varepsilon+1)v^2 = (\lambda/2)a^2 ,$$

hence a is odd so

$$2\varepsilon(u/2)^2 + 4\varepsilon + 1 \equiv 1 \pmod 8 ,$$

hence $(u/2)^2 \equiv 2 \pmod 4$, a contradiction.

To conclude, we see that all values of λ are excluded, showing that our quartics $Y^2 = \varepsilon(2X^4 - 34Z^4)$ have no solutions. Putting everything together, we obtain that $|\widehat{\alpha}(\widehat{E}(\mathbb{Q}))| = 2$ hence that $r_p = r(E) = 0$. □

Remark. For all three quartics we have been able to show local insolubility at 2 directly. In general however, it will be necessary to parametrize one of the conics using the general theory of Diophantine equations of degree 2, and replace in the other.

8.3 Description of General 2-Descent

From now on, we do *not* assume that our elliptic curve $y^2 = x^3 + ax + b$ has a rational 2-torsion point, and in fact we explicitly assume that it does not, in other words that the polynomial $x^3 + ax + b$ is irreducible. As usual we may always assume that a and b are rational integers.

There are essentially two methods to deal with this case. The first method is algebraic, and consists in imitating the above method by placing ourselves in a larger number field containing a 2-torsion point. This has the advantage of being easy to explain since it is a simple generalization, and also of being useful also for the computation of the group of points of an elliptic curve over an arbitrary number field instead of $\mathbb{Q}$. It has the disadvantage of not being very efficient for small examples, although for large ones it is competitive. The second method consists in using invariant theory. It is often more efficient than the first, but has the disadvantage of being applicable only over $\mathbb{Q}$. We will only describe the first method, and refer to [Cre2] for complete details on the second method.

8.3.1 The Fundamental 2-Descent Map

Let $K = \mathbb{Q}(\theta)$ be the number field generated over $\mathbb{Q}$ by a root θ of the equation $x^3 + ax + b = 0$. Consider the map α from $E(\mathbb{Q})$ to K^*/K^{*2} defined by $\alpha(\mathcal{O}) = 1 \pmod{K^{*2}}$ and

$$\alpha(P) = x - \theta \pmod{K^{*2}} \text{ if } P = (x, y) \neq \mathcal{O} ,$$

where of course modulo is taken in the multiplicative sense. As in the rational 2-torsion case, the main usefulness of this map comes from the following result.

Proposition 8.3.1. (1) *The map α is a group homomorphism from $E(\mathbb{Q})$ to K^*/K^{*2}.*
(2) *The kernel of α is equal to $2E(\mathbb{Q})$.*

Proof. (1). We treat the generic case, leaving the (easy) special cases to the reader. Clearly if $P = (x, y)$ then

$$\alpha(-P)\alpha(P) = \alpha((x, -y))\alpha((x, y)) = (x - \theta)^2 \equiv 1 \pmod{K^{*2}} ,$$

hence α sends inverses to inverses. Thus we must prove that if $P_1 + P_2 + P_3 = \mathcal{O}$ then $\alpha(P_1)\alpha(P_2)\alpha(P_3) \equiv 1 \pmod{K^{*2}}$. Let $y = mx + n$ be the equation of the line passing through the three points. Writing the intersection of the line with the cubic equation, we see that the three abscissas x_i of the points P_i are the three roots of the equation $A(x) = 0$ with

$$A(X) = (X^3 + aX + b) - (mX + n)^2 ,$$

hence by definition of θ we have

$$(x_1-\theta)(x_2-\theta)(x_3-\theta) = -A(\theta) = (m\theta+n)^2 \equiv 1 \pmod{K^{*2}} ,$$

proving (1).

(2). It follows from (1) that

$$\alpha(2P) \equiv \alpha(P)^2 \equiv 1 \pmod{K^{*2}} ,$$

so that $2E(\mathbb{Q}) \subset \mathrm{Ker}(\alpha)$. Conversely, assume that $Q=(x,y) \in \mathrm{Ker}(\alpha)$ with $Q \neq \mathcal{O}$, in other words that $x-\theta = u^2$ for some $u = u_2\theta^2+u_1\theta+u_0 \in K$ with $u_i \in \mathbb{Q}$ for all i. Expanding u^2 and using $\theta^3 = -a\theta - b$, we obtain the three equations

$$\begin{cases} au_2^2 - u_1^2 - 2u_0u_2 = 0 \\ bu_2^2 + 2au_1u_2 - 2u_0u_1 = 1 \\ -2bu_1u_2 + u_0^2 = x . \end{cases}$$

Clearly $u_2 \neq 0$, otherwise $u_1 = 0$ by the first equation, hence $0 = 1$ by the second. I claim that the point $P = (u_1/u_2, 1/u_2)$ is in $E(\mathbb{Q})$ and is such that $Q = \pm 2P$ for a suitable sign $\pm$. As in the rational 2-torsion case this a simple but tedious verification. Indeed, first note that using the above equations we have

$$\left(\frac{u_1}{u_2}\right)^3 + a\left(\frac{u_1}{u_2}\right) + b = \frac{u_1^3+au_1u_2^2+bu_2^3}{u_2^3} = \frac{u_1(au_2^2-2u_0u_2)+au_1u_2^2+bu_2^3}{u_2^3}$$
$$= \frac{2au_1u_2-2u_0u_1+bu_2^2}{u_2^2} = \frac{1}{u_2^2} ,$$

hence $P \in E(\mathbb{Q})$. Furthermore, multiplying the first of the above equations by $2u_0$ and subtracting u_1 times the second, we obtain the identity

$$u_1 = u_2(bu_1u_2 + 2au_1^2 - 2au_0u_2 + 4u_0^2) .$$

Thus if we set $2P = (x_3, y_3)$ we have $x_3 = m^2 - 2(u_1/u_2)$ with

$$m = \frac{3(u_1/u_2)^2+a}{2/u_2} = \frac{3u_1^2+au_2^2}{2u_2} = \frac{3(au_2^2-2u_0u_2)+au_2^2}{2u_2} = 2au_2 - 3u_0 .$$

Using the above identity, it follows that

$$\begin{aligned} x_3 &= 4a^2u_2^2 - 12au_0u_2 + 9u_0^2 - 2(bu_1u_2 + 2au_1^2 - 2au_0u_2 + 4u_0^2) \\ &= u_0^2 - 8au_0u_2 - 4au_1^2 + 4a^2u_2^2 - 2bu_1u_2 \\ &= u_0^2 - 2bu_1u_2 + 4a(au_2^2 - 2u_0u_2 - u_1^2) = x \end{aligned}$$

by the first and third of the basic relations above. Since $P \in E(\mathbb{Q})$, it follows that $y_3 = \pm y$ hence that $Q = \pm 2P$ as claimed, proving the proposition. □

Corollary 8.3.2. *The map α induces an injective group homomorphism from $E(\mathbb{Q})/2E(\mathbb{Q})$ to K^*/K^{*2} (which by abuse of notation we will still denote by α). In addition, if the image of α is finite then $E(\mathbb{Q})$ is finitely generated of rank r equal to the dimension of the image of α as an $\mathbb{F}_2$-vector space.*

Proof. The first statement is clear. For the second we note that by assumption E has no rational 2-torsion, hence if $d = \dim_{\mathbb{F}_2}(\mathrm{Im}(\alpha))$ we have $|E(\mathbb{Q})/2E(\mathbb{Q})| = |\mathrm{Im}(\alpha)| = 2^d$, so Theorem 8.2.7 implies that $E(\mathbb{Q})$ is finitely generated of some rank r such that $2^r = |E(\mathbb{Q})/2E(\mathbb{Q})|$, hence that $r = d$ as claimed. □

To have precise information on $E(\mathbb{Q})$ we must therefore determine the image of α. For this we need the notion of T-Selmer group of a number field (not to be confused with the Selmer group of the elliptic curve, although the notions are related).

8.3.2 The T-Selmer Group of a Number Field

For the reader's convenience in the following definitions we have included the classical definitions of T-unit group and T-class group.

Definition 8.3.3. *Let T be a finite set of finite places of K.* [1]

(1) *We say that an element $u \in K^*$ is a T-unit if $v_{\mathfrak{p}}(u) = 0$ for every prime ideal $\mathfrak{p}$ such that $\mathfrak{p} \notin T$. The group of T-units is denoted $U_T(K)$.*
(2) *We define the T-class group $Cl_T(K)$ as the quotient group of the ordinary class group $Cl(K)$ by the subgroup generated by the classes of the elements of T.*
(3) *We say that an element $u \in K^*$ is a T-virtual square if $v_{\mathfrak{p}}(u) \equiv 0 \pmod 2$ for every prime ideal $\mathfrak{p}$ such that $\mathfrak{p} \notin T$.*
(4) *We define the T-Selmer group $S_T(K)$ as the set of classes of virtual squares modulo K^{*2}.*

Remark. Most authors use the notation $K(T, 2)$ instead of $S_T(K)$.

Denote by $\mathcal{A}$ the group of fractional ideals generated by the elements of T. The reader can easily check that u is a T-unit if and only if $u\mathbb{Z}_K \in \mathcal{A}$ and that u is a T-virtual square if and only if $u\mathbb{Z}_K = \mathfrak{q}^2\mathfrak{a}$ for some ideal $\mathfrak{q}$ and some $\mathfrak{a} \in \mathcal{A}$.

The main properties of these notions are summarized in the following proposition.

Proposition 8.3.4. *Let K be a number field of signature (r_1, r_2), let T be a finite set of finite places of K, and denote by t its cardinality.*

[1] We use T instead of the more standard S to avoid notation such as $S_S(K)$

(1) *The group $U_T(K)$ is a finitely generated abelian group of rank $r_1 + r_2 + t - 1$, whose torsion subgroup is independent of T and equal to the (cyclic) group of roots of unity of K. In particular*

$$\left|\frac{U_T(K)}{U_T(K)^2}\right| = 2^{r_1+r_2+t} .$$

(2) *We have a natural split exact sequence*

$$1 \longrightarrow \frac{U_T(K)}{U_T(K)^2} \longrightarrow S_T(K) \longrightarrow Cl_T(K)[2] \longrightarrow 1 ,$$

where as usual for an abelian group G, $G[2]$ denotes the subgroup of G killed by 2. In particular $S_T(K)$ is finite and its cardinality is equal to $2^{r_1+r_2+t+s'}$, where s' denotes the 2-rank of $Cl_T(K)$, hence $|S_T(K)|$ divides $2^{r_1+r_2+t+s}$ where s denotes the 2-rank of $Cl(K)$.

Proof. (1). Although the proof is well-known and easy we repeat it here. We have a natural exact sequence

$$1 \longrightarrow U(K) \longrightarrow U_T(K) \longrightarrow \mathcal{A} \longrightarrow Cl(K) \longrightarrow Cl_T(K) \longrightarrow 1 ,$$

where the map starting from $U_T(K)$ sends u to the ideal $u\mathbb{Z}_K$, and the map starting from $\mathcal{A}$ sends an ideal to its ideal class. It is immediately checked that the sequence is indeed exact. Since $Cl(K)$ and a fortiori $Cl_T(K)$ are finite groups, it follows that $U_T(K)$ is finitely generated and its rank is equal to that of $U(K)$ $(r_1 + r_2 - 1)$ plus that of $\mathcal{A}$, equal to t. The statement concerning the torsion subgroup is clear.

(2). Let $\overline{u} \in U_T(K)$, so that $u\mathbb{Z}_K = \mathfrak{q}^2\mathfrak{a}$ for some $\mathfrak{a} \in \mathcal{A}$. We send $\overline{u}$ to the class of $\mathfrak{q}$ in $Cl_T(K)$. Clearly this does not depend on the decomposition $\mathfrak{q}^2\mathfrak{a}$ or on the chosen representative u of $\overline{u}$ in K^*. Since $\mathfrak{q}^2 = u\mathfrak{a}^{-1}$ it is clear that the class of $\mathfrak{q}$ belongs in fact to $Cl_T(K)[2]$. With this map defined, it is then easily checked that the given sequence is exact and split. The statements concerning the cardinality of $S_T(K)$ follow. □

It is clear that $S_T(K)$ is an $\mathbb{F}_2$-vector space, and from the existence of these two exact sequences it is not difficult to give an $\mathbb{F}_2$-basis for $S_T(K)$. As always in this course we assume that we have at our disposal a CAS such as `Pari/GP` which can efficiently compute class and unit groups of number fields. We first compute explicitly $U_T(K)$ using the algorithm given in [Coh1] Proposition 7.4.7, whence an $\mathbb{F}_2$-basis of $U_T(K)/U_T(K)^2$. We compute $Cl_T(K)$ as a quotient of $Cl(K)$ by using the general quotient algorithm for abelian groups ([Coh1] Algorithm 4.1.7), and we can then easily compute $Cl_T(K)[2]$ and use the splitting of the exact sequence to obtain an $\mathbb{F}_2$-basis of $S_T(K)$. In the frequent special case where the class number $h(K) = |Cl(K)|$ of K is *odd* (in particular when it is equal to 1), then $S_T(K) = U_T(K)/U_T(K)^2$ and as an

$\mathbb{F}_2$ basis of $S_T(K)$ we can take the disjoint union of generators of the $h(K)$th power of each prime ideal of T (which are principal ideals) together with a system of fundamental units and a generator of the group of roots of unity of K. We will see several explicit examples below.

8.3.3 Description of the Image of α

With these definitions and properties, it is now easy to determine the image of α. We keep all the above assumptions and notation, in other words E is an elliptic curve defined over $\mathbb{Q}$ by a Weierstrass equation $y^2 = x^3 + ax + b$ with a and b in $\mathbb{Z}$, we let θ be a root of $x^3 + ax + b = 0$, assumed to be irreducible, and we set $K = \mathbb{Q}(\theta)$. Finally, we set $I(\theta) = [\mathbb{Z}_K : \mathbb{Z}[\theta]]$, the index of $\mathbb{Z}[\theta]$ in the full ring of integers $\mathbb{Z}_K$. Thus, if $d(K)$ is the discriminant of the number field K we have $-(4a^3 + 27b^2) = d(K)I(\theta)^2$.

Proposition 8.3.5. *Let $P = (x, y) \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$, assume that $\mathfrak{q}$ is a prime ideal of K such that $v_{\mathfrak{q}}(x-\theta)$ is odd, and denote by q the prime number below $\mathfrak{q}$. Then $v_{\mathfrak{q}}(x-\theta) \geqslant 1$, $\mathfrak{q} \mid (3\theta^2 + a)$, $v_q(y) \geqslant 1$, $v_q(3x^2 + a) \geqslant 1$, and $q \mid I(\theta)$ (hence in particular $q^2 \mid (4a^3 + 27b^2)$).*

Proof. Set $\gamma = x - \theta \in K$. We can write $y^2 = \gamma C$ with $C = \gamma^2 + 3\theta\gamma + 3\theta^2 + a$. If $v_{\mathfrak{q}}(\gamma)$ was negative we would have $v_{\mathfrak{q}}(\gamma) = v_{\mathfrak{q}}(y^2) - v_{\mathfrak{q}}(C) = 2(v_{\mathfrak{q}}(y) - v_{\mathfrak{q}}(\gamma)) \equiv 0 \pmod 2$, since a and θ are integral. Thus when $v_{\mathfrak{q}}(\gamma)$ is odd we have $v_{\mathfrak{q}}(\gamma) \geqslant 1$, and we deduce from the expression for C that $v_{\mathfrak{q}}(C) \geqslant 0$. Since $v_{\mathfrak{q}}(C) = 2v_{\mathfrak{q}}(y) - v_{\mathfrak{q}}(\gamma) \equiv 1 \pmod 2$, we have $v_{\mathfrak{q}}(C) \geqslant 1$, hence $v_{\mathfrak{q}}(3\theta^2 + a) = v_{\mathfrak{q}}(C - \gamma(\gamma + 3\theta)) \geqslant 1$, proving the first two results. Since $y^2 = \gamma C$ and $\mathfrak{q} \mid \gamma$ (or C), we have $v_q(y) \geqslant 1$. Furthermore $3x^2 + a = 3(\gamma + \theta)^2 = 3\gamma^2 + 6\gamma\theta + 3\theta^2 + a$, and since $\mathfrak{q} \mid \gamma$ and $\mathfrak{q} \mid (3\theta^2 + a)$ it follows that $v_q(3x^2 + a) \geqslant 1$.

The result $q \mid I(\theta)$ and its proof was communicated to me by D. Simon. We prove the following:

Lemma 8.3.6. *If $q \nmid I(\theta)$ then $\mathfrak{q}$ is the only ideal $\mathfrak{q}_i$ above q such that $x-\theta \in \mathfrak{q}_i$, and it has residual degree 1.*

Proof. By Proposition 3.3.18, since $q \nmid I(\theta)$ the decomposition of $q\mathbb{Z}_K$ into prime ideals copies the decomposition of the polynomial $R(X) = X^3 + aX + b$ modulo q. Thus, write $R(X) \equiv \prod_i R_i(X)^{e_i} \pmod q$, where $R_i(X)$ are monic polynomials in $\mathbb{Z}[X]$. We then have $q\mathbb{Z}_K = \prod_i \mathfrak{q}_i^{e_i}$, where $\mathfrak{q}_i = q\mathbb{Z}_K + R_i(\theta)\mathbb{Z}_K$, and $f(\mathfrak{q}_i/q) = \deg(R_i)$, and we reorder the $\mathfrak{q}_i$ so that $\mathfrak{q}_1 = \mathfrak{q}$. If we write $x = n/d$ with coprime n and d in $\mathbb{Z}$, we see that $v_q(d) = 0$, otherwise $v_{\mathfrak{q}}(x-\theta) = v_{\mathfrak{q}}(n/d - \theta) < 0$ since $v_{\mathfrak{q}}(\theta) \geqslant 0$. Thus if we set $x_1 = nd^{-1} \bmod q$ we have $v_q(x - x_1) \geqslant 1$, hence $x_1 - \theta \in \mathfrak{q}$. Since $(R_1(X) - R_1(x_1))/(X - x_1) \in \mathbb{Z}[X]$, it follows that $R_1(\theta) - R_1(x_1) \in \mathfrak{q}$, hence that $R_1(x_1) \in \mathfrak{q}$, in other words $R_1(x_1) \equiv 0 \pmod q$. Since $\overline{R_1}$ is irreducible in $(\mathbb{Z}/q\mathbb{Z})[X]$, this means that $R_1(X) = X - x_1$, and in particular that $\deg(R_1) = 1$, so that $f(\mathfrak{q}/q) = 1$.

Furthermore, since the R_i are pairwise coprime modulo q, x_1 cannot be a root of R_i for $i \neq 1$, hence $x - \theta$ cannot belong to $\mathfrak{q}_i$ for $i \neq 1$. □

Resuming the proof of the proposition, if we assume by contradiction that $q \nmid f(\theta)$ we thus have $(x-\theta)\mathbb{Z}_K = \mathfrak{q}^v\mathfrak{a}$ where $v = v_{\mathfrak{q}}(x-\theta)$ and $\mathfrak{a}$ is an ideal coprime to all ideals above $\mathfrak{q}$. Since $f(\mathfrak{q}/q) = 1$ we thus have

$$y^2 = |x^3 + ax + b| = |\mathcal{N}_{K/\mathbb{Q}}(x-\theta)| = \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{q})^v \, \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a}) = q^v \, \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a}) \, ,$$

hence $v = v_{\mathfrak{q}}(x-\theta) = 2v_q(y)$ is even, in contradiction with the assumption of the proposition, and finishing the proof. □

Corollary 8.3.7. *Denote by T the set of prime ideals $\mathfrak{q}$ of K such that $\mathfrak{q} \mid (3\theta^2 + a)$ and $q \mid I(\theta)$, where q is the prime number below $\mathfrak{q}$. The image of α is equal to the group of $\overline{u} \in S_T(K)$ such that $\mathcal{N}_{K/\mathbb{Q}}(u)$ is a square in $\mathbb{Q}$ for some (or any) lift of $\overline{u}$ to K^*, and for which there exists a lift u of the form $x - \theta$.*

Proof. Let $P = (x, y) \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$, so that $\alpha(P) = x - \theta$. By the proposition, if $v_{\mathfrak{q}}(x-\theta)$ is odd we have $\mathfrak{q} \mid (3\theta^2+a)$ and $q \mid I(\theta)$, hence $\mathfrak{q} \in T$, in other words the class $\overline{u}$ of $\alpha(P)$ belongs to $S_T(K)$. It is evidently the class of an element of the form $x - \theta$, and since $\mathcal{N}_{K/\mathbb{Q}}(u) = x^3 + ax + b$ it follows that $(x, y) \in E(\mathbb{Q})$ if and only if $\mathcal{N}_{K/\mathbb{Q}}(u) = y^2$ is a square in $\mathbb{Q}$. □

Remarks.

(1) If E is given by an equation $y^2 = R(x)$ with $R(x) = x^3 + ax^2 + bx + c$, it is clear that the above corollary is still valid if we replace the first condition defining T by $\mathfrak{q} \mid R'(\theta)$.

(2) It can be shown (see [Sch-Sto]) that an additional condition on q is that the Tamagawa number c_q be even. Even though we have not defined this notion, note that these numbers can easily be computed.

Corollary 8.3.8 (Mordell). *The group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite and the group $E(\mathbb{Q})$ is finitely generated. More precisely $|E(\mathbb{Q})/2E(\mathbb{Q})|$ divides $2^{r_1+r_2+t+s}$, using the above notation.*

Proof. The finiteness and the bound for $E(\mathbb{Q})/2E(\mathbb{Q})$ follow from the above proposition and Proposition 8.3.4. The statement for $E(\mathbb{Q})$ follows from Theorem 8.2.7. □

Although our aim is practical, note that we have finished the proof of the Mordell–Weil theorem over $\mathbb{Q}$.

8.3.4 Practical Use of 2-Descent in the General Case

We now explain how to use the above results in practice, keeping in mind that, as in the rational 2-torsion case, there does not exist any unconditional algorithm for computing the rank.

We begin by computing $\mathrm{disc}(R)$, the number field $K = \mathbb{Q}(\theta)$, its discriminant $d(K)$ as well as the index $I(\theta) = \sqrt{\mathrm{disc}(R)/d(K)}$, and finally the set T of prime ideals $\mathfrak{q}$ of K such that $\mathfrak{q} \mid (3\theta^2 + a)$ and $q \mid I(\theta)$. Using the algorithms explained at the end of Section 8.3.2 we then compute an $\mathbb{F}_2$-basis of $S_T(K)$. Using [Coh1], Algorithm 4.1.11 we then compute the kernel $S_T(K,1)$ of the norm map from $S_T(K)$ to $\mathbb{Q}^*/\mathbb{Q}^{*2}$. By Corollary 8.3.7 the image of α is exactly the group of elements $\overline{u} \in S_T(K,1)$ which have a lift $u \in K^*$ of the form $x - \theta$. Up to this point the computation is completely algorithmic. However the determination of such elements $\overline{u}$ is the nonalgorithmic part of the method since we are going to see that, as in the rational 2-torsion case, it leads to the determination of rational points on hyperelliptic quartics.

Let $u = u_2\theta^2 + u_1\theta + u_0$ be any lift of $\overline{u}$. We must determine whether there exists $\gamma = c_2\theta^2 + c_1\theta + c_0 \in K^*$ such that $u\gamma^2 = x - \theta$. Expanding, we have

$$u\gamma^2 = q_2(c_0,c_1,c_2)\theta^2 - q_1(c_0,c_1,c_2)\theta + q_0(c_0,c_1,c_2)\ ,$$

where the q_i are explicit integral quadratic forms in the c_j. Thus we must solve the equations $q_2(c_0,c_1,c_2) = 0$, $q_1(c_0,c_1,c_2) = 1$, and then x is determined thanks to $q_0(c_0,c_1,c_2) = x$. The solubility of the first equation can easily be determined thanks to the Hasse–Minkowski theorem, an explicit solution can then be found using the algorithm explained in Section 6.3.3, and the general solution is given by Proposition 6.3.4 and its corollary. Thus there exist quadratic polynomials $P_i(X,Y)$ such that $q_2(c_0,c_1,c_2) = 0$ if and only if there exist coprime integers s and t and $d \in \mathbb{Q}$ such that $c_i = dP_i(s,t)$ for $0 \leqslant i \leqslant 2$. The equation $q_1(c_0,c_1,c_2) = 1$ can thus be written

$$q_1(P_0(s,t),P_1(s,t),P_2(s,t)) = 1/d^2\ ,$$

which is a hyperelliptic quartic equation. The rest of the process is similar to the case of rational 2-torsion: we must determine if this quartic equation is everywhere locally soluble. If it is not, we exclude $\overline{u}$ from the consideration of the points in the image of α. If it is, we look as intelligently as possible for rational points on the quartic. If we find one, we include $\overline{u}$ in the image of α (and $x = d^2q_0(P_0(s,t),P_1(s,t),P_2(s,t))$ is the explicit abscissa of the corresponding point in $E(\mathbb{Q})$). If we cannot find one, we are stuck and cannot determine $E(\mathbb{Q})$ without further work such as a second descent.

Remark. The group of $\overline{u} \in S_T(K,1)$ such that the corresponding quartic is everywhere locally soluble is the smallest group containing $E(\mathbb{Q})/2E(\mathbb{Q})$ which can be determined algorithmically using only a 2-descent. It is called the 2-*Selmer group* of the elliptic curve E and denoted $S_2(E)$. The quotient

of $S_2(E)$ by its subgroup $E(\mathbb{Q})/2E(\mathbb{Q})$ is the part of the so-called *Tate–Shafarevitch* group $Ш(E)$ of E killed by 2, so that we have an exact sequence (analogous to the one for $S_T(K)$, whence the name and the notation)

$$1 \longrightarrow\longrightarrow \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \longrightarrow S_2(E) \longrightarrow Ш(E)[2] \longrightarrow 1 .$$

The group $Ш(E)[2]$ is the the obstruction to performing a 2-descent. In the rational 2-torsion case, the groups $Ш(E)[2]$ and $Ш(\widehat{E})[2]$ are both obstructions to performing a 2-descent, although if either of them is trivial there is no obstruction to performing a second descent (I owe this remark to J. Cremona).

8.3.5 Examples of General 2-Descent

As examples of general 2-descent we consider two curves which we will need for the proof of Corollary 14.6.9 in Chapter 14.

Proposition 8.3.9. (1) *The curve E defined by $y^2 = x^3 - 16$ has rank 0 over $\mathbb{Q}$ and trivial torsion group, in other words $E(\mathbb{Q}) = \{\mathcal{O}\}$.*

(2) *The curve E defined by $y^2 = x^3 + 16$ has rank 0 over $\mathbb{Q}$ and torsion group of order 3 generated by $(x, y) = (0, 4)$, in other words $E(\mathbb{Q}) = \{\mathcal{O}, (0, \pm 4)\}$.*

Proof. The statements concerning the torsion subgroups easily follow from the results of Section 8.1.3, so we only compute the ranks. In both cases we have $K = \mathbb{Q}(\beta)$ with $\beta^3 = 2$, and $\theta = 2\varepsilon\beta$ where $\varepsilon = 1$ for the first equation and $\varepsilon = -1$ for the second. We compute that $\mathrm{disc}(R) = -2^8 \cdot 3^3$, and $\mathrm{disc}(K) = -2^2 3^3$, hence $I(\theta) = 2^6$, so T only contains prime ideals above 2. Since 2 is totally ramified as $2\mathbb{Z}_K = \mathfrak{p}_2^3$ with $\mathfrak{p}_2 = \beta\mathbb{Z}_K$and $\mathfrak{p}_2 \mid \theta$, we take $T = \{\mathfrak{p}_2\}$. Since the class number of K is equal to 1, it follows that an $\mathbb{F}_2$-basis of $S_T(K)$ is given by the classes modulo squares of the union of a generator of $\mathfrak{p}_2$ with the fundamental units and generator of torsion units, so here by the classes modulo squares of β, $\beta - 1$, and -1 of respective absolute norms 2, 1, and -1. Thus if $u = \beta^a(\beta - 1)^b(-1)^c$ the norm of u is a square in $\mathbb{Q}$ if and only if a and c are even. We deduce that the group $S_T(K, 1)$ of elements of $S_T(K)$ whose norm is a square is an $\mathbb{F}_2$-vector space of dimension 1 generated by $\beta - 1$.

It follows that for both curves the only quartics to consider are those corresponding to $\beta - 1$. Let us compute explicitly the quadratic forms q_0, q_1 and q_2 as above, in other words such that

$$(\beta - 1)(4c_2\beta^2 + 2\varepsilon c_1\beta + c_0)^2 = q_2(c_0, c_1, c_2)\theta^2 - q_1(c_0, c_1, c_2)\theta + q_0(c_0, c_1, c_2) ,$$

where we recall that $\theta = 2\varepsilon\beta$. We find

$$q_2(c_0,c_1,c_2) = 8c_2^2 - 2c_0c_2 - c_1^2 + \varepsilon c_0c_1$$
$$q_1(c_0,c_1,c_2) = 16\varepsilon c_2^2 - 16c_1c_2 + 2c_0c_1 - \varepsilon c_0^2/2$$
$$q_0(c_0,c_1,c_2) = -32\varepsilon c_1c_2 + 16c_0c_2 + 8c_1^2 - c_0^2$$

The equation $q_2(c_0,c_1,c_2) = 0$ has the evident solution $(c_0,c_1,c_2) = (\varepsilon,1,0)$. Thus by Proposition 6.3.4 we can easily parametrize the general solution: we may choose

$$M = \begin{pmatrix} 1 & 0 & \varepsilon \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} ,$$

hence $R = (s,0,t)^t$ so (after replacing d by εd in the formula of the proposition) the general solution is given by

$$c_0 = d(8t^2 - s^2), \quad c_1 = d\varepsilon(8t^2 - 2st), \quad c_2 = d(2t^2 - st) .$$

The condition $q_1 = 1$ gives the hyperelliptic quartic equations

$$\varepsilon(-96t^4 + 96st^3 - 24s^2t^2 + 4s^3t - s^4/2) = 1/d^2 ,$$

and since s and t are (coprime) integers we have $1/d = Y$ with $Y \in \mathbb{Z}$ (we cannot have $1/d = Y/2$ with Y odd otherwise the left hand side would have a denominator 4), hence s is even hence t is odd, and writing $s = 2s_1$ we see that $8 \mid Y^2$ hence $4 \mid Y$, so writing $Y = 4Y_1$ implies that $s_1 = 2s_2$ is even, giving the equation

$$2\varepsilon(-3t^4 + 12s_2t^3 - 12s_2^2t^2 + 8s_2^3t - 4s_2^3) = Y_1^2 ,$$

implying that Y_1 is even, hence that t is also even, a contradiction since s and t are assumed coprime. It follows that the quartic associated to $\beta - 1$ is not 2-adically soluble, hence the image of the 2-descent map α is trivial, proving that the rank of the two curves is equal to 0 by Corollary 8.3.2. □

8.4 Description of 3-Descent with Rational 3-Torsion Subgroup

Although 2-descent (possibly followed by a second descent) often works, there are many cases where it does not. The obstruction to this is the fact that the Tate–Shafarevitch group Ш of the curve has a nontrivial 2-part, analogous to the fact that the obstruction to nonunique factorization in number fields is a nontrivial class group. It is not necessary to understand precisely the definition of Ш to grasp the underlying philosophy.

When 2-descent does not work, we can try p-descent for a larger prime p (I will not give the precise definition), hoping that the p-part of Ш is trivial.

In the present section I will give the example of 3-descent when there exists a rational 3-torsion subgroup, and I thank T. Fisher and J. Cremona for many explanations. It is very analogous to 2-descent when there exists a rational 2-torsion point (Section 8.2.3).

8.4.1 Rational 3-Torsion Subgroups

We first have to emphasize that there is a difference between having a rational 3-torsion *point*, and having a rational 3-torsion *subgroup*, the latter meaning that there exists a subgroup of order 3 of $E(\mathbb{Q})$ which is stable under the action of Galois conjugation, but not necessarily composed of three rational points. More precisely, we set the following definition.

Definition 8.4.1. *Let E be an elliptic curve defined over a perfect commutative field K, and let $\mathcal{T}$ be a finite subgroup of E. We say that $\mathcal{T}$ is a K-rational subgroup of E if it is globally stable by any K-automorphism σ of any extension of K, in other words if $T \in \mathcal{T}$ implies that $\sigma(T) \in \mathcal{T}$.*

A more elegant (but strictly equivalent way) of expressing this definition is simply to say that $\mathcal{T}$ is stable under $\mathrm{Gal}(\overline{K}/K)$, without introducing the field L.

Proposition 8.4.2. *Let E be an elliptic curve defined over a perfect commutative field K of characteristic different from 2 and having a K-rational subgroup of order 3, necessarily of the form $\mathcal{T} = \{\mathcal{O}, T, -T\}$.*

(1) *The abscissa $x(T)$ of T is in K.*
(2) *Up to a change of x into $x - x_0$ for some $x_0 \in K$ the equation of E is $y^2 = x^3 + d(ax+1)^2$ for some $d \in K^*$ and $a \in K$, and then $T = (0, \sqrt{d})$.*
(3) *If in addition E has a K-rational point T of order 3, up to the same change the equation of E is $y^2 = x^3 + (ax+b)^2$ for some $a \in K$ and $b \in K^*$, and then $T = (0, b)$.*

Proof. We have necessarily $\mathcal{T} = \{\mathcal{O}, (x,y), (x,-y)\}$ with $x = x(T)$ and $y = y(T)$. Let L and G be as in the definition of a K-rational subgroup. If $\sigma \in G$ we must have $(\sigma(x), \sigma(y)) \in \mathcal{T}$, hence since it is an affine point we have $(\sigma(x), \sigma(y)) = (x, \pm y)$ for a suitable sign $\pm$. In particular $\sigma(x) = x$ for all $\sigma \in G = \mathrm{Gal}(L/K)$, so by Galois theory $x \in K$, proving (1). For (2), we note that thanks to (1), changing x into $x - x_0$ we may assume that $x(T) = 0$, so that $T = (0, \theta)$ with θ not necessarily in K. If the equation of E in the new coordinates is $y^2 = x^3 + Ax^2 + Bx + C$ then $C = \theta^2$, and $C \neq 0$ since otherwise T is also of order 2, which is impossible since $T \neq \mathcal{O}$. We thus have $x(2T) = (B/(2y(T)))^2 - A = (B^2 - 4AC)/(4C)$, and T has order 3 if and only if $x(2T) = x(-T) = x(T) = 0$, hence if and only if $B^2 - 4AC = 0$. Since $C \neq 0$ we thus have $Ax^2 + Bx + C = d(ax+1)^2$ for $d = C$ and $a = B/(2C)$, proving (2), and (3) is an immediate consequence. □

When E has a K-rational subgroup of order 3 it will be more convenient to work with a more general equation of the form

$$y^2 = x^3 + d(ax+b)^2$$

instead of $y^2 = x^3 + d(ax+1)^2$, which is of course equivalent to the preceding form since $d(ax+b)^2 = db^2((a/b)x+1)^2$ and $b \neq 0$, keeping in mind that we can change (d,a,b) into $(df^2, a/f, b/f)$. We note for future reference that the discriminant of the elliptic curve E is given by

$$\mathrm{disc}(E) = 16d^2b^3(27b - 4a^3d) ,$$

so that in particular $d \neq 0$, $b \neq 0$, and $27b - 4a^3d \neq 0$.

8.4.2 The Fundamental 3-Isogeny

From now on we follow what we have done for 2-descent in Section 8.2. The proofs are very similar, the main difference being that we will have to deal with elements of $\mathbb{Q}(\sqrt{d})$ and not only of $\mathbb{Q}$.

Thus from now on let E be an elliptic curve defined over $\mathbb{Q}$ having a rational subgroup of order 3, so that by the above proposition, up to translation of the x-coordinate we may assume that E is given by an equation of the form $y^2 = x^3 + d(ax+b)^2$. We fix the 3-torsion point $T = (0, b\sqrt{d})$, which may not be in $\mathbb{Q}$, but the group of order 3 $\{\mathcal{O}, T, -T\}$ is a rational subgroup.

As in Section 8.2 we will work with a pair of elliptic curves E and $\widehat{E}$, defined by a similar equation $y^2 = x^3 + \widehat{d}(\widehat{a}x + \widehat{b})^2$, where

$$\widehat{d} = -3d, \quad \widehat{a} = a, \quad \widehat{b} = \frac{27b - 4a^3d}{9} .$$

Note that $\widehat{b} = -\mathrm{disc}(E)/(144d^2b^3) \neq 0$, and since

$$\mathrm{disc}(\widehat{E}) = 16\widehat{d}^2\widehat{b}^3(27\widehat{b} - 4\widehat{a}^3\widehat{d}) = 1296\widehat{d}^2\widehat{b}^3 b ,$$

the curve $\widehat{E}$ is indeed nonsingular, hence is an elliptic curve.

This curve has the same form as E, and it thus has a rational subgroup of order 3 generated by

$$\widehat{T} = \left(0, \frac{27b - 4a^3d}{9}\sqrt{-3d}\right) .$$

Note that $\widehat{\widehat{d}} = 9d$, $\widehat{\widehat{a}} = a$ and $\widehat{\widehat{b}} = 9b$, hence the curve $\widehat{\widehat{E}}$ is the curve $y^2 = x^3 + 9d(ax+9b)^2$ which is trivially isomorphic to E by replacing x by $9x$ and y by $27y$.

Proposition 8.4.3. *For any $P = (x, y) \in E$ set*

$$\phi(P) = (\widehat{x}, \widehat{y}) = \left(\frac{x^3 + 4d((a^2/3)x^2 + abx + b^2)}{x^2}, \frac{y(x^3 - 4db(ax + 2b))}{x^3} \right)$$

for P not equal to $\pm T$ or $\mathcal{O}$, and set $\phi(T) = \phi(-T) = \phi(\mathcal{O}) = \widehat{\mathcal{O}}$. Then ϕ is a group homomorphism from E to $\widehat{E}$, whose kernel is equal to $\{\mathcal{O}, T, -T\}$. Dually, there exists a homomorphism $\widehat{\phi}$ from $\widehat{E}$ to E defined for $\widehat{P} = (\widehat{x}, \widehat{y})$ different from $\pm\widehat{T}$ and $\widehat{\mathcal{O}}$ by

$$\widehat{\phi}(\widehat{P}) = (x, y) = \left(\frac{\widehat{x}^3 + 4\widehat{d}((\widehat{a}^2/3)\widehat{x}^2 + \widehat{a}\widehat{b}\widehat{x} + \widehat{b}^2)}{9\widehat{x}^2}, \frac{\widehat{y}(\widehat{x}^3 - 4\widehat{d}\widehat{b}(\widehat{a}\widehat{x} + 2\widehat{b}))}{27\widehat{x}^3} \right)$$

and by $\widehat{\phi}(\widehat{T}) = \widehat{\phi}(-\widehat{T}) = \widehat{\phi}(\widehat{\mathcal{O}}) = \mathcal{O}$. Furthermore for all $P \in E$ we have $\widehat{\phi} \circ \phi(P) = 3P$, and for all $\widehat{P} \in \widehat{E}$ we have $\phi \circ \widehat{\phi}(\widehat{P}) = 3\widehat{P}$.

Proof. As in the 2-descent case, it is enough to check the given formulas. However this is not satisfactory and does not explain how they have been obtained. I give here a partial justification. For $P = (x, y) \in E$ we will set with evident notation $\widehat{x} = x(P) + x(P + T) + x(P - T) - x(\widehat{T})$ and $\widehat{y} = y\dfrac{d}{dx}\widehat{x}$ (in the case of a p-isogeny with a point T of order p we would set $\widehat{x} = \sum_{0 \leqslant i \leqslant p-1} x(P + iT)$ up to some constant translation). A small computation gives the formula of the proposition. In any case, we check that $\phi(P) \in \widehat{E}$ and that its kernel (more precisely the inverse image of $\widehat{\mathcal{O}}$) is our given group of order 3. We must now show that ϕ is a group homomorphism. In fact, since ϕ is a morphism of algebraic curves and sends $\mathcal{O}$ to $\widehat{\mathcal{O}}$ this follows from Theorem 7.1.5, but let us show this directly, as usual putting ourselves in the generic situation. Thus let P_1, P_2, P_3 be three points on E such that $P_1 + P_2 + P_3 = 0$, and let $y = mx + n$ be the line through those three points (which has this form since we are in the generic case). Once again I could give directly the equation of the line passing through the $\widehat{P}_i$, but instead let us find this equation. We thus want to find $\widehat{m}$ and $\widehat{n}$ such that $\widehat{y} = \widehat{m}\widehat{x} + \widehat{n}$ for $(x, y) = (x_i, y_i)$, $1 \leqslant i \leqslant 3$. Since $y_i = mx_i + n$ this implies that the x_i are three roots of the equation

$$(mx + n)(x^3 - 4db(ax + 2b))/x^3 = \widehat{m}(x^3 + 4d((a^2/3)x^2 + abx + b^2))/x^2 + \widehat{n} \, ,$$

in other words

$$(m - \widehat{m})x^4 + (n - \widehat{n} - (4/3)a^2d\widehat{m})x^3 \\ - 4abd(m + \widehat{m})x^2 - 4bd(b(2m + \widehat{m}) + an) - 8b^2dn = 0 \, .$$

Since we are in a generic situation this means that this polynomial must be divisible by the third degree polynomial of which the x_i are roots, in

other words by $x^3+d(ax+b)^2-(mx+n)^2$. Computing the remainder, we obtain three linear equations in the two unknowns $\widehat{m}$ and $\widehat{n}$, and after some computation we find that they are compatible and that

$$\widehat{m}=\frac{(n^2+3db^2)m-4adbn}{n^2-db^2} \quad \text{and}$$
$$\widehat{n}=\frac{n^3-(4/3)a^2dmn^2+(4abm^2+(4/3)a^3bd-9b^2)dn-4db^2m^3}{n^2-db^2}\,.$$

As in the 2-descent case, we could now start from these values and check that they satisfy $\widehat{y}_i=\widehat{m}\widehat{x}_i+\widehat{n}$ for $1\leqslant i\leqslant 3$, but here it is not necessary.

Applying the first part of the proposition to $\widehat{E}$ gives a map $\widehat{\phi_1}$ from $\widehat{E}$ to $\widehat{\widehat{E}}$, and composing with the isomorphism $(x,y)\mapsto(x/9,y/27)$ between $\widehat{\widehat{E}}$ and E gives the map $\widehat{\phi}$ of in the proposition. □

8.4.3 Description of the Image of ϕ

Although we want to copy almost verbatim what we have done in the 2-descent case, a difficulty arises from the fact that the 3-torsion point $T=(0,b\sqrt{d})$ does not necessarily have rational coordinates, although the group it generates is rational. It will thus be necessary to work in the field $K_d=\mathbb{Q}(\sqrt{d})$, which is equal to $\mathbb{Q}$ if d is a square, and is a quadratic field otherwise. Note however that this field is only a necessary *tool*, but that we will *not* need to consider the whole group $E(K_d)$.

Proposition 8.4.4. *Denote by $\widehat{I}=\phi(E(\mathbb{Q}))$ the image of the rational points of E in $\widehat{E}(\mathbb{Q})$.*

(1) *$\widehat{\mathcal{O}}\in\widehat{I}$, and $\pm\widehat{T}\in\widehat{I}$ if and only if $\widehat{d}=-3d$ is a square and* $\mathrm{disc}(E)=144d^2b^3\widehat{b}$ *is a cube in $\mathbb{Q}^*$ (or, equivalently, $\widehat{d}/(2\widehat{b})$ is a cube).*

(2) *Otherwise, a general point $\widehat{P}=(\widehat{x},\widehat{y})\in\widehat{E}(\mathbb{Q})$ different from $\pm\widehat{T}$ belongs to $\widehat{I}$ if and only if there exists $\gamma\in K_{\widehat{d}}=\mathbb{Q}(\sqrt{-3d})$ such that*

$$\gamma^3=\widehat{y}-(\widehat{a}\widehat{x}+\widehat{b})\sqrt{\widehat{d}}\,.$$

Proof. (1). Since $\widehat{I}\subset\widehat{E}(\mathbb{Q})$, it is clear that a necessary condition for $\widehat{T}$ to be in $\widehat{I}$ is that its ordinate be in $\mathbb{Q}$, in other words that $\widehat{d}=\delta^2$ for some $\delta\in\mathbb{Q}$. Thus assume that this is the case. Since the only affine points with zero x-coordinates on $\widehat{E}$ are $\pm\widehat{T}$, the definition of ϕ shows that $\widehat{T}\in\widehat{I}$ if and only if there exists $x\in\mathbb{Q}^*$ such that $x^3+4d((a^2/3)x^2+abx+b^2)=0$, and this last equation implies $x\neq 0$ since $bd\neq 0$. We compute that the discriminant of this polynomial is equal to $-(16/27)b^2d^2(4a^3d-27b)^2$, which is always strictly negative, so that our cubic equation has only one real root. An application of Cardano's formula or a direct check shows that this root is given by the simple formula

$$x = -\frac{3b\delta}{a\delta - (a^3\delta^3 + (81/4)b\delta)^{1/3}} .$$

It follows that there exists a rational root if and only if $a^3\delta^3 + (81/4)b\delta$ is a cube in $\mathbb{Q}^*$, hence if and only if its square $\widehat{d}(a^3\widehat{d} + (81/4)b)^2 = (27/4)^2\widehat{d}\widehat{b}^2$ is a cube in $\mathbb{Q}^*$, hence if and only if $\widehat{d}/(2\widehat{b})$ is a cube, if and only if $\mathrm{disc}(E) = (\widehat{d}/(2\widehat{b}))^2(4\widehat{b}\widehat{b})^3$ is a cube, proving (1).

(2). Since $x = 0$ implies $(x, y) = \pm T$ hence $\phi((x, y)) = \widehat{\mathcal{O}}$, we may assume $x \neq 0$. Thus let $(x, y) \in E(\mathbb{Q})$ with $x \neq 0$. A short computation shows that

$$\widehat{y} - (\widehat{a}\widehat{x} + \widehat{b})\sqrt{\widehat{d}} = \left(\frac{y - ((a/3)x + b)\sqrt{\widehat{d}}}{x}\right)^3 ,$$

showing that this expression is a cube in $K_{\widehat{d}}$, more precisely that it is equal to γ^3, where $\gamma = (y - ((a/3)x + b)\sqrt{\widehat{d}})/x$. Conversely, assume that $\widehat{P} = (\widehat{x}, \widehat{y}) \in \widehat{E}(\mathbb{Q})$ is such that there exists γ such that $\gamma^3 = \widehat{y} - (\widehat{a}\widehat{x} + \widehat{b})\sqrt{\widehat{d}}$. Note that $\gamma = 0$ implies that

$$0 = \widehat{y}^2 - \widehat{d}(\widehat{a}\widehat{x} + \widehat{b})^2 = \widehat{x}^3 ,$$

hence that $\widehat{x} = 0$, i.e., $\widehat{P} = \pm\widehat{T}$, and conversely. Therefore in the present case we have $\gamma \neq 0$. We have the following lemma.

Lemma 8.4.5. *Set* $u = (\gamma + \widehat{x}/\gamma)/2$ *and* $v = (\gamma - \widehat{x}/\gamma)/(2\sqrt{\widehat{d}})$.

(1) u *and* v *are in* $\mathbb{Q}$.
(2) *We have*

$$(\widehat{x}/\gamma)^3 = \widehat{y} + (\widehat{a}\widehat{x} + \widehat{b})\sqrt{\widehat{d}} .$$

(3) *We have* $b = -(v + a/3)(u^2 - d(v - 2a/3)^2)$.

Proof. (1). This is trivial if $\sqrt{\widehat{d}} \in \mathbb{Q}$, so assume that this is not the case. Then denoting by $\sigma(\gamma)$ the conjugate of γ in the quadratic field $K_{\widehat{d}}$ we have

$$(\gamma\sigma(\gamma))^3 = \widehat{y}^2 - \widehat{d}(\widehat{a}\widehat{x} + \widehat{b})^2 = \widehat{x}^3 .$$

Since $\gamma\sigma(\gamma)$ and $\widehat{x}$ are in $\mathbb{Q}$ this implies that $\gamma\sigma(\gamma) = \widehat{x}$, so that $\widehat{x}/\gamma = \sigma(\gamma)$, proving (1).

(2). This is clear since

$$\left(\frac{\widehat{x}}{\gamma}\right)^3 = \frac{\widehat{y}^2 - \widehat{d}(\widehat{a}\widehat{x} + \widehat{b})^2}{\widehat{y} - (\widehat{a}\widehat{x} + \widehat{b})\sqrt{\widehat{d}}} = \widehat{y} + (\widehat{a}\widehat{x} + \widehat{b})\sqrt{\widehat{d}} .$$

(3). We may thus write $\gamma = u + v\sqrt{\widehat{d}}$ and $\widehat{x}/\gamma = u - v\sqrt{\widehat{d}}$, hence $\widehat{x} = u^2 - \widehat{d}v^2 = u^2 + 3dv^2$. We compute $\gamma^3 - (\widehat{x}/\gamma)^3$ in two different ways. On the one hand we have

$$\gamma^3 - (\widehat{x}/\gamma)^3 = 2\sqrt{\widehat{d}}(3u^2v + v^3\widehat{d}) = -2\sqrt{\widehat{d}}(3dv^3 - 3u^2v) \ ,$$

while by (2) we have

$$\gamma^3 - (\widehat{x}/\gamma)^3 = -2\sqrt{\widehat{d}}(\widehat{a}\widehat{x} + \widehat{b}) = -2\sqrt{\widehat{d}}(a(u^2 + 3dv^2) + (27b - 4a^3d)/9) \ .$$

Identifying both expressions gives

$$b = -u^2(v + a/3) + d(v^3 - av^2 + 4a^3/27) = (v + a/3)(d(v - 2a/3)^2 - u^2) \ ,$$

proving the lemma. □

It is now easy to finish the proof of the proposition. Since $b \neq 0$, the lemma implies that $v + a/3 \neq 0$. Thus we can set

$$x = -b/(v + a/3) = u^2 - d(v - 2a/3)^2 \quad \text{and} \quad y = ux = u^3 - du(v - 2a/3)^2 \ .$$

We thus have $y^2 = u^2x^2 = u^2b^2/(v + a/3)^2$, while by the lemma we have

$$\begin{aligned}(v + a/3)^3(x^3 + d(ax + b)^2) &= -b^3 + db^2(v + a/3)(-a + v + a/3)^2 \\ &= b^2(-b + d(v + a/3)(v - 2a/3)^2) \\ &= b^2(v + a/3)u^2 \ ,\end{aligned}$$

so that we indeed have $y^2 = x^3 + d(ax+b)^2$, hence $(x, y) \in E(\mathbb{Q})$. Furthermore we have $\phi((x, y)) = (\widehat{x}_1, \widehat{y}_1)$, with

$$\begin{aligned}\widehat{x}_1 &= x + 4d(a^2/3 + a(b/x) + (b/x)^2) \\ &= u^2 - d(v - 2a/3)^2 + d(4a^2/3 - 4a(v + a/3) + 4(v + a/3)^2) \\ &= u^2 + 3dv^2 = \widehat{x}\end{aligned}$$

and

$$\begin{aligned}\widehat{y}_1 &= u(x - 4d(a(b/x) + 2(b/x)^2)) \\ &= u(u^2 - d(v - 2a/3)^2 + d(4a(v + a/3) - 8(v + a/3)^2)) = u(u^2 - 9v^2d) \ .\end{aligned}$$

On the other hand by the above lemma we have

$$\widehat{y} = (\gamma^3 + (\widehat{x}/\gamma)^3)/2 = u^3 + 3uv^2\widehat{d} = u(u^2 - 9v^2d) = \widehat{y}_1 \ ,$$

finishing the proof. □

The following corollary is immediate by considering the dual isogeny.

Corollary 8.4.6. *Set $I = \widehat{\phi}(\widehat{E}(\mathbb{Q}))$.*

(1) *$\mathcal{O} \in I$, and $\pm T \in I$ if and only if d is a square and $d/(2b)$ is a cube in $\mathbb{Q}^*$.*

(2) *Otherwise, a general point $P = (x, y) \in E(\mathbb{Q})$ different from $\pm T$ belongs to I if and only if there exists $\gamma \in K_d = \mathbb{Q}(\sqrt{d})$ such that $\gamma^3 = y - (ax + b)\sqrt{d}$.*

8.4.4 The Fundamental 3-Descent Map

We continue to imitate what we have done for 2-descent. We keep the assumptions and notation of the preceding sections. In particular, recall that we have set $K_d = \mathbb{Q}(\sqrt{d})$, which is equal to $\mathbb{Q}$ when d is a square.

Definition 8.4.7. *We define the* 3-descent map α *from the group* $E(\mathbb{Q})$ *to the multiplicative group* K_d^*/K_d^{*3} *as follows.*

(1) $\alpha(\mathcal{O}) = 1$, *and if* $T \in E(\mathbb{Q})$ (*in other words if* $\sqrt{d} \in \mathbb{Q}^*$) *then* $\alpha(T) = 4db^2$.
(2) *When* $P = (x, y) \in E(\mathbb{Q})$ *with* $P \neq T$ *then* $\alpha((x, y)) = y - (ax + b)\sqrt{d}$.

In the above, all the values are of course understood modulo the multiplicative action of K_d^{*3}.

The main result is the following.

Proposition 8.4.8. (1) *The* 3*-descent map* α *is a group homomorphism.*
(2) *The kernel of* α *is equal to* $\widehat{\phi}(\widehat{E}(\mathbb{Q}))$.
(3) *The map* α *induces an injective group homomorphism from* $E(\mathbb{Q})/\widehat{\phi}(\widehat{E}(\mathbb{Q}))$ *to the subgroup of* K_d^*/K_d^{*3} *of elements whose norm is trivial in* $\mathbb{Q}^*/\mathbb{Q}^{*3}$ *when* $\sqrt{d} \notin \mathbb{Q}$, *and to* $\mathbb{Q}^*/\mathbb{Q}^{*3}$ *otherwise.*

Proof. If $P = (x, y) \neq T$, then $\alpha(-P) = \alpha((x, -y)) = -y - (ax + b)\sqrt{d}$, so $\alpha(P)\alpha(-P) = -(y^2 - d(ax + b)^2) = (-x)^3 \in \mathbb{Q}^{*3}$, and if $P = T = (0, b\sqrt{d})$ then by definition

$$\alpha(T)\alpha(-T) = 4db^2\alpha((0, -b\sqrt{d})) = (-2b\sqrt{d})^3 \in K_d^{*3},$$

so α sends inverses to inverses. Thus we must show that if $P_1 + P_2 + P_3 = \mathcal{O}$ then $\alpha(P_1)\alpha(P_2)\alpha(P_3) \in K_d^{*3}$. If one of the P_i is equal to $\mathcal{O}$ we are in the case that we have just treated, so we exclude that case. If one of the P_i is equal to T then either all three P_i are equal to T, and the result is clear, or only one, say P_1, is equal to T. In that case none of the P_i is equal to $2T$, otherwise the third one would be equal to $\mathcal{O}$. Thus by what we have proved about inverses we have

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = (\alpha(-P_1)\alpha(-P_2)\alpha(-P_3))^{-1}$$

(as usual modulo the multiplicative action of K_d^{*3}), and now none of the $-P_i$ is equal to $\mathcal{O}$ or to T, so we are in the generic case which we now treat.

Let $y = mx + n$ be the equation of the line going through the points $P_i = (x_i, y_i)$. Note that we can indeed choose the equation to be of this form since the excluded equations are $x = k$, which intersect the curve E in two affine points together with $\mathcal{O}$, a case which we have excluded. The x_i are thus the three roots of the polynomial $f(x) = x^3 + d(ax + b)^2 - (mx + n)^2$. An easy computation shows that

$$\prod_i (y_i - (ax_i + b)\sqrt{d}) = \prod_i (mx_i + n - (ax_i + b)\sqrt{d}) = (n - b\sqrt{d})^3 \in K_d^3 ,$$

finishing the proof of (1).

(2). This follows immediately from Corollary 8.4.6: $\mathcal{O}$ is evidently in the kernel of α, and by definition $T \in \mathrm{Ker}(\alpha)$ if and only if $4db^2$ is a cube, if and only if $(d/2b) = 4db^2/(2b)^3$ is a cube, hence by the corollary if and only if $T \in I$. Finally a point $P = (x, y)$ different from $\mathcal{O}$ and T is in the kernel of α if and only if there exists $\gamma \in K_d^*$ such that $\gamma^3 = y - (ax + b)\sqrt{d}$, hence by the corollary if and only if $P \in I$, proving (2).

(3). From (1) and (2) we deduce that α induces an injection $\overline{\alpha}$ from $E(\mathbb{Q})/\widehat{\phi}(\widehat{E}(\mathbb{Q}))$ to K_d^*/K_d^{*3}. If $\sqrt{d} \in \mathbb{Q}^*$ the image of $\overline{\alpha}$ is in $\mathbb{Q}^*/\mathbb{Q}^{*3}$ and there is nothing else to say. Otherwise $T \notin E(\mathbb{Q})$ and for $P = (x, y) \neq \mathcal{O}$ we have that $\mathcal{N}_{K_d/\mathbb{Q}}(\alpha((x, y))) = x^3$ is a cube in $\mathbb{Q}^*$, proving the proposition. □

We leave to the reader to state and prove an analogue of Proposition 8.2.4 (3) and (4), see Exercise 15, and we will not study 3-descent any further, but apply it to the Diophantine equations $ax^3+by^3+cz^3$ considered in Chapter 6.

8.4.5 Application to $ax^3 + by^3 + cz^3 = 0$

The relation between the Diophantine equation of the title and 3-descent is the following. Let a, b, and c be three nonzero rational numbers, let E_{abc} be the elliptic curve with affine equation $y^2 = x^3 + (4abc)^2$. This is an equation of the form considered above with $d = 1$, hence $K_d = \mathbb{Q}$ and $T = (0, 4abc)$ is a rational point of order 3. We have $\alpha(T) = 4(4abc)^2 = (abc)^2$ up to cubes, and for $P = (x, y) \neq T$ we have $\alpha(P) = y - 4abc$. Finally, by Proposition 8.4.8 we know that α is a group homomorphism.

Proposition 8.4.9. *Let $\mathcal{C}$ be the cubic curve with projective equation $ax^3 + by^3 + cz^3 = 0$, and define*

$$\phi(x, y, z) = (-4abcxyz,\ -4abc(by^3 - cz^3),\ ax^3) .$$

(1) *The map ϕ sends $\mathcal{C}(\mathbb{Q})$ into $E(\mathbb{Q})$ (of course in projective coordinates).*

(2) *Let G be the set of $(X, Y, Z) \in E(\mathbb{Q})$ such that there exists $\lambda \in \mathbb{Q}^*$ such that $c(Y - 4abcZ) = bZ\lambda^3$. The image $\phi(\mathcal{C}(\mathbb{Q}))$ is equal to G, together with $\mathcal{O}$ if $c/b \in \mathbb{Q}^{*3}$, and together with T if $b/a \in \mathbb{Q}^{*3}$. More precisely, if (X, Y, Z) is such a point different from $\mathcal{O}$ and T then*

$$(x, y, z) = (2bc\lambda Z,\ -cX,\ b\lambda^2 Z) \in \mathcal{C}(\mathbb{Q})$$

is a preimage of (X, Y, Z), if $c/b = \gamma^3 \in \mathbb{Q}^{*3}$ a preimage of $\mathcal{O}$ is $(0, -\gamma, 1)$, and if $b/a = \beta^3 \in \mathbb{Q}^{*3}$ a preimage of T is $(-\beta, 1, 0)$.

(3) *$\mathcal{C}(\mathbb{Q})$ is nonempty if and only if the class of b/c modulo cubes lies in the image of the 3-descent map α from $E_{abc}(\mathbb{Q})$ to $\mathbb{Q}^*/\mathbb{Q}^{*3}$.*

Proof. (1). Once again the proof is a series of simple verifications: set $\phi(x,y,z) = (X,Y,Z)$. Then when $ax^3 + by^3 + cz^3 = 0$ we have

$$\begin{aligned} Y^2Z - (4abc)^2Z^3 &= (4abc)^2ax^3((by^3 - cz^3)^2 - (ax^3)^2) \\ &= (4abc)^2ax^3((by^3 - cz^3)^2 - (by^3 + cz^3)^2) \\ &= -(4abc)^2ax^3(4bcy^3z^3) = (-4abcxyz)^3 = X^3 \ . \end{aligned}$$

Furthermore we cannot have $X = Y = Z = 0$ since otherwise $x = 0$, hence $by^3 + cz^3 = 0$, and $by^3 - cz^3 = 0$, hence $x = y = z = 0$, which is excluded. Thus $\phi(x,y,z) \in E(\mathbb{Q})$, proving (1).

(2). Note that

$$c(Y - 4abcZ) = -4abc^2(by^3 - cz^3 + ax^3) = 8abc^3z^3 = bZ\lambda^3$$

with $\lambda = 2cz/x \in \mathbb{Q}^*$ when x and z are nonzero, so $\phi(x,y,z) \in G$ in that case. It is immediate to check that $\mathcal{O}$ and T are not in G. Now x can be equal to 0 if and only if $c/b = (-y/z)^3 \in \mathbb{Q}^{*3}$, and in that case we have $\phi(0,y,z) = \mathcal{O}$. Similarly z can be equal to 0 if and only if $b/a = (-x/y)^3 \in \mathbb{Q}^{*3}$, and in that case it is clear that $\phi(x,y,0) = T$, proving (2).

(3). Evidently $\mathcal{C}(\mathbb{Q})$ is nonempty if and only if $\phi(\mathcal{C}(\mathbb{Q}))$ is nonempty, hence thanks to (2) if and only if either there exists $(X,Y,Z) \in E(\mathbb{Q})$ different from $\mathcal{O}$ and T, and $\lambda \in \mathbb{Q}^*$, such that $c(Y - 4abcZ) = bZ\lambda^3$, or if $c/b \in \mathbb{Q}^{*3}$, or if $b/a \in \mathbb{Q}^{*3}$. In projective coordinates the 3-descent map α is defined for (X,Y,Z) different from $\mathcal{O}$ and T by $\alpha((X,Y,Z)) = (Y - 4abcZ)/Z$, hence the first case implies that b/c is in the image of α in $\mathbb{Q}^*/\mathbb{Q}^{*3}$. In the second case, $b/c \in \mathbb{Q}^{*3}$ which is the image of $\mathcal{O}$. Finally in the third case we have

$$\alpha(T) = (abc)^2 = (b/c)(b/a)(ac)^3 = b/c \pmod{\mathbb{Q}^{*3}} \ ,$$

proving (3). □

Once again I thank T. Fisher for explaining this proposition to me.

Thus to check whether an equation $ax^3 + by^3 + cz^3 = 0$ has a nontrivial solution we proceed as follows. Using either `mwrank` or the 2-descent methods, we compute if possible the complete Mordell–Weil group $E(\mathbb{Q})$ of the curve with affine equation $y^2 = x^3 + (4abc)^2$, and we also compute the torsion subgroup (which we know will contain the subgroup of order 3 generated by T). If $P_1, \ldots, P_r$ form a basis of the free part of $E(\mathbb{Q})$ then $P_0 = T$, $P_1, \ldots, P_r$ form an $\mathbb{F}_3$-basis of $E(\mathbb{Q})/3E(\mathbb{Q})$. We then check whether the class of b/c modulo cubes belong to the group generated by the $\alpha(P_i) \in \mathbb{Q}^*/\mathbb{Q}^{*3}$, which is done using simple linear algebra over $\mathbb{F}_3$.

Example. To illustrate, consider the equation $x^3+55y^3+66z^3$. Using Proposition 6.4.2 we check that it is everywhere locally soluble, but none of the results given in Section 6.4.4 allow us to determine whether or not the equation is globally soluble.

Thus we consider the curve E with affine equation $y^2 = x^3 + (4\cdot 55\cdot 66)^2$. We find that the torsion subgroup has order 3 and generated by $P_0 = T = (0, 14520)$. In less than a second the `mwrank` program tells us that the curve has rank 1, a generator being $P_1 = (504, 18408)$. We have (modulo cubes) $\alpha(P_0) = 2^2\cdot 3^2\cdot 5^2\cdot 11$ and $\alpha(P_1) = 2\cdot 3^2$, while $b/c = 2^2\cdot 3^2\cdot 5$. Here the linear algebra can be done naively: if $b/c = \alpha(uP_0+vP_1) = \alpha(P_0)^u\alpha(P_1)^v$, where u and v are defined modulo 3 we see that $u = 0$ because of the 11 factor, which is impossible since there is a factor of 5 in b/c and none in $\alpha(P_1)$. This shows that our equation has no nontrivial solutions in $\mathbb{Q}$.

8.5 The Use of $L(E, s)$

8.5.1 Introduction

We have seen in Section 8.1.2 the definition and main properties of the L-function $L(E, s)$ attached to an elliptic curve E defined over $\mathbb{Q}$. Thanks to the work of Wiles et al. (see Theorem 8.1.4), we know that $L(E, s)$ extends to an entire function with a functional equation of the form $\Lambda(E, 2-s) = \varepsilon(E)\Lambda(s)$, where $\Lambda(E, s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E, s)$ and $\varepsilon(E) = \pm 1$. Finally the Birch–Swinnerton-Dyer Conjecture 8.1.7 predicts that the rank $r(E)$ should be equal to the order of vanishing of $L(E, s)$ at $s = 1$. This conjecture is a theorem when the order of vanishing is equal to 0 or 1.

Even though BSD is a conjecture, it suggests many useful approaches. First, it implies the *parity conjecture*, saying that $(-1)^{r(E)} = \varepsilon(E)$. Since there exists an algorithm to compute $\varepsilon(E)$, this gives a conjectural parity for $r(E)$. For instance, this explains the remark made after the proof of Proposition 8.2.15.

When the parity does not suffice to determine the rank, we proceed as follows. We search more or less intelligently for rational points on the curve. There are many methods to do this, but we simply mention that even if a 2-descent has not succeeded in giving the rank, it still may help in the search for points.

If after a sufficiently long search we find sufficiently many independent points compared to the upper bound on the rank given by descent arguments, we are happy and can conclude. Unfortunately in many cases this does not happen, either because the points we are looking for have a very large height, or more simply because the rank is simply not equal to the upper bound given by descent. It is in this case that we must appeal to the computation of $L(E, s)$, hence rely on the BSD conjecture.

The numerical computation of $L(E,s)$ (and of its derivatives) involves two completely different tasks: first the evaluation of some transcendental functions (the exponential function in the simplest case), which will be studied in great detail below, and second the arithmetic computation of the coefficients $a_p(E)$. In the case of a general elliptic curve these coefficients are computed either using Legendre symbol sums (Lemma 7.3.9) for small p, by the Shanks–Mestre baby step giant step method (see Algorithm 7.4.12 of [Coh0]) for moderate p, which should be sufficient for the computation of $L(E,s)$, or even by the Schoof–Elkies–Atkin algorithm for very large p (see for instance [Coh-Fre]).

However, in the special case of an elliptic curve E with *complex multiplication* the computation of $a_p(E)$ can be done quite simply. In the next subsection we explain how this is done in the important special cases of complex multiplication by $\mathbb{Z}[i]$ and $\mathbb{Z}[\rho] = \mathbb{Z}[\zeta_3]$.

8.5.2 The Case of Complex Multiplication

We begin by the following.

Proposition 8.5.1. *Let E be the elliptic curve with affine equation $y^2 = x^3 - x$, and as usual for a prime p set $a_p(E) = p + 1 - |E(\mathbb{F}_p)|$. Then when $p = 2$ or $p \equiv 3 \pmod 4$ we have $a_p(E) = 0$, and when $p \equiv 1 \pmod 4$ we have $a_p(E) = -\left(\frac{2}{p}\right)2a = (-1)^{(p+3)/4}2a$, where $p = a^2 + b^2$ with $a \equiv -1 \pmod 4$.*

Proof. Assume that $p \equiv 3 \pmod 4$. Since $\left(\frac{-1}{p}\right) = -1$ it follows that for each x not equal to 0 or ± 1 there is exactly one value in $\{x, -x\}$ such that $x^3 - x$ is a square. It follows that $a_p(E) = 0$ in that case, and it is also immediate that $a_2(E) = 0$ (more generally, if E has complex multiplication by an imaginary quadratic order of discriminant D then $a_p(E) = 0$ when $\left(\frac{D}{p}\right) = -1$, exactly for the same reason). Assume now that $p \equiv 1 \pmod 4$. By Proposition 2.5.20 we know that there exists a character χ of order 4 and that $J(\chi,\chi) = a + bi$ with $a^2 + b^2 = p$, $2 \mid b$, and $a \equiv -1 \pmod 4$. It is slightly more natural to reason backward and start from the result. Since χ has exact order 4, When n is not a square we have $\chi(n) = \pm i$, hence $\Re(\chi(n)) = 0$. Since χ^2 is equal to the Legendre symbol we have

$$2a = 2\Re(J(\chi,\chi)) = 2\sum_{x\in\mathbb{F}_p}\Re(\chi(x(1-x))) = 2\sum_{\substack{x\in\mathbb{F}_p\\ \exists y\in\mathbb{F}_p,\ x(1-x)=y^2}}\left(\frac{y}{p}\right)$$

$$= \sum_{\substack{x,y\in\mathbb{F}_p\\ (2x-1)^2=1-4y^2}}\left(\frac{y}{p}\right) = \left(\frac{2}{p}\right)\sum_{\substack{X,Y\in\mathbb{F}_p\\ X^2=1-Y^2}}\left(\frac{Y}{p}\right)$$

$$= \left(\frac{2}{p}\right)\sum_{Y\in\mathbb{F}_p}\left(\frac{Y}{p}\right)\sum_{X\in\mathbb{F}_p,\ X^2=1-Y^2}1 = \left(\frac{2}{p}\right)\sum_{Y\in\mathbb{F}_p}\left(\frac{Y}{p}\right)\left(1+\left(\frac{1-Y^2}{p}\right)\right)$$

$$= \left(\frac{2}{p}\right)\sum_{Y\in\mathbb{F}_p}\left(\frac{Y^3-Y}{p}\right) = -\left(\frac{2}{p}\right)a_p\ ,$$

since by Lemma 7.3.9 we have $a_p(E) = -\sum_{Y\in\mathbb{F}_p}\left(\frac{Y^3-Y}{p}\right)$, proving the proposition. □

Corollary 8.5.2. *For $n \neq 0$ let E_n be the elliptic curve with affine equation $y^2 = x^3 - n^2x$. When $p \mid 2n$ or $p \equiv 3 \pmod 4$ we have $a_p(E_n) = 0$, and when $p \nmid 2n$ and $p \equiv 1 \pmod 4$ we have*

$$a_p(E_n) = -\left(\frac{2n}{p}\right)2a\ ,$$

where $p = a^2 + b^2$ with $a \equiv -1 \mod 4$.

Proof. Immediate from Proposition 7.3.14 and the above proposition. □

It follows from this corollary that, even without using Tunnell's Theorem 6.12.4, but still assuming BSD, it is very easy to make large tables of congruent numbers: using Cornacchia's algorithm as explained in the remarks following Proposition 2.5.20 we compute decompositions $p = a^2 + b^2$ with $a \equiv -1 \pmod 4$ for a large number of primes $p \equiv 1 \pmod 4$. Thanks to the above corollary it is then immediate to compute an approximate value of $L(E_n, 1)$, and we conclude thanks to BSD and Proposition 6.12.1.

We perform a similar task for cubic twists of the elliptic curve $y^2 = x^3 + 1$, having complex multiplication by $\mathbb{Z}[\rho]$, where we recall that ρ denotes a primitive cube root of unity. The handling of cubic twists being slightly more delicate, we consider directly the curve with equation $y^2 = x^3 + n$, which is in fact a *sextic* twist.

Proposition 8.5.3. *Let E_n be the elliptic curve with affine equation $y^2 = x^3 + n$. When $p \mid 3n$ or $p \equiv 2 \pmod 3$ we have $a_p(E_n) = 0$, and when $p \nmid 3n$ and $p \equiv 1 \pmod 3$ we have*

$$a_p(E_n) = \left(\frac{n}{p}\right) \begin{cases} b-2a & \text{if } (4n)^{(p-1)/3} \equiv 1 \pmod p \\ a+b & \text{if } (4n)^{(p-1)/3} \equiv -a/b \pmod p \\ a-2b & \text{if } (4n)^{(p-1)/3} \equiv (a-b)/b \pmod p, \end{cases}$$

where $p = a^2 - ab + b^2$ *with* $3 \mid b$ *and* $a \equiv -1 \mod 3$.

Proof. The case $p \mid 3n$ being immediate we assume $p \nmid 3n$. When $p \equiv 2 \pmod 3$ the map $x \mapsto x^3$ is a bijection of $\mathbb{F}_p$ onto itself, since $3 \nmid |\mathbb{F}_p^*| = p-1$. It follows that for every value of y there is exactly one value of x, hence that $|E_n(\mathbb{F}_p)| = p+1$ so that $a_p(E_n) = 0$. Assume now that $p \equiv 1 \pmod 3$, fix a primitive root g modulo p, and let χ be a character of order 3. Changing if necessary χ into $\overline{\chi} = \chi^2$ we may assume that $\chi(g) = \rho$. By Proposition 2.5.20, we know that $J(\chi,\chi) = a + b\rho$ with $a^2 - ab + b^2 = p$, $3 \mid b$ and $a \equiv -1 \pmod 3$. On the other hand, since $1+\rho+\rho^2 = 0$ it is clear that the expression $1 + \chi(x) + \chi(x^2)$ is equal to 1 if $x = 0$, to 3 if x is a cube in $\mathbb{F}_p$, and to 0 otherwise. Since $\chi(x^2) = \overline{\chi}(x)$ it follows that for a given y the number of x such that $x^3 = y^2 - 1$ is equal to $1 + \chi(y^2-1) + \overline{\chi}(y^2-1)$, hence

$$|E_n(\mathbb{F}_p)| = p + 1 + 2\Re\left(\sum_{y \in \mathbb{F}_p} \chi(y^2 - n)\right),$$

in other words

$$a_p(E_n) = -2\Re\left(\sum_{y \in \mathbb{F}_p} \chi(y^2 - n)\right).$$

Assume first that $\left(\frac{n}{p}\right) = 1$, and let $k \in \mathbb{Z}$ be such that $k^2 \equiv n \pmod p$. Setting $y = k(2t-1)$ (which is a bijection since $p \mid 2n$) and using $\chi(-1) = 1$, we thus have

$$a_p(E_n) = -2\Re\left(\chi(-4k^2)\sum_{t \in \mathbb{F}_p} \chi(t - t^2)\right) = -2\Re(\chi(4n)J(\chi,\chi)).$$

Now by Exercise 30 of Chapter 2 we know that the integers a and b such that $J(\chi,\chi) = a + b\rho$ are completely determined by the congruence $a + bg^{(p-1)/3} \equiv 0 \pmod p$, since we have chosen χ such that $\chi(g) = \rho$, so that $g^{(p-1)/3} \equiv -a/b \pmod p$. Since g is a primitive root modulo p there exists k such that $4n \equiv g^k \pmod p$, hence $\chi(4n) = \chi(g)^k = \rho^k = \rho^{k \bmod 3}$. On the other hand

$$(4n)^{(p-1)/3} \equiv g^{k(p-1)/3} \equiv (-a/b)^k \pmod p,$$

and $k \bmod 3$ is determined by this congruence. The proposition follows when n is a quadratic residue modulo p by distinguishing the three possible values of $k \bmod 3$ and noting that $(-a/b)^2 \equiv (a-b)/b \pmod p$.

If n is a quadratic nonresidue modulo p, we note that the twist $E_{n,n}$ of E_n by n itself has equation $ny^2 = x^3 + n$, which is isomorphic to $Y^2 = X^3 + n^4$

by setting $Y = ny$ and $X = ny$. Since n^4 is trivially a quadratic residue, on the one hand by what we have just proved we have

$$a_p(E_{n,n}) = -2\Re\left(\chi(4n^4)(a+b\rho)\right) = -2\Re\left(\chi(4n)(a+b\rho)\right) \ ,$$

and on the other hand by Proposition 7.3.14 we have $a_p(E_{n,n}) = \left(\frac{n}{p}\right)a_p(E_n)$, so the result follows in general. □

In the special case $n = 1$, since by Proposition 2.5.20 we know the cubic character of 2, hence of 4, we obtain:

Corollary 8.5.4. *When $p = 3$ or $p \equiv 2 \pmod 3$ we have $a_p(E_1) = 0$, and when $p \equiv 1 \pmod 3$ we have*

$$a_p(E_1) = \begin{cases} b - 2a & \text{if } b \text{ is even} \\ a + b & \text{if } a \text{ and } b \text{ are odd} \\ a - 2b & \text{if } a \text{ is even and } b \text{ is odd,} \end{cases}$$

where $p = a^2 - ab + b^2$ with $3 \mid b$ and $a \equiv -1 \mod 3$.

Proof. See Exercise 17. □

As in the preceding example it follows from the proposition that assuming BSD it is very easy to make large tables of $L(E_n, 1)$, since once again using Cornacchia's algorithm it is immediate to compute the decompositions $p = a^2 - ab + b^2$ with $3 \mid b$ and $a \equiv -1 \pmod 3$. Thanks to Proposition 7.2.3 and the remarks following it, this enables us for instance to compute tables of integers c which are sums of two rational cubes, by computing $L(E_{-432c^2}, 1)$ or $L(E_{16c^2}, 1)$ (which are equal since the two curves are isogenous).

8.5.3 Numerical Computation of $L^{(r)}(E, 1)$

In this section we will explain how to compute numerically the derivatives of $L(E, s)$. Once again we emphasize that using a suitable error analysis it is always easy to prove that a given real number (here $L^{(r)}(E, 1)$) is *not* equal to 0 (of course when it is not), while it is impossible to prove that it *is* equal to 0. The only thing we can do is have a reasonable certainty if the value we obtain is less in absolute value than 10^{-20}, say.

We refer to [Dok] for a detailed analysis and implementation of the general problem of computing special values of L-functions and their derivatives, using a slightly different approach than that given here.

By Wiles et al., we know that $L(E, s)$ satisfies a functional equation of standard form. It is not sufficiently well-known that this automatically implies that there exists an exponentially convergent series for computing $L(E, s)$ and its derivatives numerically. The result is as follows (see for instance [Coh1] Section 10.3 for a proof). Recall first the following definition:

Definition 8.5.5. *The incomplete gamma function is defined for* $\Re(x) > 0$ *and all* $s \in \mathbb{C}$ *by*

$$\Gamma(s,x) = x^s \int_1^\infty e^{-xt} t^s \, \frac{dt}{t} \, ,$$

so that in particular if $x \in \mathbb{R}_{>0}$

$$\Gamma(s,x) = \int_x^\infty t^s e^{-t} \, \frac{dt}{t} \, .$$

Proposition 8.5.6. *Write* $L(E,s) = \sum_{n \geqslant 1} a_n(E) n^{-s}$, *and let* N *and* $\varepsilon(E)$ *be as above. Then for all* t_0 *we have*

$$L(E,s) = \sum_{n \geqslant 1} \frac{a_n(E)}{n^s} \Gamma\Big(s, \frac{2\pi n}{t_0\sqrt{N}}\Big) + \varepsilon(E) \Big(\frac{2\pi}{\sqrt{N}}\Big)^{2s-2} \sum_{n \geqslant 1} \frac{a_n(E)}{n^{2-s}} \Gamma\Big(2-s, \frac{2\pi n t_0}{\sqrt{N}}\Big) \, .$$

If $\varepsilon(E) = -1$ we clearly have $L(E,1) = 0$. If $\varepsilon(E) = 1$ we obtain:

Corollary 8.5.7. *Assume that* $\varepsilon(E) = 1$. *Then*

$$L(E,1) = 2 \sum_{n \geqslant 1} \frac{a_n(E)}{n} e^{-2\pi n/\sqrt{N}} \, .$$

Proof. We simply choose $t_0 = 1$ in the proposition, and note that

$$\Gamma(1,x) = \int_x^\infty e^{-t} \, dt = e^{-x} \, .$$

□

We see that we obtain an exceedingly simple fast formula for $L(E,1)$. Note however that it is useful only when N is not too large, say $N < 10^{15}$. If N is much larger, it is difficult to estimate $L(E,1)$ by this method.

Remark. Most number-theory oriented packages such as `Pari/GP` or `magma` provide built-in functions for computing the conductor N and the sign of the functional equation $\varepsilon(E)$, which are necessary to use the above formulas. However, if these are not available we can easily compute them indirectly by using the free parameter t_0 occurring in the formula for $L(E,s)$. Since the result must be independent of t_0, it is not difficult to compute N and $\varepsilon(E)$, aided by the fact that the prime divisors of N are the same as those of $\mathrm{disc}(E)$. In practice it is reasonably easy to compute N using Tate's algorithm, and so the only quantity that we really need to compute if one does not have a suitable CAS available is $\varepsilon(E)$, and this requires only two distinct values of t_0.

We now need to compute derivatives. For this we set the following definition.

Definition 8.5.8. *We define by induction the functions* $\Gamma_r(s,x)$ *by*

$$\Gamma_{-1}(s,x) = e^{-x}x^s \quad \textit{and} \quad \Gamma_r(s,x) = \int_x^\infty \frac{\Gamma_{r-1}(s,t)}{t}\,dt \quad \textit{for} \quad r \geqslant 0\ .$$

For instance, $\Gamma_0(s,x) = \Gamma(s,x)$, the incomplete gamma function, hence for example $\Gamma_0(1,x) = e^{-x}$ and

$$\Gamma_1(1,x) = \int_x^\infty \frac{e^{-t}}{t}\,dt = E_1(x)\ ,$$

the *exponential integral.*

The functions Γ_r should not be confused with the higher gamma functions of Barnes.

Proposition 8.5.9. *Set*

$$\omega = \log\left(\frac{2\pi}{t_0\sqrt{N}}\right)\ .$$

We have the formula

$$\begin{aligned}\frac{L^{(r)}(E,s)}{r!} &= \sum_{n\geqslant 1}\frac{a_n(E)}{n^s}\Gamma_r\Big(s,\frac{2\pi n}{t_0\sqrt{N}}\Big)\\ &\quad + (-1)^r\varepsilon(E)\Big(\frac{2\pi}{\sqrt{N}}\Big)^{2s-2}\sum_{n\geqslant 1}\frac{a_n(E)}{n^{2-s}}\Gamma_r\Big(2-s,\frac{2\pi n t_0}{\sqrt{N}}\Big)\\ &\quad + \sum_{k=1}^{r}(-1)^{k-1}\frac{L^{(r-k)}(E,s)}{(r-k)!}\frac{\omega^k}{k!}\ .\end{aligned}$$

Proof. It immediately follows from the first formula of Proposition 8.5.11 below that

$$\frac{d}{ds}\Gamma_r(s,x) = \Gamma_r(s,x)\log(x) + (r+1)\Gamma_{r+1}(s,x)\ .$$

Using Proposition 8.5.6, the above proposition easily follows by induction on r. □

Generalizing Corollary 8.5.7, we have the following.

Corollary 8.5.10. *Assume that* $\varepsilon(E) = (-1)^r$ *and in addition that* $L^{(k)}(E,1) = 0$ *when* $0 \leqslant k \leqslant r-1$, $k \equiv r \pmod 2$. *Then*

$$\frac{L^{(r)}(E,1)}{r!} = 2\sum_{n\geqslant 1}\frac{a_n(E)}{n}\Gamma_r\left(1,\frac{2\pi n}{\sqrt{N}}\right)\ .$$

In particular, if $\varepsilon(E) = -1$ *then*

$$L'(E,1) = 2\sum_{n\geqslant 1}\frac{a_n(E)}{n}E_1\left(\frac{2\pi n}{\sqrt{N}}\right) ,$$

where as above

$$E_1(x) = \int_x^\infty \frac{e^{-t}}{t}\,dt$$

is the exponential integral function.

Proof. Since $\varepsilon(E) = (-1)^r$, the functional equation implies that $L^{(k)}(E,1) = 0$ for all $k \not\equiv r \pmod 2$. Thus the hypotheses of the corollary and the above proposition applied with $t_0 = 1$ give the first formula. For $r = 1$, we note that

$$\Gamma_1(1,x) = \int_x^\infty \frac{\Gamma_0(1,t)}{t}\,dt = \int_x^\infty \frac{e^{-t}}{t}\,dt = E_1(x) ,$$

proving the corollary. □

There remains the problem of numerically computing the functions $\Gamma_r(1,x)$ for positive x. This is done in two completely different ways depending on whether x is small or large, and we will treat these cases separately.

8.5.4 Computation of $\Gamma_r(1,x)$ for Small x

We begin by the following essential integral representation, useful whether x is small or large.

Proposition 8.5.11. *For $r \geqslant 0$ we have*

$$\Gamma_r(s,x) = x^s\int_1^\infty \frac{\log(t)^r}{r!}e^{-xt}t^s\,\frac{dt}{t} = \int_x^\infty \frac{\log(t/x)^r}{r!}e^{-t}t^s\,\frac{dt}{t} .$$

Proof. We prove this by induction on r, calling $g_r(x)$ the first integral on the right hand side. It is clear that it is true for $r = 0$. It is also clear that $g_r(x)$ tends exponentially fast to 0 when x tends to infinity, so by definition of $\Gamma_r(s,x)$ we must show that $g_r'(x) = -g_{r-1}(x)/x$. We have

$$g_r'(x) = sx^{s-1}\int_1^\infty \frac{\log(t)^r}{r!}e^{-xt}t^s\,\frac{dt}{t} - x^s\int_1^\infty \frac{\log(t)^r}{r!}e^{-xt}t^{s+1}\,\frac{dt}{t} .$$

Now integration by parts shows that

$$\int_1^\infty \frac{\log(t)^r}{r!}e^{-xt}t^{s+1}\,\frac{dt}{t} = \frac{1}{x}\int_1^\infty e^{-xt}t^s\left(\frac{\log(t)^{(r-1)}}{(r-1)!} + s\frac{\log(t)^r}{r!}\right)\frac{dt}{t} ,$$

so that

$$g_r'(x) = -x^{s-1}\int_1^\infty e^{-xt}t^s\frac{\log(t)^{(r-1)}}{(r-1)!}\,\frac{dt}{t} = -\frac{g_{r-1}(x)}{x}$$

as claimed. □

Recall that $\zeta(s) = \sum_{n\geqslant 1} n^{-s}$ for $\Re(s) > 1$ (we will study this function in much more detail in later chapters) and that Euler's constant γ is defined by

$$\gamma = \lim_{N\to\infty} \sum_{n=1}^{N} \frac{1}{n} - \log(N) = \lim_{s\to 1^+} \zeta(s) - \frac{1}{s-1} .$$

Proposition 8.5.12. *Set*

$$G_r(x) = \sum_{n\geqslant 1} (-1)^{n-1} \frac{x^n}{n^r\, n!} ,$$

and define constants a_k by the formal equality

$$\exp\left(\sum_{k\geqslant 1} \frac{\zeta(k)}{k} x^k\right) = \sum_{k\geqslant 0} a_k x^k ,$$

where by convention we set $\zeta(1) = \gamma$. Then

$$(-1)^r \Gamma_r(1,x) = \sum_{k=0}^{r} a_k \frac{\log(x)^{r-k}}{(r-k)!} - G_r(x) .$$

Proof. When $r = 0$ we have $\Gamma_0(1,x) = e^{-x}$ and $G_0(x) = 1 - e^{-x}$, hence the formula is true in that case, so we may assume that $r \geqslant 1$. Integrating by parts we have

$$\begin{aligned}
\Gamma_r(1,x) &= \int_x^\infty \frac{\log(t/x)^r}{r!} e^{-t}\, dt = \int_x^\infty \frac{\log(t/x)^{r-1}}{(r-1)!} e^{-t} \frac{dt}{t} \\
&= \int_1^\infty \frac{\log(t/x)^{r-1}}{(r-1)!} e^{-t} \frac{dt}{t} + \int_0^1 \frac{\log(t/x)^{r-1}}{(r-1)!} (e^{-t}-1) \frac{dt}{t} \\
&\quad + \int_x^1 \frac{\log(t/x)^{r-1}}{(r-1)!} \frac{dt}{t} - \int_0^x \frac{\log(t/x)^{r-1}}{(r-1)!} (e^{-t}-1) \frac{dt}{t} .
\end{aligned}$$

First, let $I_r(x)$ be the sum of the first two integrals from 1 to ∞ and from 0 to 1. Expanding by the binomial theorem, it is clear that

$$I_r(x) = \sum_{k=0}^{r-1} (-1)^{r-1-k} C_k \frac{\log(x)^{r-1-k}}{(r-1-k)!} ,$$

where

$$C_k = \int_1^\infty \frac{\log(t)^k}{k!} e^{-t} \frac{dt}{t} + \int_0^1 \frac{\log(t)^k}{k!} (e^{-t}-1) \frac{dt}{t} .$$

Thus

$$\sum_{k\geqslant 0} C_k s^k = \int_1^\infty e^{-t}t^s\,\frac{dt}{t} + \int_0^1 (e^{-t}-1)t^s\,\frac{dt}{t}\,,$$

which is clearly valid for $\Re(s) > -1$. Thus, for $\Re(s) > 0$ we have

$$\sum_{k\geqslant 0} C_k s^k = -\frac{1}{s} + \int_0^\infty e^{-t}t^s\,\frac{dt}{t} = \Gamma(s) - \frac{1}{s}\,,$$

and by analytic continuation this last equality is also valid for $\Re(s) > -1$. It follows that

$$1 + \sum_{k\geqslant 0} C_k s^{k+1} = \Gamma(s+1) = \exp\left(\sum_{k\geqslant 1}(-1)^k\frac{\zeta(k)}{k}s^k\right) = \sum_{k\geqslant 0}(-1)^k a_k s^k$$

by the well-known power series expansion of $\log(\Gamma(s+1))$ (see Proposition 9.7.15 for a proof). It follows that $C_k = (-1)^{k+1}a_{k+1}$ for $k \geqslant 0$, hence

$$I_r(x) = (-1)^r \sum_{k=1}^{r} a_k \frac{\log(x)^{r-k}}{(r-k)!}\,,$$

giving the first term in the formula, apart from the $k = 0$ summand.

Furthermore we have

$$\int_x^1 \frac{\log(t/x)^{r-1}}{(r-1)!}\,\frac{dt}{t} = \left.\frac{\log(t/x)^r}{r!}\right|_x^1 = (-1)^r\frac{\log(x)^r}{r!}\,,$$

giving the $k = 0$ summand since $a_0 = 1$.

Finally

$$\int_0^x \frac{\log(t/x)^{r-1}}{(r-1)!}(e^{-t}-1)\,\frac{dt}{t} = \int_0^1 \frac{\log(t)^{r-1}}{(r-1)!}(e^{-tx}-1)\,\frac{dt}{t} = \sum_{n\geqslant 1}(-1)^n\frac{x^n}{n!}J_{n,r-1}\,,$$

where

$$J_{n,k} = \int_0^1 t^n\frac{\log(t)^k}{k!}\,\frac{dt}{t} = \int_0^\infty e^{-nt}\frac{(-t)^k}{k!}\,dt = \frac{(-1)^k}{n^{k+1}}$$

by definition of the gamma function, hence

$$\int_0^x \frac{\log(t/x)^{r-1}}{(r-1)!}(e^{-t}-1)\,\frac{dt}{t} = (-1)^r\sum_{n\geqslant 1}(-1)^{n-1}\frac{x^n}{n^r\,n!} = (-1)^r G_r(x)\,,$$

proving the proposition. □

Example: We have $a_0 = 1$, $a_1 = \gamma$, $a_2 = (\gamma^2 + \zeta(2))/2$, $a_3 = (\gamma^3 + 3\gamma\zeta(2) + 2\zeta(3))/6$.

The above proposition reduces the computation of $\Gamma_r(1,x)$ to that of $G_r(x)$. When x is small (say $x < 10$) this is perfectly fine. When x is larger there are two closely related pitfalls which plague the computation, coming from numerical cancellation. First, since $G_r(x)$ is an alternating series, when x is large we will lose a lot of accuracy in the computation. By comparison with the series for $\exp(-x)$, it can be shown that to obtain D decimals digits of relative accuracy we need to perform the computations to $D + 2x/\log(10)$ decimal digits in all the intermediate computations. This becomes prohibitive for x large. The second closely related pitfall is that since $\Gamma_r(1,x)$ is exponentially small, the additional polynomial in $\log(x)$ that must be subtracted from $G_r(x)$ will be of comparable size, so we will have an expression of the form $a-b$ with a and b possibly very accurate real numbers, but almost equal, the nightmare of the numerical analyst. Note that no naïve rearrangement of the alternating series can help with this.

The following proposition shows that we can at least dispense with the problem of alternating series, although it does not remove the second pitfall (cancellation with the logarithmic terms), which can be avoided only by the use of methods specific to the case where x is large, which we shall study in the next section.

Proposition 8.5.13. *Recall that*

$$G_r(x) = \sum_{n \geqslant 1} (-1)^{n-1} \frac{x^n}{n^r\, n!} \ .$$

Set $H_k(n) = \sum_{1 \leqslant j \leqslant n} 1/j^k$, *and define arithmetic functions* $A_k(n)$ *by a formal expansion similar to that giving the constants* a_k*:*

$$\exp\left(\sum_{k \geqslant 1} \frac{H_k(n)}{k} x^k\right) = \sum_{k \geqslant 0} A_k(n) x^k \ .$$

Then

$$G_r(x) = e^{-x} \sum_{n \geqslant 1} \frac{x^n}{n!} A_r(n) \ .$$

Proof. We prove the proposition by induction on r, the case $r = 0$ being clear since

$$G_0(x) = 1 - e^{-x} = e^{-x} \sum_{n \geqslant 1} \frac{x^n}{n!} \ .$$

Define by induction on r $A_0(n) = 1$ for $n \geqslant 0$ for $r \geqslant 1$

$$A_k(n) = \sum_{j=1}^{n} \frac{A_{k-1}(j)}{j}$$

(we will see below that this is the same definition as in the proposition). Assume the proposition true for $r-1$, in other words that

$$G_{r-1}(x) = e^{-x} \sum_{n \geqslant 1} \frac{x^n}{n!} A_{r-1}(n) \ .$$

By our induction hypothesis we have

$$\begin{aligned} G_r(x) &= \int_0^x \sum_{n \geqslant 1} (-1)^{n-1} \frac{t^{n-1}}{n^{r-1}\, n!}\, dt \\ &= \int_0^x \frac{G_{r-1}(t)}{t}\, dt = \sum_{k \geqslant 1} \frac{A_{r-1}(k)}{k!} \int_0^x e^{-t} t^{k-1}\, dt \ . \end{aligned}$$

Now by induction we have

$$\int_0^x e^{-t} t^{k-1} = (k-1)! \left(1 - e^{-x} \sum_{n=0}^{k-1} \frac{x^n}{n!} \right) = (k-1)! e^{-x} \sum_{n \geqslant k} \frac{x^n}{n!} \ ,$$

so that

$$G_r(x) = e^{-x} \sum_{k \geqslant 1} \frac{A_{r-1}(k)}{k} \sum_{n \geqslant k} \frac{x^n}{n!} = e^{-x} \sum_{n \geqslant 1} \frac{x^n}{n!} \sum_{1 \leqslant k \leqslant n} \frac{A_{r-1}(k)}{k} \ ,$$

proving the result by induction on r.

It remains to see that the $A_k(n)$ defined above are given as in the proposition. Set $f(x,n) = \sum_{k \geqslant 0} A_k(n) x^k$. Then by definition

$$\left(1 - \frac{x}{n}\right) f(x,n) = \sum_{r \geqslant 0} \left(A_r(n) - \frac{A_{r-1}(n)}{n} \right) x^r = f(x, n-1) \ ,$$

and since $f(x,0) = 1$ we obtain

$$f(x,n) = \prod_{1 \leqslant j \leqslant n} 1/(1 - x/j) \ ,$$

so the result follows by taking logarithms and expanding formally. □

Note that all the series and integral manipulations are justified by absolute convergence, all the series having infinite radius of convergence. For the same reason, this enables us to compute $G_r(x)$ even for large x without loss of accuracy. However we still need $x^n/n!$ to be small, hence n at least of the order of x (plus a small amount to account for the desired accuracy), and also we must keep in mind the cancellation phenomenon with the logarithmic terms in the formula of Proposition 8.5.12. In practice we do not advise to use the above formulas for x larger than 50, say, and even for $x > 10$.

Examples. We have $A_0(n) = 1$, $A_1(n) = H_1(n)$, $A_2(n) = (H_1(n)^2 + H_2(n))/2$, etc..., the formulas being formally identical to those for the coefficients a_k (note that $\zeta(k) = \lim_{n \to \infty} H_k(n)$ for $k \geqslant 2$).

Corollary 8.5.14. *With the notation of Proposition 8.5.12 and the above proposition we have*

$$(-1)^r\Gamma_r(1,x)=\sum_{k=0}^{r}a_k\frac{\log(x)^{r-k}}{(r-k)!}-e^{-x}\sum_{n\geqslant 1}\frac{x^n}{n!}A_r(n)\ .$$

8.5.5 Computation of $\Gamma_r(1,x)$ for Large x

For large x we can use the following proposition.

Proposition 8.5.15. *Define arithmetic functions $C_k(n)$ by the formal expansion*

$$\exp\left(\sum_{k\geqslant 1}(-1)^{k-1}\frac{H_k(n)}{k}x^k\right)=\sum_{k\geqslant 0}C_k(n)x^k\ .$$

Then for $r\geqslant 1$ we have

$$\Gamma_r(1,x)=e^{-x}\sum_{n\geqslant 0}\frac{(-1)^{n+r+1}n!C_{r-1}(n)}{x^{n+1}}\ ,$$

where the divergent series is to be interpreted as meaning that $e^x\Gamma_r(1,x)$ is always between two successive partial sums of the series.

Proof. Set

$$E_r(x)=\int_x^\infty\frac{e^{-t}}{t^r}\,dt\ .$$

Integrating by parts gives $E_r(x)=e^{-x}/x^r-rE_{r+1}(x)$. It follows that

$$E_r(x)=\frac{e^{-x}}{(r-1)!}\sum_{n=0}^{m-1}\frac{(-1)^n(n+r-1)!}{x^{n+r}}+(-1)^m\frac{(m+r-1)!}{(r-1)!}E_{m+r}(x)\ .$$

Since $E_{m+r}(x)>0$ for all x, with the interpretation of the divergent series given in the proposition we can write

$$E_r(x)=\frac{e^{-x}}{(r-1)!}\sum_{n\geqslant 0}\frac{(-1)^n(n+r-1)!}{x^{n+r}}\ .$$

Thus since $\Gamma_1(1,x)=E_1(x)$ the proposition is proved for $r=1$.

Define $C_0(n)=1$ for $n\geqslant 0$ and by induction on $r\geqslant 1$

$$C_r(n)=\sum_{k=1}^{n}\frac{C_{r-1}(k-1)}{k}$$

(once again we will see below that these are the same as those defined in the proposition). Let $r\geqslant 2$ and assume by induction that for $k\leqslant r-1$ we have

$$\Gamma_k(1,x) = e^{-x} \sum_{n=0}^{m-1} \frac{(-1)^{n+k-1} n! C_{k-1}(n)}{x^{n+1}} + (-1)^{m+k-1} I_{m,k}(x)$$

with $I_{m,k}(x) > 0$ for all x. We now use the induction formula

$$\Gamma_r(1,x) = \int_x^\infty \frac{\Gamma_{r-1}(1,t)}{t}\, dt$$

the expression obtained for $E_r(x)$ applied to a suitable m, and denoting by the generic letter P a nonnegative quantity, we obtain

$$\begin{aligned}
\Gamma_r(1,x) &= \sum_{n=0}^{m-1} (-1)^{n+r} n! C_{r-2}(n) E_{n+2}(x) + (-1)^{m+r} \int_x^\infty \frac{I_{m,r}(t)}{t}\, dt \\
&= \sum_{n=0}^{m-1} \frac{(-1)^{n+r} n! C_{r-2}(n)}{(n+1)!} \left(e^{-x} \sum_{k=0}^{m-n-1} \frac{(-1)^k (k+n+1)!}{x^{k+n+2}} + (-1)^{m-n} P \right) \\
&\qquad + (-1)^{m+r} P \\
&= e^{-x} \sum_{N=0}^{m-1} \frac{(-1)^{N+r} (N+1)!}{x^{N+2}} \sum_{n+k=N} \frac{C_{r-2}(n)}{n+1} + (-1)^{m+r} P \\
&= e^{-x} \sum_{n=1}^{m} \frac{(-1)^{n+r+1} n!}{x^{n+1}} \sum_{1 \leqslant k \leqslant n} \frac{C_{r-2}(k-1)}{k} + (-1)^{m+r} P\,,
\end{aligned}$$

proving the formula of the proposition.

As before, it remains to see that the $C_k(n)$ defined above are given as in the proposition. Set $g(x,n) = \sum_{k \geqslant 0} C_k(n) x^k$. Then by definition

$$\left(1 + \frac{x}{n}\right) g(x, n-1) = \sum_{r \geqslant 0} \left(C_r(n-1) + \frac{C_{r-1}(n-1)}{n} \right) x^r = g(x,n)\,,$$

and since $g(x,0) = 1$ we obtain

$$g(x,n) = \prod_{1 \leqslant j \leqslant n} (1 + x/j)\,,$$

so the result follows once again by taking logarithms and expanding formally. □

Examples. We have $C_1(n) = 1$, $C_2(n) = H_1(n)$, $C_3(n) = (H_1(n)^2 - H_2(n))/2$, etc..., the formulas being formally the same as for $A_k(n)$, changing $H_k(n)$ into $-H_k(n)$ for even values of k.

Remarks.

(1) To compute $\Gamma_r(1,x)$, say to approximately 18 decimal digits, which is almost always sufficient for practical uses, we thus suggest the following method. If $x \leqslant 50$, we use directly the power series expansion given by Corollary 8.5.14, remembering to take into account the cancellation which occurs between the logarithmic terms and the power series. Note that 50 is not any number but chosen so that $\exp(-50) < 10^{-20}$. If $x > 50$ we use the asymptotic expansion given by Proposition 8.5.15. This gives good results. If it is really necessary to compute to more than 18 decimal digits, simply increase 50 to a larger value.

(2) Note that in Corollary 8.5.10 we need the values of $\Gamma_r(1,x)$ to a given *absolute* accuracy. Since it is exponentially decreasing with x, when x is large it is not necessary to compute it to a large relative accuracy. We leave the details to the reader.

(3) In the special case where $r = 1$ we can do better. It can be shown that the asymptotic expansion can be expanded into the following *continued fraction* which should of course be used instead:

$$\Gamma_1(1,x) = E_1(x) = \cfrac{e^{-x}}{x+1-\cfrac{1^2}{x+3-\cfrac{2^2}{x+5-\cfrac{3^2}{x+7-\ddots}}}}.$$

This continued fraction converges for all $x > 0$, and rapidly for large x, see Exercise 20.

(4) A continued fraction corresponds to linear recurring sequences of order 2. It can be shown that there exist similar recurring sequences but of order $r+1$ for $\Gamma_r(1,x)$, also leading to faster methods to compute them, but this is beyond the scope of this book (and not really essential in practice).

8.5.6 The Famous Curve $y^2 + y = x^3 - 7x + 6$

The above curve (written in minimal form) is famous because it was used to give an explicit solution to an old problem of Gauss on lower bounds for class numbers of imaginary quadratic fields. It is the curve with smallest conductor of rank 3 over $\mathbb{Q}$. Let us prove that it has rank 3. After completing the square and changing x into $x/4$ we obtain the equation $y^2 = x^3 - 112x + 400$. This curve has no torsion, so we will compute its rank using the method explained in Section 8.3.4. We let θ be a root of $P(x) = x^3 - 112x + 400 = 0$ and $K = \mathbb{Q}(\theta)$. The number field K has class number 2, and fundamental units $\theta^2/4 + 2\theta - 13$ and $\theta^2 - 12\theta + 33$. The discriminant of the polynomial $P(x)$ is equal to $2^8 \cdot 5077$ with 5077 prime, so the only primes of K to consider are those above 2 (because of the condition $p^2 \mid \mathrm{disc}(P)$ seen in Corollary 8.3.7). In fact 2 ramifies completely as $2\mathbb{Z}_K = \mathfrak{p}^3$, so T is reduced to the

single prime ideal $\mathfrak{p}$, which of course automatically divides $3\theta^2+a$. To find $U_T(K)$ we should use Proposition 7.4.7 of [Coh1], but here we are lucky since we find that $\mathfrak{p}$ is a principal ideal generated by $\varepsilon_1 = -\theta/2+4$. We compute that a generator of the square of a generator of the class group of K is equal to $\varepsilon_2 = \theta^2/2+4\theta-25$. Finally the fundamental and torsion units are $\varepsilon_3 = \theta^2/4+2\theta-13$, $\varepsilon_4 = \theta^2-12\theta+33$ and $\varepsilon_5 = -1$. It follows that $S_T(K)$ is generated over $\mathbb{F}_2$ by the classes modulo squares of the 5 elements that we have just listed. The respective norms of these elements being 2, -25, -1, 1 and -1 it follows that the kernel $S_T(K,1)$ of the norm map modulo squares is generated by $-\varepsilon_2$, $-\varepsilon_3$ and ε_4. We could now proceed with the algorithm, and for each of these generators compute the quadratic forms $q_i(c_0,c_1,c_2)$, find a particular solution to $q_2=0$, then the general solution, and replace in $q_1=1$ to obtain the quartic, one for each generator. We then have to search for a point on these three quartics. This can be done. However we will cheat to avoid such tedious computations. Since the dimension of $S_T(K,1)$ is equal to 3 we know that the rank $r(E)$ of our curve is at most equal to 3. On the other hand on the initial equation $y^2+y=x^3-7x+6$ we readily discover the points $P_1=(2,0)$, $P_2=(-1,3)$ and $P_3=(4,6)$. To show that they are independent we use Theorem 8.1.17. Using for instance the algorithms of [Coh0] we compute that the determinant of the height pairing matrix of the P_i is equal to $0.41714355875838397\ldots$, hence is definitely different from 0, so that the points are independent. It follows that $r(E)$ is at least equal to 3, and we have shown that $r(E)\leqslant 3$, so that $r(E)=3$ as claimed. We have *not* shown that the P_i are generators, only that they generate a subgroup of $E(\mathbb{Q})$ of finite index, but this is indeed the case.

We now use the method of the preceding sections to compute $L(E,s)$ and its derivatives. A computation shows that the sign of the functional equation is -1. It follows that $L^{(r)}(E,1)=0$ for all even $r\geqslant 1$, and in particular $L(E,1)=L''(E,1)=0$. On the other hand we compute numerically that $L'(E,1)$ is almost equal to 0 (equal within the limits of accuracy of our computation). Note that however precisely we perform our computation we will never be able to *prove* that $L'(E,1)=0$. Here we must apply a difficult theorem of Gross–Zagier which implies in particular that if $L'(E,1)\neq 0$ then the curve has rank 1. Since we know that it has three independent points this is not possible, *proving* that $L'(E,1)=0$. Finally using the formulas given above we compute that

$$\frac{L'''(E,1)}{3!} = 1.73184990011930068979\ldots$$

On the other hand the quantity $\omega_1(E)$ which enters in the BSD conjecture is easily computed to be $2.07584399154346652494\ldots$. Since there is no torsion, the Tamagawa numbers $c_p(E)$ for finite p can be shown to be equal to 1, and $c_\infty(E)=2$, we deduce the equality

$$|Ш(E)|R(E) = 0.41714355875838397\ldots$$

This is exactly the determinant of the height pairing matrix that we have found above by completely different methods. Thus the BSD conjecture tells us both that the points P_i given form a basis of $E(\mathbb{Q})$ (this is easy to show directly) and that $Ш(E)$ is the trivial group, which at present nobody knows how to prove, even on this specific curve.

8.6 The Heegner Point Method

I would like to thank C. Delaunay for writing a large part of this section.

8.6.1 Introduction and the Modular Parametrization

The Heegner point method is applicable if and only if the elliptic curve E has analytic rank exactly equal to 1. We therefore assume that we know this for a fact by having computed that $\varepsilon(E) = -1$ and that $L'(E,1) \neq 0$, which can be done rigorously as already explained. We then know that $E(\mathbb{Q})$ has a point of infinite order on it, and the purpose of the method is to find it explicitly, and even to find a generator of the torsionfree part of $E(\mathbb{Q})$.

Remarks.

(1) If we have done a 2-descent showing that the rank is equal to 1, it is not necessary to use this method since a nontorsion point can easily be computed explicitly from the 2-descent method.

(2) Once a point of infinite order has been found, finding a generator is straightforward, see Exercise 22. It follows that we only want to find a point of infinite order.

Recall that the BSD conjecture involves quantities that we know how to compute, and others that we do not know directly. More precisely, given an elliptic curve E defined over $\mathbb{Q}$, we can algorithmically compute its conductor N, which enters in the functional equation and which is divisible exactly by the primes where E has bad reduction, we can compute the (finite number of) Euler factors corresponding to these bad primes, and the so-called Tamagawa numbers c_p for $p \mid N$. All these steps are done simultaneously using variants of an algorithm due to Tate. In addition we can compute the real period $\omega_1(E)$ as an elliptic integral using the arithmetic-geometric mean, and the torsion subgroup $E_t(\mathbb{Q})$ using one of the methods explained above. Next, for any given $p \nmid N$ we can compute $a_p = p+1-|E(\mathbb{F}_p)|$ hence the corresponding Euler factor, and so as many terms as we want of the Dirichlet series for the global L function $L(E,s)$. Finally, using the method of Section 8.5.3, we can compute $L^{(r)}(E,1)$ to any desired accuracy, and in particular use Corollaries 8.5.7 and 8.5.10.

In addition, we can also compute the *volume* $\mathrm{Vol}(E)$ of E, in other words the volume (or determinant) of the lattice Λ such that $E(\mathbb{C}) = \mathbb{C}/\Lambda$. Although

this is not necessary for the BSD formula, it will be needed in the Gross–Zagier formula below.

All the algorithms (and many more) for doing these computations are explained in great detail in [Cre2], see also [Coh0].

The quantities which we do not know how to compute at first are the regulator $R(E)$, which is known only once a generating set for the Mordell–Weil group has been computed, and the Tate–Shafarevitch group order $|Ш(E)|$, of which we know little apart from the fact that, if finite, it will be the square of an integer. Note that since our goal is to find a point of infinite order on $E(\mathbb{Q})$, we can assume any conjecture for doing so.

The *Heegner point method* which we consider in this section is based on a number of facts which are outside the scope of this book, but which lead to an algorithm which is sufficiently simple and important to be explained here. Thus several of the terms used below will not be defined, and we ask the reader to be patient until we come to the actual description of the algorithm. Note however that the theory that we sketch in a few lines is very beautiful and described in many papers and textbooks, see for example [Cre1], [Dar], and [Zag].

First, if $L(E,s) = \sum_{n\geqslant 1} a_n n^{-s}$ then the Taniyama–Weil conjecture asserts that $f_E(\tau) = \sum_{n\geqslant 1} a_n q^n$ (as usual with $q = e^{2i\pi\tau}$ and $\tau \in \mathcal{H}$, the upper half plane) is a modular form of weight 2 on $\Gamma_0(N)$. Thanks to Wiles and successors this conjecture is now a theorem, but as already explained, for the work that we are doing we may assume any conjecture that we like.

Since $f_E(\tau)d\tau$ is a holomorphic differential the integral

$$\tilde{\phi}(\tau) = 2i\pi \int_{\infty}^{\tau} f_E(z)dz$$

(where ∞ is the point at infinity in the upper half plane) is independent of the chosen path hence defines a map from $\mathcal{H}$ to $\mathbb{C}$. Explicitly, for $\tau \in \mathcal{H}$ we clearly have

$$\tilde{\phi}(\tau) = \sum_{n\geqslant 1} \frac{a_n}{n} q^n \ ,$$

where as usual $q = e^{2i\pi\tau}$. The modularity property of f_E is equivalent to the fact that $\tilde{\phi}$ induces an analytic map ϕ from $X_0(N)$ to $\mathbb{C}/\Lambda$, where $X_0(N) = (\mathcal{H} \cup \mathbb{P}_1(\mathbb{Q}))/\Gamma_0(N)$ is the modular curve associated to $\Gamma_0(N)$, and Λ is the lattice formed by the *periods* of f_E, corresponding to the values of $\tilde{\phi}$ for $\tau = \gamma(\infty)$ and $\gamma \in \Gamma_0(N)$ (which cannot be directly computed from the infinite series but only from the integral definition).

The lattice Λ is very often a sublattice of the lattice Λ_E associated to the minimal model of the elliptic curve E, hence in this case $\tilde{\phi}$ induces an analytic map ϕ from $X_0(N)$ to $\mathbb{C}/\Lambda_E$. To come back to points $(x,y) \in E(\mathbb{C})$ we use the classical isomorphism from $\mathbb{C}/\Lambda_E$ to $E(\mathbb{C})$ given by the Weierstrass $\wp$ function and its derivative.

However in principle it might happen that Λ is not a sublattice of Λ_E, due to the fact that the so-called "Manin constant" of E may not be equal to 1 (even assuming Manin's conjecture saying that this should be the case for the strong Weil curve in the isogeny class of f). In practice it does not happen, but if it did it would be easy to deal with.

Putting everything together, we see that for any $\tau \in \mathcal{H}$ (and even $\tau \in \mathcal{H} \cup \mathbb{P}_1(\mathbb{Q})$, but we do not need this extra generality) we can associate a point $\varphi(\tau) \in E(\mathbb{C})$, where $\varphi = \wp \circ \phi$. The map φ from $X_0(N)$ to E is called the *modular parametrization* of E, and Wiles's theorem states that such a parametrization exists (and is unique up to sign).

8.6.2 Heegner Points and Complex Multiplication

We begin by defining Heegner points.

Definition 8.6.1. (1) *Let $\tau \in \mathcal{H}$. We say that τ is a* complex multiplication point (*or simply a* CM point) *if it is a root of a quadratic equation $A\tau^2 + B\tau + C = 0$ with A, B, C integral and $B^2 - 4AC < 0$.*

(2) *If in addition we choose A, B, C such that $\gcd(A, B, C) = 1$ and $A > 0$ (which makes them unique), then $(A, B, C) = Ax^2 + Bxy + Cy^2$ is called the (positive definite binary) quadratic form associated to τ, and its discriminant $\Delta(\tau) = B^2 - 4AC$ is called the discriminant of τ.*

(3) *For a given integer $N \geqslant 1$, we will say that τ is a Heegner point of level N if $\Delta(N\tau) = \Delta(\tau)$.*

The above definition of a Heegner point is due to B. Birch. The following proposition shows that this notion depends only on the class of τ in $X_0(N)$.

Proposition 8.6.2. *If $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ (in particular if $\gamma \in \Gamma_0(N)$) then $\Delta(\gamma(\tau)) = \Delta(\tau)$, and if $\gamma \in \Gamma_0(N)$ and τ is a Heegner point of level N, so is $\gamma(\tau)$.*

Proof. This comes from the fundamental group equality

$$\Gamma_0(N) = \Gamma \cap \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} \Gamma \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$$

with $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, and is left to the reader. □

Proposition 8.6.3. *Let $\tau \in \mathcal{H}$ be a quadratic irrationality and let (A, B, C) be the quadratic form with discriminant D associated to τ. Then τ is a Heegner point of level N if and only if $N \mid A$ and one of the following equivalent conditions is satisfied:*

(1) $\gcd(A/N, B, CN) = 1$
(2) $\gcd(N, B, AC/N) = 1$
(3) *There exists $F \in \mathbb{Z}$ such that $B^2 - 4NF = D$ with $\gcd(N, B, F) = 1$.*

Proof. We have $\tau = (-B+\sqrt{D})/(2A)$, hence $N\tau = (-NB+N\sqrt{D})/(2A)$. For this to have the same discriminant, it must be of the form $(-B' + \sqrt{D})/(2A')$ hence by identification of imaginary parts $A = NA'$ hence $B' = B$, so that $N \mid A$. It follows that $N\tau$ is a root of $(A/N)(N\tau)^2+B(N\tau)+CN = 0$, and since this equation has discriminant $D = B^2 - 4AC$, this must be the smallest equation satisfied by $N\tau$, hence τ is a Heegner point of level N if and only if $N \mid A$ and $\gcd(A/N, B, CN) = 1$. The equivalence with the other two properties is a straightforward exercise left to the reader. □

Corollary 8.6.4. *If τ is a Heegner point of level N and discriminant D, then so is $W(\tau) = -1/(N\tau)$.*

Proof. Indeed if (A, B, C) is the quadratic form associated to τ then clearly $(CN, -B, A/N)$ is the quadratic form associated to $-1/(N\tau)$, so the result follows from the proposition. Equivalently, since $\Delta(-1/\tau) = \Delta(\tau)$ it is immediate to check from the definition that $\Delta(NW(\tau)) = \Delta(W(\tau))$. □

From now on we assume that D is a *fundamental discriminant*, in other words the discriminant of the quadratic field $K = \mathbb{Q}(\sqrt{D})$. Recall that the class group $Cl(K)$ of K is in one-to-one correspondence with classes of positive definite primitive quadratic forms (A, B, C) of discriminant D modulo the action of $\mathrm{SL}_2(\mathbb{Z})$. More precisely to the class of such a form (A, B, C) we associate the class of the ideal $\mathbb{Z} + (-B + \sqrt{D})/(2A)\mathbb{Z}$.

Proposition 8.6.5. *Let τ be a Heegner point of discriminant D and level N. If D is a fundamental discriminant the condition $\gcd(N, B, F) = 1$ of the above proposition is automatically satisfied and for all $p \mid \gcd(D, N)$ we have $p \| N$, in other words $v_p(N) = 1$.*

Proof. Let p be a prime dividing $\gcd(N, B, F)$. Since $B^2 - 4NF = D$ we deduce that $p^2 \mid D$ which implies that $p = 2$ and $D/4 \equiv 2$ or 3 modulo 4 since D is fundamental. But then $(B/2)^2 = (D/4) + NF \equiv (D/4) \equiv 2$ or 3 modulo 4 since $2 \mid N$ and $2 \mid F$, which is absurd, proving the first statement. Now let $p \mid \gcd(D, N)$ and assume that $p^2 \mid N$. Since $B^2 - 4NF = D$ we deduce that $p \mid B$, hence $p^2 \mid D$ hence $p = 2$. But once again since $4 \mid N$ this gives $(B/2)^2 \equiv (D/4) + NF \equiv 2$ or 3 modulo 4, which is absurd. □

We have the following.

Proposition 8.6.6. *There is a one-to-one correspondence between on the one hand classes modulo $\Gamma_0(N)$ of Heegner points of discriminant D and level N, and on the other hand pairs $(\beta, [\mathfrak{a}])$ where $\beta \in \mathbb{Z}/2N\mathbb{Z}$ is such that $b^2 \equiv D \pmod{4N}$ for any lift b of β to $\mathbb{Z}$, and $[\mathfrak{a}] \in Cl(K)$ is an ideal class. The correspondence is as follows: if $(\beta, [\mathfrak{a}])$ is as above, there exists a primitive quadratic form (A, B, C) whose class is equal to $[\mathfrak{a}]$ and such that $N \mid A$ and $B \equiv \beta \pmod{2N}$, and the corresponding Heegner point*

is $\tau = (-B + \sqrt{D})/(2A)$. *Conversely, if* (A, B, C) *is the quadratic form associated to a Heegner point* τ *we take* $\beta = B \bmod 2N$ *and* $\mathfrak{a} = \mathbb{Z} + \tau\mathbb{Z}$.

Proof. This consists in a series of easy verifications, which are essentially identical to those made when checking that the ideal class group of K is isomorphic to the group of classes of positive definite primitive quadratic forms of discriminant D, and the details are left to the reader. Note that if b is defined modulo $2N$ then b^2 is indeed defined modulo $4N$. □

Thanks to this proposition, it is often more natural to consider a (class of) Heegner point as a pair $(\beta, [\mathfrak{a}])$ rather than as a complex number.

We need one last ingredient from algebraic number theory. Let K be a number field (in our case $K = \mathbb{Q}(\sqrt{D})$ will be an imaginary quadratic field). There exists a finite extension H of K, called the Hilbert class field, which has many remarkable properties. The most important one for us is that it is an Abelian extension of K whose Galois group is canonically isomorphic to the class group $Cl(K)$ through a completely explicit map Art from $Cl(K)$ to $\mathrm{Gal}(H/K)$. In other words any element of $\mathrm{Gal}(H/K)$ has the form $\mathrm{Art}([\mathfrak{a}])$ for a unique ideal class $[\mathfrak{a}]$. The action of an element $\sigma \in \mathrm{Gal}(H/K)$ on $h \in H$ will be written h^σ.

The theorem which makes the whole method work is the main theorem of *complex multiplication* which we will not prove. The results are due to Deuring and Shimura, but in the present context I refer to the paper of Gross [Gro].

Theorem 8.6.7. *Let* $\tau = (\beta, [\mathfrak{a}])$ *be a Heegner point of level* N *and discriminant* D, *let* $K = \mathbb{Q}(\sqrt{D})$, *and denote by* H *the Hilbert class field of* K. *Then* $\varphi(\tau) \in E(H)$, *and we have the following properties:*

(1) *For any* $[\mathfrak{b}] \in Cl(K)$ *then*

$$\varphi((\beta, [\mathfrak{a}]))^{\mathrm{Art}([\mathfrak{b}])} = \varphi((\beta, [\mathfrak{a}\mathfrak{b}^{-1}]))\ .$$

(2)

$$\varphi(W(\beta, [\mathfrak{a}])) = \varphi((-\beta, [\mathfrak{a}\mathfrak{n}^{-1}]))\ ,$$

where $\mathfrak{n} = N\mathbb{Z} + \dfrac{B + \sqrt{D}}{2}\mathbb{Z}$ *and* B *is any integer whose class modulo* $2N$ *is equal to* β.

(3) *If* $\bar{}$ *denotes complex conjugation then*

$$\overline{\varphi((\beta, [\mathfrak{a}]))} = \varphi((-\beta, [\mathfrak{a}^{-1}]))\ .$$

Thus we see that using the analytic function φ, we can obtain a point with coordinates in H, hence with algebraic coordinates. This is the "miracle" of complex multiplication, which generalizes the fact that the exponential function evaluated at rational multiples of $2i\pi$ gives algebraic numbers.

The first formula gives all the conjugates over K of $\varphi(\tau)$, and is called Shimura's reciprocity law. In particular, we can compute the trace P of $\varphi(\tau)$ as a point in $E(H)$ as

$$P = \sum_{\sigma \in \mathrm{Gal}(H/K)} \varphi((\beta,[\mathfrak{a}]))^{\sigma} = \sum_{[\mathfrak{b}] \in Cl(K)} \varphi((\beta,[\mathfrak{a}\mathfrak{b}^{-1}])) = \sum_{[\mathfrak{b}] \in Cl(K)} \varphi((\beta,[\mathfrak{b}]))\ ,$$

the sum being computed with the group law of E. By Galois theory we will have $P \in E(K)$, so we have considerably reduced the field of definition of the algebraic point found on E. Finally, we have the following easy result:

Lemma 8.6.8. *If $\varepsilon = -1$, then in fact $P \in E(\mathbb{Q})$.*

Proof. Indeed, it is easy to see that $\varepsilon = -1$ is equivalent to saying that $\varphi \circ W = \varphi$, so that

$$\overline{\varphi((\beta,[\mathfrak{b}]))} = \overline{\varphi(W(\beta,[\mathfrak{b}]))} = \overline{\varphi((-\beta,[\mathfrak{b}\mathfrak{n}^{-1}]))} = \varphi((\beta,[\mathfrak{b}^{-1}\mathfrak{n}]))\ ,$$

hence

$$\overline{P} = \sum_{[\mathfrak{b}] \in Cl(K)} \varphi((\beta,[\mathfrak{b}^{-1}\mathfrak{n}])) = \sum_{[\mathfrak{b}] \in Cl(K)} \varphi((\beta,[\mathfrak{b}])) = P\ ,$$

so by Galois theory once again we deduce that $P \in E(\mathbb{Q})$. □

We thus see that the Heegner point method does give us a point in $E(\mathbb{Q})$ (which of course may be a torsion point). It immediately follows from the Gross–Zagier Theorem 8.6.9 and the work of Kolyvagin that if the rank (analytic or algebraic) is strictly greater than 1, this point *will* always be a torsion point, so the method is useless. Furthermore a similar proof to that of the above lemma shows that if $\varepsilon = 1$ then $P + \overline{P}$ is a torsion point, so once again the method is useless. Hence, as claimed from the beginning, the Heegner point method is applicable only in the rank 1 case. Without any exaggeration it can be said that this is the *only* reason for which nothing is known on the BSD conjecture when the rank is strictly greater than 1.

8.6.3 Use of the Theorem of Gross–Zagier

Although it would already be possible to use the method as explained above, an important additional result due to Gross–Zagier usually simplifies the computations. Recall from Definition 7.3.13 that the *quadratic twist* of an elliptic curve E given by a Weierstrass equation $y^2 = x^3 + ax^2 + bx + c$ by a fundamental discriminant D is the curve E_D with equation $y^2 D = x^3 + ax^2 + bx + c$. If desired this can be put in ordinary Weierstrass form, and extended to curves in generalized Weierstrass form. The important (and easy) point is that the L-function of E_D can easily be obtained from that of E: in our case, since D is a fundamental discriminant which is a square modulo $4N$, Proposition 8.6.5 tells us that if $p \mid \gcd(D,N)$ then $p^2 \nmid N$. This

implies that the conductor N_D of E_D is equal to $ND^2/\gcd(D,N)$ and that if $L(E,s)=\sum_{n\geqslant 1} a_n n^{-s}$, then

$$L(E_D,s)=\sum_{n\geqslant 1}\left(\frac{D}{n}\right)\frac{a_n}{n^s}\,.$$

Furthermore, it is not difficult to show that the sign of the functional equation for $L(E_D,s)$ is equal to $\left(\frac{D}{-N}\right)$ times that of $L(E,s)$. In particular, in our context that of E is equal to -1, $\left(\frac{D}{N}\right)=1$, and $D<0$, hence the sign of the functional equation for $L(E_D,s)$ is equal to $+1$. Finally recall that we have defined a canonical height function $\widehat{h}$ on $E(\mathbb{Q})$, see Theorem 8.1.17.

Theorem 8.6.9 (Gross–Zagier). *If* $\gcd(D,2N)=1$ *and* $D\neq -3$ *the point* P *computed above satisfies*

$$\widehat{h}(P)=\frac{\sqrt{|D|}}{4\,\mathrm{Vol}(E)}L'(E,1)L(E_D,1)$$

(*for* $D=-3$ *the right hand side should be multiplied by* 9, *see below*).

Since $L(E_D,1)$ can easily be computed using the exponentially convergent series given above, this allows us to check whether or not $\widehat{h}(P)$ is close to 0, hence whether we will obtain a torsion point or not. But it is especially interesting to combine it with the BSD formula: indeed, in the rank 1 case we have $R(E)=\widehat{h}(G)$, where G is a generator of the Mordell–Weil group of E. Since $P\in E(\mathbb{Q})$ it has the form $\ell G+Q$ for some torsion point Q, hence $\widehat{h}(P)=\ell^2\widehat{h}(G)$. The combination of the two formulas thus reads:

$$\frac{\ell^2}{|Ш(E)|}=\omega_1(E)\frac{c(E)\sqrt{|D|}}{4\,\mathrm{Vol}(E)|E_t(\mathbb{Q})|^2}L(E_D,1)\,,$$

where $c(E)$ is the product of the Tamagawa numbers $c_p(E)$ including c_∞.

Although $|Ш(E)|$ is unknown, it is usually small and very often equal to 1 (and in our case is known to be finite hence equal to the square of an integer), so this very often gives the value of ℓ.

It is useful to be able to generalize this formula to the case $\gcd(D,2N)>1$ and also to $D=-3$ and $D=-4$. This leads to formulate the following reasonable conjecture.

Conjecture 8.6.10. *Let* E *be an elliptic curve of analytic rank* 1 (*in other words* $\varepsilon(E)=-1$ *and* $L'(E,1)\neq 0$), *and let* D *be a negative fundamental discriminant which is a square modulo* $4N$. *Assume that* $L(E_D,1)\neq 0$ *and that for any* $p\mid\gcd(D,N)$ *we have* $a_p=-1$. *Then*

$$\frac{\ell^2}{|Ш(E)|}=\omega_1(E)\frac{c(E)\sqrt{|D|}(w(D)/2)^2}{4\,\mathrm{Vol}(E)|E_t(\mathbb{Q})|^2}2^{\omega(\gcd(D,N))}L(E_D,1)\,,$$

where $w(D)$ is the number of roots of unity in $\mathbb{Q}(\sqrt{D})$ ($w(-3)=6$, $w(-4)=4$ and $w(D)=2$ for $D<-4$), and as usual $\omega(\gcd(D,N))$ is the number of distinct prime factors of $\gcd(D,N)$.

The condition $a_p=-1$ for $p \mid \gcd(D,N)$ is necessary to obtain a nontorsion Heegner point, and for the validity of the formula. Furthermore, the conditions on D in the conjecture imply that $\varepsilon(E_D)=1$, hence $L(E_D,1)$ can also be computed by the exponentially convergent series given above. The truth of this conjecture is of course mainly supported by the work of Gross–Zagier, but the additional terms are due to work of Y. Hayashi (see [Gro], [Hay]). In addition it has also been verified in numerous cases. As already mentioned, to compute a rational point we can always assume any reasonable conjecture.

8.6.4 Practical Use of the Heegner Point Method

The most lengthy computations will be the evaluations of $\phi((-B+\sqrt{D})/(2A))$ for the $|Cl(K)|$ classes of quadratic forms (A,B,C). Two remarks must be made.

Remarks.

(1) Since the convergence of the series for $\phi(\tau)$ is essentially that of a geometric series with ratio $\exp(-2\pi\Im(\tau))=\exp(-2\pi\sqrt{|D|}/(2A))$, and since $N \mid A$, it will be particularly slow when N is large. The method will thus be inapplicable for large conductors, say $N>10^8$.

(2) Thanks to the relation $\overline{\varphi((\beta,[\mathfrak{a}]))}=\varphi((\beta,[\mathfrak{a}^{-1}\mathfrak{n}]))$ which we have used above we only need to compute approximately half of the necessary values of ϕ: indeed, if $[\mathfrak{a}]$ corresponds to the class of the form (A,B,C), then $[\mathfrak{a}^{-1}\mathfrak{n}]$ corresponds to the class of the form $(CN,B,A/N)$, hence the value of ϕ on $(CN,B,A/N)$ is simply the conjugate of $\phi((A,B,C))$ modulo the lattice Λ.

We give the method as an algorithm, and then apply it to a large example.

Algorithm 8.6.11 (Heegner Point Method) Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N, and assume that E has analytic rank 1, in other words that $\varepsilon(E)=-1$ and $L'(E,1)\neq 0$. We assume that E is given by a minimal Weierstrass equation $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ with integer coefficients. This algorithm outputs a nontorsion rational point in $E(\mathbb{Q})$. We assume computed the standard values associated to E, and in particular we denote by $\omega_1(E)$ and $\omega_2(E)$ standard $\mathbb{Z}$-generators of the period lattice Λ of E with $\omega_1(E)\in\mathbb{R}_{>0}$, and by $\mathrm{Vol}(E)$ the area of the fundamental parallelogram.

1. [Compute necessary accuracy] Compute the product $|Ш(E)|R(E)$ thanks to the BSD formula

$$|Ш(E)|R(E)=\frac{|E_t(\mathbb{Q})|^2\,L'(E,1)}{c(E)\omega_1(E)}\,,$$

where $L'(E,1)$ is computed thanks to Corollary 8.5.10. Compute the height difference bound HB given by Theorem 8.1.18, in other words compute $HB = |j(E)|/12 + \mu(E) + 1.946$, where $\mu(E)$ is given by the above-mentioned theorem, and finally set $d = 2(|Ш(E)|R(E) + HB)$. All computations will now be done with a default accuracy of $\lceil d/\log(10) \rceil + 10$ decimal digits, and in particular recompute all the floating point quantities such as $\omega_i(E)$ and $\mathrm{Vol}(E)$ to that accuracy.

2. [Loop on fundamental discriminants] For each successive negative fundamental discriminant $D = -3$, -4, etc... execute the rest of the algorithm until a nontorsion point of $E(\mathbb{Q})$ is found. Check that D is a square modulo $4N$, that $a_p = -1$ for each $p \mid \gcd(D,N)$, and by computing

$$L(E_D,1) = 2\sum_{n\geqslant 1} \frac{a_n}{n}\left(\frac{D}{n}\right)\exp\left(\frac{-2\pi n}{\sqrt{ND^2/\gcd(D,N)}}\right)$$

check that $L(E_D,1)$ is numerically not equal to 0. If any of these conditions is not satisfied, choose the next fundamental discriminant. Otherwise fix $\beta \in \mathbb{Z}/(2N)\mathbb{Z}$ such that $D \equiv \beta^2 \pmod{4N}$ and compute $m > 0$ such that

$$m^2 = \omega_1(E)\frac{c(E)\sqrt{|D|}(w(D)/2)^2}{4\,\mathrm{Vol}(E)|E_t(\mathbb{Q})|^2}2^{\omega(\gcd(D,N))}L(E_D,1)\ .$$

This m should be very close to an integer, or at least to a rational number with small denominator.

3. [Find List of Forms] Using Subalgorithm 8.6.12 below, compute a list $\mathcal{L}$ of $|Cl(K)|$ representatives (A,B,C) of classes of positive definite quadratic forms of discriminant D, where A must be chosen divisible by N and minimal, and $B \equiv \beta \pmod{2N}$ (this is always possible). Whenever possible pair elements (A,B,C) and (A',B',C') of this list such that (A',B',C') is equivalent to $(CN,B,A/N)$ by computing the unique canonical reduced form equivalent to each.

4. [Main Computation] Compute the complex number

$$z = \sum_{(A,B,C)\in\mathcal{L}} \phi\left(\frac{-B+\sqrt{D}}{2A}\right) \in \mathbb{C}\ ,$$

using the formula $\phi(\tau) = \sum_{n\geqslant 1}(a_n/n)q^n$ (with $q = e^{2i\pi\tau}$) given above and the fact that $\phi((-B'+\sqrt{D})/(2A')) = \overline{\phi((-B+\sqrt{D})/(2A))}$, where (A',B',C') is paired with (A,B,C) as in Step 3. The number z should be computed to at least $d/\log(10)$ decimal digits of accuracy. This means that the number of terms to be taken in the series for $\phi((-B+\sqrt{D})/(2A))$ should be a little more than $Ad/(\pi\sqrt{|D|})$.

5. [Find Rational Point] Let e be the exponent of the group $E_t(\mathbb{Q})$, $\ell = \gcd(e, m^\infty) = \gcd(e, m^3)$, and $m' = m\ell$. For each pair $(u,v) \in [0, m'-1]^2$,

set $z_{u,v} = (\ell z + u\omega_1(E) + v\omega_2(E))/m'$. Compute $x = \wp(z_{u,v})$, where $(\wp, \wp')$ is the isomorphism from $\mathbb{C}/\Lambda$ to $E(\mathbb{C})$. For each (u, v) such that the corresponding point $(x, y) \in E(\mathbb{C})$ has real coordinates (in fact, we can know in advance which of these m or $2m$ points are real, see the remarks below), test whether x is close to a rational number with a square denominator f^2. If the computation has been performed with sufficient accuracy, at least one of these points x must be a rational number. Otherwise, we must slightly increase the accuracy used in the computations. Once x is found corresponding to a nontorsion point, compute y using the equation of the curve (which must be a rational number whose denominator is equal to f^3) and terminate the algorithm.

To compute the list of forms necessary in Step 3, we could use a sophisticated method. However, since the time spent on doing this is completely negligible compared to the time spent in the main computation of Step 4, the following naïve algorithm is sufficient.

Subalgorithm 8.6.12 (Compute list of forms) Given a fundamental negative discriminant D and β such that $\beta^2 \equiv D \pmod{4N}$, this subalgorithm computes a list $\mathcal{L}$ of forms as in Step 3 above.

1. [Initialize] Using any method (since D is small), compute the number $h(D)$ of classes of forms of discriminant D, set $\mathcal{L} \leftarrow \emptyset$, $\mathcal{L}_r \leftarrow \emptyset$, and let b be such that $b \equiv \beta \pmod{2N}$.
2. [Fill lists] Set $R \leftarrow (b^2 - D)/(4N)$, and for all positive divisors d of R do as follows: set $f \leftarrow (dN, b, R/d)$ and let f_r be the unique reduced quadratic form (A, B, C) equivalent to f (in other words $|B| \leqslant A \leqslant C$ and $B \geqslant 0$ if either $|B| = A$ or $A = C$). If $f_r \notin \mathcal{L}_r$, set $\mathcal{L}_r \leftarrow \mathcal{L}_r \cup \{f_r\}$, using Subalgorithm 8.6.13 below, find a form $f' = (A', B', C')$ equivalent to f still with $N \mid A'$ and $B' \equiv \beta \pmod{2N}$, but with A' minimal, and set $\mathcal{L} \leftarrow \mathcal{L} \cup \{f'\}$.
3. [Finished?] If $|\mathcal{L}| < h(D)$ set $b \leftarrow b + 2N$ and go to Step 2, otherwise terminate the subalgorithm.

In Step 2 the reduction from f to f_r is done using a standard algorithm such as Algorithm 5.4.2 of [Coh0]. The reduction of f to f' is done as follows.

Subalgorithm 8.6.13 (Compute minimal A) Given a positive definite form $f = (A, B, C)$ of discriminant $D < 0$ with $N \mid A$, this algorithm finds a form $f' = (A', B', C')$ equivalent to f with $N \mid A'$ and $B' \equiv B \pmod{2N}$ with A' minimal.

1. [Initialize] Set $u \leftarrow -B/(2A/N)$, $v_2 \leftarrow |D|/(2A/N)^2$. By any reasonable method (see below) find some (c_0, d_0) with $\gcd(c_0 N, d_0) = 1$ and such that $(c_0 u + d_0)^2 + c_0^2 = m_0$ is as small as possible by the chosen method. Note that we can always set $c_0 \leftarrow 0$, $d_0 \leftarrow 1$, and $m_0 \leftarrow 1$. Set $L \leftarrow \sqrt{m_0/v_2}$. If $L \leqslant 1$, output (A, B, C) and terminate the algorithm, otherwise set $c \leftarrow 0$.

2. [Loop on c] Set $c \leftarrow c+1$, and if $c \geqslant L$ go to Step 3. Otherwise, set $d \leftarrow \lfloor -cu \rceil^*$ (the nearest integer to $-cu$ prime to cN) and set $r \leftarrow (cu+d)^2+c^2v_2$. If $r < m_0$, set $m_0 \leftarrow r$, $c_0 \leftarrow c$, $d_0 \leftarrow d$, and $L \leftarrow \sqrt{m_0/v_2}$. Go to Step 2.
3. [Find form] If $m_0 = 1$, output (A,B,C). Otherwise, using the extended Euclidean algorithm, compute a_0 and b_0 such that $a_0d_0 - b_0Nc_0 = 1$, let $f' = (A',B',C')$ be the form $f(a_0x+b_0y, c_0x+d_0y)$ and output f'. Terminate the subalgorithm.

Proof. If we write $\tau = (-B+\sqrt{D})/(2A) = x+iy$, then $x = \Re(\tau) = -B/(2A)$ and $y = \Im(\tau) = \sqrt{|D|}/(2A)$. It follows that finding a minimal A' is equivalent to finding the corresponding τ' with the largest imaginary part. It is immediately checked that the relations $N \mid A'$ and $B' \equiv B \pmod{2N}$ are preserved by $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ (for all forms f) if and only if $\gamma \in \Gamma_0(N)$, so we write Nc instead of c. Finally, it is clear that

$$\Im(\gamma(\tau)) = \frac{\Im(\tau)}{|Nc\tau+d|^2} ,$$

so we must make $|Nc\tau+d|^2$ minimal, where

$$|Nc\tau+d|^2 = (Ncx+d)^2 + N^2c^2y^2 = (cu+d)^2 + c^2v_2$$

using the notation of the algorithm. This quantity can trivially be made equal to m_0 by choosing $(c,d) = (c_0,d_0)$ of Step 1. Hence if we want it to be strictly less than m_0 we must have $c < \sqrt{m_0/v_2} = L$, and c being fixed the optimal value of d is the one making $|cu+d|$ minimal, in other words the nearest integer to $-cu$ coprime to cN, since we must apply the extended Euclidean algorithm in Step 3. □

To find a good (c_0,d_0) in Step 1 of the above subalgorithm, we can, for example, either use a continued fraction approximation to $-Nx \approx d_0/c_0$, or use Gaussian reduction of the quadratic form $(c,d) \mapsto (cu+d)^2 + c^2v_2$ in order to find small vectors. Having a small m_0 in Step 1 is important for the efficiency of Step 3.

Remarks.

(1) As already mentioned, the above two subalgorithms are not at all optimal. However since the time spent in computing the necessary forms is negligible compared to the time spent in computing the values of ϕ, it does not matter at all. What is essential is that we choose a representative (A',B',C') with a minimal A', otherwise the computation of ϕ will be much longer.

(2) Since by Proposition 7.3.1 we have $x = n/f^2$ and $y = n'/f^3$, the detection of y as a rational number is much more costly than that of x, so it is preferable to compute x first, then y. This proposition also explains the choice of the accuracy d made in Step 1 of the main algorithm.

(3) The default accuracy d should depend not only on E, but also very slightly on the chosen discriminant D. If the choice of D is reasonable (say $|D| < 10^6$), the added constant 10 more than compensates for this dependence.

(4) We could directly compute $(\wp(z), \wp'(z))$, which will be a nontorsion point of $E(\mathbb{Q})$, and identify its coordinates as rational numbers. However in general we need very high accuracy for doing this computation, hence this can be done only on small examples (see below). The use of the integer m in the above algorithm considerably reduces the necessary accuracy.

(5) If P denotes the point of $E(\mathbb{Q})$ corresponding to $z \in \mathbb{C}/\Lambda$, we have $P = mG + T$ where G is a nontorsion point and $T \in E_t(\mathbb{Q})$. If the order of T is prime to m we can also write $P = mG + mT'$ for a suitable $T' \in E_t(\mathbb{Q})$, so the point $G + T'$ will correspond to $z/m + \omega$ for some $\omega \in \Lambda/m$. Unfortunately, the order of T may not be prime to m. Nevertheless, we have $\ell P = m'G + \ell T$ and the order of ℓT is prime to m' so that we can apply the previous case with ℓz instead of z. Note that Mazur's Theorem 8.1.16 implies that $\gcd(e, m^\infty) = \gcd(e, m^3)$ (see Definition 9.5.7).

(6) A point $z = \lambda_1\omega_1(E) + \lambda_2\omega_2(E)$ will correspond to a real point if and only if $\lambda_2 \in \mathbb{Z}$ if $\Delta < 0$, or $\lambda_2 \in \frac{1}{2}\mathbb{Z}$ if $\Delta > 0$. It is therefore easy to find for which $(u, v) \in [0, m' - 1]^2$ the point $z_{u,v}$ corresponds to a real point.

(7) Even after dividing by m' as in $z_{u,v}$ above, the point that we will obtain may be a large multiple of the Mordell–Weil generator. This will occur when $Ш(E)$ is nontrivial. In this case we can either increase the accuracy of the computations, or choose small multiples of m instead of m itself.

(8) The number of coefficients a_n which must be used in the series for ϕ can well exceed the capacity of a computer. In this case they must be computed inductively, see [GBZ] for details.

(9) As noted above, it may happen that the so-called Manin constant of the curve is not equal to 1. In that case we must on the contrary *multiply* the values $z_{u,v}$ by a small constant, which technically is the degree of the isogeny between E and the strong Weil curve in its isogeny class.

(10) Although the main algorithm suggests choosing discriminants D in increasing absolute value, it is clear that the best choice is to choose D for which the smallest value of $\sqrt{|D|}/A$ in Step 4 is as large as possible. The smallest $|D|$ is not always the best for this.

(11) We can also use the so-called Atkin–Lehner operators in order to increase the imaginary parts of the points $\tau \in \mathcal{H}$ corresponding to the forms (A, B, C), see Exercises 25 and 26. For this we must slightly adapt Subalgorithm 8.6.13 and use the fact that if W is such an operator then $\varphi \circ W = \varepsilon_W\varphi + T$ where $T \in E_t(\mathbb{Q})$ and $\varepsilon_W = \pm 1$ can easily be computed. Note also that we do not need to compute T.

For many practical improvements on this method, we refer to ongoing work of Delaunay, Watkins, and Cremona–Silverman.

8.6.5 A Complete Example

We consider the following problem. By Tunnell's theorem or by the BSD conjecture, we know that 157 is a congruent number, in other words there exists a rational nontorsion point on the elliptic curve $y^2 = x^3 - 157^2 x$. We want to compute such a point (from which it is easy to compute explicitly a Pythagorean triangle with area 157). We give explicitly the GP commands so that the reader can reproduce the computations himself. We should first choose a sufficiently large stack (200 MB is sufficient). We begin by the command `e = ellinit([0, 0, 0, -157^2, 0])` which computes a number of needed constants. In particular, the period lattice is generated by `om1 = e.omega[1]` and `om2 = e.omega[2]`, and since the discriminant is positive the real period is `om = 2*om1`. The command `et = elltors(e)` shows that $|E_t(\mathbb{Q})| = 4$, which we knew already in the congruent number problem, `vole = e.area` gives the volume, `ered = ellglobalred(e)` gives the conductor `N = ered[1]`, the Tamagawa product `c = ered[3]`, and the fact that the equation for E is in fact a minimal model. We now compute the necessary accuracy: we find that $|Ш(E)|R(E) \approx 54.6$ and $HB \approx 10.6$, hence $d \approx 130.4$, so we will perform our computations with a default accuracy of 67 decimal digits.

Since we performed the `ellinit` command with the default accuracy of 28, we must now change the default accuracy with the command `\p 67`, and then recompute `ellinit` and the values of the corresponding floating point numbers given above.

We now search for suitable fundamental discriminants. We find that up to $D = -40$, only $D = -31$ and $D = -39$ are squares modulo $4N$. The quantity $m^2 = m^2(D)$ of the algorithm can be computed by defining the function

```
m2(D) = v = ellan(e, 1000000); q = exp(-2*Pi/sqrt(N*D^2)); \
q1 = 1.; s = 0.; for (n = 1, 1000000, q1 *= q; \
s += v[n]/n*kronecker(D,n)*q1); \
                sqrt(-D)*c*om/(4*vole*et[1]^2)*2*s.
```

In the above, 1000000 is overkill, but we are lazy since the computation is very fast. We find that `m2(-31)` is very close to 0, so -31 is not suitable, but `m2(-39)` is very close to 16, so we choose $D = -39$ and $m = 4$. We easily find that $b = 1275547$ satisfies $b^2 \equiv D \pmod{4N}$, so we write `D = -39` and `b = 1275547`.

There are four classes of quadratic forms of discriminant -39, and with the notation of the algorithm, it is easy to see that we have $z = 2\Re(\phi(x_1)+\phi(x_2))$ with $x_j = (-b+\sqrt{-39})/(2jN)$. The largest value of A in the quadratic forms (A, B, C) is thus $A = 2N$. It follows that to compute z we will need more than $Ad/(\pi\sqrt{|D|})$ terms, giving here approximately 10.5 million. We thus write `v=ellan(e,10500000)`. This only requires 84 seconds on a 3.06 Ghz PC. Being lazy, we then write the function

```
ph(tau) = s = 0.; q = exp(2*I*Pi*tau); q1 = 1.; \
                for (n = 1, 10500000, q1 *= q; s += v[n]/n*q1); s
```

(we do not need 10.5 million terms for the computation of $\phi(x_1)$, but we are not optimizing here), and we compute z (in 78 seconds) thanks to the commands

```
z1 = ph((-b + I*sqrt(39))/(2*N)); \
          z2 = ph((-b + I*sqrt(39))/(4*N)); z = 2*real(z1 + z2);
```

and we find

$$z = -5.639111275008317660076961663073160363235624065747 06\cdots$$

We write `z += 27*om1` to make it as small as possible. Among the possible points to be studied in the algorithm, we see that $2z + 2\omega_1$ already does the trick. Since the nontrivial torsion points are $\omega_1/2$, $\omega_2/2$, and $(\omega_1 + \omega_2)/2$, it follows that $2z + 6\omega_1$, $2z + 2\omega_1 + 4\omega_2$, and $2z + 6\omega_1 + 4\omega_2$ would also work. Thus we compute $\wp((2z + 2\omega_1)/8)$ thanks to the command `x1 = ellwp(e, (2*z + 2*om1)/8)`. To have `x` as a rational number we write `rx = contfrac(real(x1))` (the imaginary part of `x1` is zero to the accuracy of our computations). This gives a continued fraction for the approximation x, which has a large partial quotient toward the end, precisely after index 39. We thus write

```
mx = contfracpnqn(vector(39, i, rx[i])); x = mx[1,1]/mx[2,1].
```

We check that the denominator of x is a perfect square, which is a good sign. To obtain the value of y, we can be lazy and use the built-in function `y=ellordinate(e,x)[1]`, or else write $x = n_x/f^2$, compute $n_x^3 - 157^2 n_x f^4$ and check that it is the square of some integer n_y, so that $y = n_y/f^3$. In any case we finally find the rational point

$$P = \left(\frac{957323593545015812583644 53}{277487787329244632169121}, \frac{834062764128948944072857085701103222940}{14617254579172152656815525943819 6081}\right).$$

See Exercise 30 for another example of the use of Heegner points.

8.7 Computation of Integral Points

For this section I have closely followed the presentation of Chapter XIII of [Sma].

8.7.1 Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$, but which we now assume to be given by a generalized Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \ ,$$

where the a_i are all integral. We want to compute the complete set $E(\mathbb{Z})$ of integral points on E, which by Siegel's theorem we know to be finite. Note

that although $E(\mathbb{Q})$ does not depend on the chosen model (i.e., equation or system of equations) for E, on the other hand $E(\mathbb{Z})$ does depends on the model.

We first describe the general strategy, and give details afterward. We assume that using one of the above methods we have completely computed the Mordell–Weil group $E(\mathbb{Q})$ (and not only the rank), in other words that we know the torsion subgroup $E_t(\mathbb{Q})$ of $E(\mathbb{Q})$ and an r-element basis $(P_i)_{1\leqslant i\leqslant r}$ of the torsionfree part of $E(\mathbb{Q})$, where r is the rank of E. Thus any element P of $E(\mathbb{Q})$, and in particular any element of $E(\mathbb{Z})$ can be written in the form

$$P = T + \sum_{1\leqslant j\leqslant r} p_j P_j$$

for some $T \in E_t(\mathbb{Q})$ and some $p_i \in \mathbb{Z}$.

A deep theorem generalizing the theorems of A. Baker on linear forms in logarithms to linear forms in *elliptic* logarithms implies that when $P \in E(\mathbb{Z})$, the $|p_j|$ are bounded by a (usually very large) constant. When we say very large, we mean something like e^{1000} for instance (see examples below). However the sheer *existence* of this bound is sufficient to continue. Applying a now classical method used by several authors and systematized by Tzanakis and de Weger, using lattice reduction algorithms such as the LLL algorithm we can *drastically* reduce the upper bound on the $|p_j|$ (see Section 2.3.5). Thus typically after two passes of the LLL algorithm we often obtain bounds such as $|p_j| \leqslant 30$. It then becomes possible to do a systematic search on the possible p_j, and we thus obtain the set $E(\mathbb{Z})$ of integral points.

The search for integral points on an elliptic curve is an important Diophantine problem, and although it requires techniques of a different kind than those that we have studied up to now, its importance justifies a detailed study of the necessary tools. By nature the present section is more algorithmic than most of the rest of this book.

8.7.2 An Upper Bound for the Elliptic Logarithm on $E(\mathbb{Z})$

Let E be an elliptic curve defined over $\mathbb{Q}$ by a generalized (affine) Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ where we assume $a_i \in \mathbb{Z}$. We assume (and this is of course the essential and difficult assumption) that we have explicitly computed the Mordell–Weil group $E(\mathbb{Q})$, in other words the finite group $E_t(\mathbb{Q})$ and independent points P_i for $1 \leqslant i \leqslant r$ such that

$$E(\mathbb{Q}) = E_t(\mathbb{Q}) \oplus \bigoplus_{1\leqslant i\leqslant r} \mathbb{Z}P_i\,.$$

Consider the *height pairing matrix* $Q = (\langle P_i, P_j\rangle)_{1\leqslant i,j\leqslant r}$, which we have already introduced, where as usual $\langle P_i, P_j\rangle$ is the bilinear form associated to the canonical height function $\widehat{h}$ Since by definition the P_i are independent this

matrix is nonsingular, and it is the matrix of a positive definite quadratic form on $E(\mathbb{Q})/E_t(\mathbb{Q})$, hence all its eigenvalues λ_i are strictly positive. In particular $R(E) = \det(Q) = \prod_i \lambda_i > 0$ is the *regulator* of E, and is independent of the choice of the P_i.

Now let $P = (x(P), y(P)) \in E(\mathbb{Z})$ be an (unknown) *integral* point. We can write in a unique way $P = T + \sum_{1 \leqslant i \leqslant r} p_i P_i$ for some $T \in E_t(\mathbb{Q})$ and $p_i \in \mathbb{Z}$, and we set $H = \max_i(|p_i|)$. Our main goal is to find inequalities for $1/|x(P)|$ involving H and the elliptic logarithm $\psi(P)$. Since E^{gg} is compact, it is usually very easy to find all integral points on it, hence we will always assume that $P \in E^0$ (although it would be a simple matter to generalize to the whole of $E(\mathbb{Q})$). Also we may evidently assume that $x(P) \neq 0$.

Lemma 8.7.1. *Keep the above notation, let* $c_2 = \min_{1 \leqslant i \leqslant r} \lambda_i$ *be the smallest eigenvalue of* Q*, and set* $c_1 = \exp(\mu(E) + 2.14)$ *where* $\mu(E)$ *is defined in Theorem 8.1.18. If* $P = (x(P), y(P)) \in E(\mathbb{Z})$ *is any integral point with* $x(P) \neq 0$ *and* $H = \max_i(|p_i|)$ *as above then*

$$\frac{1}{|x(P)|} \leqslant c_1 e^{-c_2 H^2} .$$

Proof. Since $x(P) \in \mathbb{Z} \setminus \{0\}$ we have $h(P) = \max(\log(|x(P)|), 0) = \log(|x(P)|)$, hence by Theorem 8.1.18 $\log(|x(P)|) \geqslant \widehat{h}(P) - \log(c_1)$, with c_1 defined as above. Let $X = (p_1, \ldots, p_r)^t$ be the column vector of the p_i. Since $\widehat{h}$ is a positive definite quadratic form on $E(\mathbb{Q})/E_t(\mathbb{Q})$ with matrix Q, we have $\widehat{h}(P) = X^t Q X$. A standard undergraduate exercise (see Exercise 32) shows that

$$\widehat{h}(P) \geqslant c_2 X^t X \geqslant c_2 \sum_{1 \leqslant i \leqslant r} p_i^2 \geqslant c_2 H^2 ,$$

proving the lemma. □

We now want a link between $x(P)$ and the elliptic logarithm $\psi(P)$. After the standard transformations explained in the preceding chapter we can put our curve in the form $Y^2 = f(X)$ with $f(X) = 4X^3 - g_2 X - g_3$, where $g_2 = c_4/12$ and $g_3 = c_6/216$, and where we recall that $X = x + b_2/12$. Denote as usual by e_1, e_2 and e_3 the complex roots of $f(X) = 0$.

The following lemma relates $\psi(P)$ to $x(P)$ for any real point $P \in E^0$, not necessarily integral.

Lemma 8.7.2. *Let* $P = (x(P), y(P)) \in E^0$ *be a real point, and assume that* $|x(P) + b_2/12| \geqslant 2\max(|e_1|, |e_2|, |e_3|)$*. If we choose the (essentially) unique determination of* $\psi(P)$ *such that* $|\psi(P)| \leqslant \omega_1/2$ *we have*

$$\psi(P)^2 \leqslant \frac{c_3}{|x(P)|} \quad \textit{where} \quad c_3 = \frac{\omega_1^2 |b_2|}{48} + 8 .$$

Proof. Write $P = (X(P), Y(P))$. Since $P \in E^0$ we have $X(P) \geqslant e_3$. Since $X(P) = x(P) + b_2/12$ this implies that $X(P) > 0$ otherwise $e_3 \leqslant X(P) \leqslant 0$, hence $|X(P)| \leqslant |e_3|$, contrary to our assumption. Now as mentioned in Section 7.3.2, for $P \in E^0$ and the chosen determination we have the explicit formula

$$\psi(P) = \mathrm{sign}(Y(P)) \int_\infty^{X(P)} \frac{dt}{\sqrt{f(t)}} \, .$$

By assumption if $t \geqslant X(P)$ we have $t \geqslant 2|e_i|$ for $1 \leqslant i \leqslant 3$, hence

$$|t - e_i| \geqslant t - |e_i| = \frac{t - 2|e_i|}{2} + \frac{t}{2} \geqslant \frac{t}{2} \, .$$

It follows that $|f(t)| = 4 \prod_{1 \leqslant i \leqslant 3} |t - e_i| \geqslant t^3/2$, hence

$$|\psi(P)| = \left| \int_\infty^{X(P)} \frac{dt}{\sqrt{f(t)}} \right| \leqslant 2^{1/2} \int_{X(P)}^\infty \frac{dt}{t^{3/2}} \leqslant \frac{2^{3/2}}{\sqrt{X(P)}}$$

or, equivalently, $X(P) \leqslant 8/\psi(P)^2$. We thus have

$$\begin{aligned} |x(P)| = \left| X(P) - \frac{b_2}{12} \right| &\leqslant X(P) + \frac{|b_2|}{12} \leqslant \frac{8}{\psi(P)^2} + \frac{|b_2|}{12} \\ &\leqslant \frac{8 + \psi(P)^2 |b_2|/12}{\psi(P)^2} \leqslant \frac{8 + \omega_1^2 |b_2|/48}{\psi(P)^2} \end{aligned}$$

since $|\psi(P)| \leqslant \omega_1/2$, proving the lemma. □

From now on, when $P \in E^0$ we will always assume that we choose the above *principal determination* of $\psi(P)$, i.e., such that $|\psi(P)| \leqslant \omega_1/2$.

Corollary 8.7.3. *Let c_i be the constants defined in the above two lemmas and set $c_5 = \sqrt{c_1 c_3}$. If $P = (x(P), y(P))$ is an integral point in E^0 with $x(P) \neq 0$ and if $|x(P) + b_2/12| \geqslant 2 \max(|e_1|, |e_2|, |e_3|)$ then*

$$|\psi(P)| \leqslant c_5 e^{-c_2 H^2/2} \, .$$

Proof. Clear by combining the two lemmas. □

8.7.3 Lower Bounds for Linear Forms in Elliptic Logarithms

Now is the time to introduce high technology. This should be taken as an easy-to-use black box, but the reader should be aware that the mathematics and computations leading to lower bounds for linear forms in logarithms (elliptic or not) initiated by A. Baker, are one of the major advances in number theory in the second half of the twentieth century.

The following theorem is due to S. David, and we only give the special case of $\mathbb{Q}$. For the general case, as well as the corresponding statements for linear forms in complex or p-adic logarithms, I refer to [Sma].

First, we need some notation. Let E be an elliptic curve defined over $\mathbb{Q}$, and as above let $Y^2 = 4X^3 - g_2X - g_3$ be the equation of E obtained after the standard changes of variable. Recall that if $P = (x_0 : \cdots : x_n) \in \mathbb{P}^n(\mathbb{Q})$ we have defined $h(P) = \max_{0 \leqslant i \leqslant n} \log(|y_i|)$, where $P = (y_0 : \cdots : y_n)$ is one of the two representations with $y_i \in \mathbb{Z}$ for all i and $\gcd(y_0, \ldots, y_n) = 1$, hence in particular if $u = n/d \in \mathbb{Q}^*$ with $\gcd(n, d) = 1$ we have $h(u) = \max(\log(|n|), \log(|d|))$. We define the height $h(E)$ of the elliptic curve by the formula

$$h(E) = \max(1, h(1, g_2, g_3), h(j(E)))$$

and we set $c_7 = 3\pi/(\omega_1^2 \Im(\omega_1/\omega_2))$. If $P \in E(\mathbb{Q})$ we define a modified height function $h_m(P)$ by the formula

$$h_m(P) = \max(\widehat{h}(P), h(E), c_7|\psi(P)|^2) \ .$$

Theorem 8.7.4 (David). *Let $P_1, \ldots, P_n$ be points in $E(\mathbb{Q})$, and set*

$$c_8 = \max(eh(E), \max_{1 \leqslant i \leqslant n} h_m(P_i)) \quad \textit{and} \quad c_9 = \frac{e}{\sqrt{c_7}} \min_{1 \leqslant i \leqslant n} \frac{\sqrt{h_m(P_i)}}{|\psi(P_i)|} \ .$$

For $p_i \in \mathbb{Z}$ we set $H = \max(|p_i|)$, and $L = \sum_{1 \leqslant i \leqslant n} x_i\psi(P_i)$, Then if $H \geqslant \exp(c_8)$ and $L \neq 0$ we have

$$\log(L) > -c_{10}(\log(H) + \log(c_9))(\log(\log(H)) + h(E) + \log(c_9))^{n+1} \ ,$$

where

$$c_{10} = 2 \cdot 10^{8+7n}(2/e)^{2n^2}(n+1)^{4n^2+10n} \log(c_9)^{-2n-1} \prod_{1 \leqslant i \leqslant n} h_m(P_i) \ .$$

Remark. Recall that $\psi(P)$ is only defined modulo Λ. This theorem is valid for any determination of $\psi(P)$. In particular we have $\psi(\mathcal{O}) \equiv 0 \pmod{\Lambda}$, so by choosing one of the P_i equal to $\mathcal{O}$ we can include any integral linear combination of ω_1 and ω_2 among the $\psi(P_i)$.

We now explain how to use this theorem combined with Corollary 8.7.3 to find integral points. As already mentioned, the fundamental assumption is that we have computed exactly the Mordell–Weil group as

$$E(\mathbb{Q}) = E_t(\mathbb{Q}) \oplus \bigoplus_{1 \leqslant i \leqslant r} \mathbb{Z}P_i \ ,$$

and we recall from Section 7.3.2 that we have a disjoint union $E(\mathbb{R}) = E^{gg} \cup E^0$, where E^0 is the connected component of the identity, and the possibly empty set E^{gg} is compact. I claim that we can assume that at most one of

the P_i is in E^{gg}: indeed, if $P_i \in E^{gg}$ and $P_j \in E^{gg}$ with $i \neq j$, then in the Mordell–Weil basis we may replace $\{P_i, P_j\}$ by $\{P_i + P_j, P_j\}$, and since $P_i + P_j \in E^0$ by Section 7.3.2, we have one point less in E^{gg}, proving my claim. We may thus assume that $P_i \in E^0$ for $2 \leqslant i \leqslant r$.

We write our integral point P as $P = T + \sum_{1 \leqslant i \leqslant r} p_i P_i$ for some unknown $T \in E_t(\mathbb{Q})$ and $p_i \in \mathbb{Z}$. We may clearly assume that $P \in E^0$, that $P \notin E_t(\mathbb{Q})$ (so that the p_i are not all equal to 0), and that $x(P) \neq 0$, since all the points that we exclude in this way are easy to find. Since we want to restrict to E^0 we set $Q_i = P_i$ for $2 \leqslant i \leqslant r$, and $Q_1 = 2P_1$ if $P_1 \in E^{gg}$ and $Q_1 = P_1$ if $P_1 \in E^0$, so that $Q_i \in E^0$ for all i. We can thus write $P = T + U + \sum_{1 \leqslant i \leqslant r} q_i Q_i$, where $q_i = p_i$ if $i \geqslant 2$ or if $i = 1$ and $P_1 \in E^0$, and $q_1 = \lfloor p_1/2 \rfloor$ if $P_1 \in E^0$, and $U = P_1$ if $P_1 \in E^{gg}$ and p_1 is odd, $U = \mathcal{O}$ otherwise. Since P and the Q_i are in E^0 we also have $T + U \in E_0$, so that $T + U$ belongs to a finite set having at most $2|E_t(\mathbb{Q})|$ elements. We will write $Q_{r+1} = T + U$ (we can of course avoid this extra point if we know in advance that it will be equal to $\mathcal{O}$, for instance if $P_1 \in E^0$ and $E_t(\mathbb{Q}) = \{\mathcal{O}\}$).

By definition the elliptic logarithm is additive modulo Λ, and since on E^0 we have chosen the principal determination it is clear that if $P = \sum_{1 \leqslant i \leqslant n} R_i$ then $\psi(P) = m\omega_1 + \sum_{1 \leqslant i \leqslant n} \psi(R_i)$ where $|m| \leqslant \lfloor n/2 \rfloor$. In particular

$$\psi(P) = m\omega_1 + \psi(Q_{r+1}) + \sum_{1 \leqslant i \leqslant r} q_i \psi(Q_i)$$

with $|m| \leqslant (1 + \sum_{1 \leqslant i \leqslant r} |q_i|)/2$, and even $|m| \leqslant \sum_{1 \leqslant i \leqslant r} |q_i|/2$ if $Q_{r+1} = \mathcal{O}$. This is a linear form in elliptic logarithms, so we can combine Corollary 8.7.3 with David's theorem. If we set $L = \psi(P)$ and

$$H_q = \max(1, \max(|q_i|)) \leqslant \max(|p_i|) = H \ ,$$

Corollary 8.7.3 tells us that when $|x(P) + b_2/12| \geqslant 2\max(|e_1|, |e_2|, |e_3|)$ we have

$$-\log(|L|) \geqslant c_2 H^2/2 - \log(c_5) \geqslant c_2 H_q^2/2 - \log(c_5) \ ,$$

and David's theorem (applied to the Q_i and to $n = r + 2$ or to $n = r + 1$ if $Q_{r+1} = \mathcal{O}$) implies that

$$-\log(|L|) < c_{10}(\log(H_r) + \log(c_9))(\log(\log(H_r)) + h(E) + \log(c_9))^{n+1} \ ,$$

where $H_r = rH_q + 1$, or $H_r = rH_q$ when $Q_{r+1} = \mathcal{O}$. Since the upper bound grows logarithmically in H_q and the lower bound grows like H_q^2, it is clear that these bounds are contradictory for H_q sufficiently large.

Since all the constants are explicit we can thus compute some bound B such that $H_q > B$ leads to a contradiction, so that we know that $H_q = \max(|q_i|) \leqslant B$. This bound will usually be extremely large, but now we use the techniques explained in Section 2.3.5 (in particular Corollary 2.3.17 and Proposition 2.3.20) to the inequality $|L| \leqslant c_5 \exp(-c_2 H_q^2/2)$, possibly two or three times, to reduce the bound to something manageable which we then enumerate by brute force.

8.7.4 A Complete Example

Since the above description contains a lot of notation and may be hard to understand at first, the best is to give in detail a complete example. We will again consider the curve $y^2+y=x^3-7x+6$ studied in detail in Section 8.5.6. We have seen that it has no torsion, and that it has rank 3, where generators can be taken to be $P_1=(2,0)$, $P_2=(-1,3)$ and $P_3=(4,6)$. The reduced Weierstrass equation of this curve is obtained by setting $Y=2y+1$ and $X=x$, so that $Y^2=4X^3-28X+25$. We thus compute that $b_2=0$, $g_2=28$, $g_3=-25$, $\mathrm{disc}(E)=5077$, $j(E)=37933056/5077$, hence $h(E)=17.45$, $\mu(E)=3.90855$, $c_1=423.5$, $\lambda_1=0.3228$, $\lambda_2=0.4925$, $\lambda_3=2.623$, hence $c_2=0.3228$, $c_3=8$, $c_5=58.21$, $e_1=-3.0124$, $e_2=1.0658$, $e_3=1.9466$. Thus if $P=p_1P_1+p_2P_2+p_3P_3\in E^0$ is an integral point such that $|x(P)|\geqslant 7$ we have the fundamental inequality $|\psi(P)|\leqslant 58.21\exp(-0.1614H^2)$, where $H=\max(p_i)$. Now among the P_i only P_2 is in E^{gg}, so we set $Q_1=P_1$, $Q_3=P_3$, and $Q_2=2P_2=(114/49,-720/343)$. Since there is no torsion we have $P=q_1Q_1+q_2Q_2+q_3Q_3+U$ with $q_1=p_1$, $q_2=\lfloor p_2/2\rfloor$, $q_3=p_3$ and $U=\mathcal{O}$ or P_2, but since we only look for $P\in E^0$, we have in fact $U=\mathcal{O}$, $q_2=p_2/2$ and $Q_4=\mathcal{O}$.

We are now ready to apply David's theorem to the form $L=m\omega_1+q_1\psi(Q_1)+q_2\psi(Q_2)+q_3\psi(Q_3)$ (hence $n=4$), where $m\leqslant(|q_1|+|q_2|+|q_3|)/2\leqslant(3/2)\max(|q_i|)$. We find $c_7=1.5599$, $h_m(Q_i)=h(E)$, hence $c_8=47.4376$, $c_9=5.8503$, and finally $c_{10}=2.97\cdot 10^{107}$. Thus we have the inequalities

$$-\log(|\psi(P)|)\geqslant 0.1614H_q^2-4.064\quad\text{and}$$
$$-\log(|\psi(P)|)\leqslant 2.97\cdot 10^{107}(\log(1.5H_q)+1.7665)(\log(\log(1.5H_q))+19.218)^5\,,$$

the second one being valid only for $1.5H_q>\exp(c_8)=4.01\cdot 10^{20}$. We immediately find that these equations are incompatible for $H_q>10^{60}$, hence we have a first basic upper bound $H_q\leqslant 10^{60}$. Note that it is completely unnecessary to take sharp bounds anywhere in this computation, since the next step, i.e., the use of the LLL algorithm, will drastically reduce the bound anyway. Since we are no longer going to use David's theorem, we can also forget the lower bound $(3/2)H_q>4.01\cdot 10^{20}$ necessary for the validity of his theorem.

After having used the above high technology, we can now use the magic of the LLL algorithm, more precisely Corollary 2.3.17 and Proposition 2.3.20 applied to the inequality

$$|m\omega_1+q_1\psi(Q_1)+q_2\psi(Q_2)+q_3\psi(Q_3)|\leqslant 58.21\exp(-0.1614H_q^2)\,,$$

where we now know that $H_q=\max(|q_i|)\leqslant 10^{60}$ and $m\leqslant 1.5\cdot 10^{60}$. We first choose $C>(10^{60})^4$, say $C=10^{250}$, and form the 4×4 matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ \lfloor C\psi(Q_1)\rceil & \lfloor C\psi(Q_2)\rceil & \lfloor C\psi(Q_3)\rceil & \lfloor C\omega_1\rceil \end{pmatrix}.$$

An application of the (integral) LLL algorithm shows that the first vector of an LLL-reduced basis of the lattice generated by the columns of $\mathcal{B}$ is an explicit vector whose entries have approximately 60 decimal digits. We easily compute that for $i = 1, 2, 3, 4$ we have $\|\mathbf{b}_1\|^2/\|\mathbf{b}_i^*\|^2 = 1, 0.718, 0.426, 0.338$ respectively, so that with the notation of Corollary 2.3.17 we have $c_1 = 1$, hence

$$d(L,0)^2 \geqslant \|\mathbf{b}_1\|^2/c_1 \geqslant 2.5 \cdot 10^{120} .$$

With the notation of Proposition 2.3.20 we have $Q = 3 \cdot 10^{120}$ and $T = (1 + 4.5 \cdot 10^{60})/2$, so $d(L,0)^2 \geqslant T^2 + Q$. Since the points Q_i are independent, we deduce from Proposition 2.3.20 that

$$|q_1\psi(Q_1) + q_2\psi(Q_2) + q_3\psi(Q_3) + m\omega_1| \geqslant 1.5 \cdot 10^{-184} .$$

Combining this with the inequality

$$|q_1\psi(Q_1) + q_2\psi(Q_2) + q_3\psi(Q_3) + m\omega_1| \leqslant 58.21e^{-0.1614H_q^2}$$

gives $H_q \leqslant 51$, which is much more manageable than our initial bound of 10^{60}.

Although 51 is now a reasonable number it is worthwhile to iterate the whole LLL process using the new inequality $H_q \leqslant 51$. This time we must be a little careful with the choice of C so as to be able to obtain an improvement using Proposition 2.3.20. We choose $C = 10^9$, and after a similar computation as that performed above we find the new bound $H_q \leqslant 11$. By using still another LLL process with $C = 10^7$, we could still reduce this to $H_q \leqslant 10$, but there is not much point in doing so.

We now perform a direct systematic search: on E^{gg} we find the integral points $(-3,0)$, $(-3,-1)$, $(-2,3)$, $(-2,-4)$, $(-1,3)$, $(-1,-4)$, $(0,2)$, $(0,-3)$, $(1,0)$, $(1,-1)$, $(2,0)$, $(2,-1)$. The points on E^0 with $x(P) \leqslant 6$ are $(3,3)$, $(3,-4)$, $(4,6)$ and $(4.-7)$. All the others are on E^0 with $x(P) \geqslant 7$, hence of the form $q_1Q_1 + q_2Q_2 + q_3Q_3$ with $|q_i| \leqslant 11$, and we may assume $q_1 \geqslant 0$ if we take care to compute also the opposites of the points which we find. Thus after searching through $12 \cdot 23^2 = 6348$ points we find (in seconds) the additional integral points (where we of course also include the opposites of the points found) $(8,21)$, $(8,-22)$, $(11,35)$, $(11,-36)$, $(14,51)$, $(14,-52)$, $(21,95)$, $(21,-96)$, $(37,224)$, $(37,-225)$, $(52,374)$, $(52,-375)$, $(93,896)$, $(93,-897)$, $(342,6324)$, $(342,-6325)$, $(406,8180)$, $(406,-8181)$, $(816,23309)$, $(816,-23310)$, all corresponding to coefficients q_i with $H_q = \max(|q_i|) \leqslant 3$. We have thus found a total of 36 integral points, and we have *proved* (this was of course the main difficulty) that there are no others.

It should be remarked that 36 is a very large number of integral points for an elliptic curve, but it is a completely general and only partly understood phenomenon: if we choose an elliptic curve having the smallest or one of the smallest conductors for a given rank, it will have a large number of integral points. Indeed, it is known that our curve is the curve of rank 3 with the smallest conductor (see Exercise 33 for rank 2).

8.8 Exercises for Chapter 8

1. Prove Corollary 8.1.9.

2. Let R be a commutative ring, let $f \in R[X]$ be a monic polynomial, let $A = R[X]/(f(X)R[X])$, and let α be the class of X modulo $f(X)$, so that $f(\alpha) = 0$. Finally, set $g(Y) = (f(Y) - f(\alpha))/(Y - \alpha) = f(Y)/(Y - \alpha) \in A[Y]$.

(a) Prove that
$$\mathrm{disc}(g) = g(\alpha)^2 \,\mathrm{disc}(f) = f'(\alpha)^2 \,\mathrm{disc}(f) \ .$$

(b) Deduce the existence of polynomials U and V in $R[X]$ such that $U(X)f(X) + V(X)(f'(X))^2 = \mathrm{disc}(f)$, thus explaining the identity used in the proof of Theorem 8.1.10 (I thank H. W. Lenstra for this proof).

3. Generalizing Theorem 8.1.10, let E be an elliptic curve given by $y^2+a_1xy+a_3y = x^3 + a_2x^2 + a_4x + a_6$ with $a_i \in \mathbb{Z}$, and let $T = (x, y)$ be a torsion point of order not dividing 2. Show the following:

(a) $(x, y) \in \mathbb{Z}^2$ and $(2y + a_1x + a_3)^2 \mid 4\,\mathrm{disc}(E)$.
(b) If $a_1 \in 2\mathbb{Z}$ then $(2y + a_1x + a_3)^2 \mid \mathrm{disc}(E)$.
(c) If $a_1 \in 2\mathbb{Z}$ and $a_3 \in 2\mathbb{Z}$ then $(y + (a_1/2)x + (a_3/2))^2 \mid \mathrm{disc}(E)/16$.

4. Using Sections 7.3.6 and 7.3.7, generalize the Nagell–Lutz Theorem 8.1.10 to a general number field.

5. Prove Corollary 8.1.15 (2).

6. Using reductions to standard Weierstrass form, compute a Weierstrass equation for the hyperelliptic quartic curve $y^2 = 226x^4 - 1$ using the known rational point $(x, y) = (1, 15)$, and show that the rank of this elliptic curve is equal to 3.

7. (Bremner–Tzanakis.) This exercise is a sequel to Exercise 40 of Chapter 6, whose notation we keep.

(a) By setting $x = -P/Q^2$ show that for $n = 7$ coprime pairs (P, Q) as in the above-mentioned exercise are in one-to-one correspondence with rational points on the elliptic curve E whose equation is $y^2 = x^3 + 6x^2 + 5x + 1$.
(b) By using the methods of this chapter, show that this curve has no torsion, and that it has rank 1 generated by the point $(-1, 1)$.
(c) Give the first seven coprime pairs (P, Q) coming from the preceding question.

In their papers [Bre-Tza1] and [Bre-Tza2] the authors solve in detail the cases $n = 8$ and $n = 12$, and conjecture that such coprime pairs cannot exist for other values of n.

8. Let E be the elliptic curve $Y^2 = X^3 - 34992$.

(a) Using `mwrank` or descent, show that E has rank 1 and no torsion, a generator being $P = [36, 108]$, which corresponds to the point $(x, y) = (1, 2)$ under the birational transformation of Proposition 7.2.3.
(b) Using the group law and that proposition, solve Fermat's challenge (which he knew how to solve) of finding *strictly positive* coprime integers x, y, and z such that $x^3 + y^3 = 9z^3$ other than $(1, 2, 1)$ and $(2, 1, 1)$ (the smallest answer has 12 decimal digits).
(c) Perform the same computation, but now using Exercise 9 (b) of Chapter 7.

9. Find all $x \in \mathbb{Q}$ be such that x^2+4 is the square of a rational number and

$$2+2x-\frac{4x}{x^2+4}+2\frac{x^2+x+2}{\sqrt{x^2+4}}$$

is also the square of a rational number (reduce to finding all rational points on an elliptic curve).

10. (Mestre.) Let r_1, r_2, r_3 and r_4 be distinct rational numbers and let $t \in \mathbb{Q}$ be a parameter. Consider the 12th degree polynomial

$$P(X)=\prod_{1\leqslant i,j\leqslant 4,\ i\neq j}(X-(r_i+tr_j))\,.$$

(a) By considering the Laurent series expansion of $Q^{1/3}$ show that for any monic polynomial Q of degree 12 there exists a unique polynomial $g \in \mathbb{Q}[X]$ such that $\deg(Q(X)-g^3(X)) \leqslant 7$, and show that in our special case we have in fact $\deg(P(X)-g^3(X)) \leqslant 6$.

(b) Show that there exists $q(X) \in \mathbb{Q}[X]$ and $r(X) \in \mathbb{Q}[X]$ such that $P(X) = g^3(X)+q(X)g(X)+r(X)$ with $\deg(q) \leqslant 2$ and $\deg(r) \leqslant 3$.

(c) Deduce from this that the equation $Y^3+q(X)Y+r(X)=0$ is the equation of a cubic with rational coefficients, and that the 12 points $(r_i+tr_j, g(r_i+tr_j))_{i\neq j}$ give 12 (not necessarily distinct) rational points on this cubic.

(d) Give explicit values of the r_i and t for which the cubic is non-singular, the above 12 points are distinct and in fact linearly independent for the group law on the cubic.

(e) Using the algorithm described in Section 7.2.4, find a Weierstrass equation corresponding to the cubic, and give explicitly an elliptic curve defined over $\mathbb{Q}$ whose rank is at least equal to 11 as well as 11 independent points on the elliptic curve (note that we have to "lose" a point in order to obtain an elliptic curve).

Remarks.

(a) To answer the last two questions of this exercise, the reader is strongly advised to use a package such as `mwrank`.

(b) The largest known rank for an elliptic curve defined over $\mathbb{Q}$ is 24, see [Mar-McM].

11. (R. Schoof.) Define a *Cassels–Sansone number* (abbreviated to CS number) as an integer a of the form $x/y+y/z+z/x$ for some nonzero integers x, y, and z. We let C_a be the curve with projective equation $x^2z+y^2x+z^2y=axyz$.

(a) Prove that C_a is an elliptic curve if and only if $a \neq 3$, and give a rational parametrization of the curve C_3. From now on we assume $a \neq 3$.

(b) Let E_a be the elliptic curve with affine equation $y^2+axy+y=x^3$. Show that E_a and C_a are isogenous over $\mathbb{Q}$, and give explicitly the isogenies and their degree.

(c) The point $T=(0,0)$ is trivially a point of order 3 on E_a. Prove that the torsion subgroup of E_a is strictly larger than $<T>$ if and only if $a=-1$ and $a=5$, and give the torsion subgroup in these cases, as well as the corresponding points on the curve C_a.

(d) Prove that a is a CS number if and only if $a=-1$, 3, 5, or if the rank of the elliptic curve E_a is at least equal to 1.

(e) Using Tate's algorithm, it can be shown that the sign of the functional equation of $L(E_a,s)$ is equal to $(-1)^{d-1}$ if $3 \nmid a$ or if $a \equiv 12 \pmod{27}$, and is equal to $(-1)^d$ otherwise, where d is the number of prime divisors of a^3-27 which are congruent to 1 modulo 3. Using BSD, deduce a sufficient condition for a to be a CS number.

(f) By computing numerically $L(E_a, 1)$ when the sign of the functional equation is equal to 1, make a small table of CS numbers.
(g) By using the Heegner point method, compute explicitly integers x, y, and z such that $x/y + y/z + z/x = -32$.
(h) Show that if a is a CS number the Diophantine equation $x^3+y^3+z^3 = axyz$ has a nontrivial solution, but that the converse is false. Does this remark simplify the Heegner point computation of the preceding question?

12. Using a software package such as `mwrank` or descent methods, show that the parabolic-type super-Fermat equations $x^2 + y^4 = 2z^4$ and $x^4 + 8y^4 = z^2$ have an *infinity* of integral solutions with x, y and z pairwise coprime (reduce to a hyperelliptic quartic). Find all such solutions with $\min(|x|, |y|, |z|) \leqslant 10^{100}$.
13. Consider the hyperelliptic quartic equation $y^2 = (x-1)x(x+1)(x+2)$.
(a) Using Proposition 7.2.1, find a generalized (not necessarily minimal) Weierstrass equation for this elliptic curve.
(b) Compute its torsion subgroup and its rank, using 2-descent.
(c) Deduce the following result due to Euler: the product of 4 integers in arithmetic progression can never be a nonzero square, in other words the only solutions in $\mathbb{Z}$ to the Diophantine equation $n(n+d)(n+2d)(n+3d) = m^2$ have $m = 0$.

14. In this chapter, in Chapter 14, and at other places we needed to explicitly compute the Mordell–Weil group of a number of elliptic curves. Although we can use Cremona's `mwrank` package, it is instructive to do some of the calculations by hand. Perform explicitly the necessary computations as follows. For each given curve E, first transform it into the canonical 2-descent form $y^2 = x^3 + ax^2 + bx$ (when it has rational 2-torsion, which will usually be the case), and compute $\alpha(E)$ and $\widehat{\alpha}(\widehat{E}(\mathbb{Q}))$ by looking at the real, 2-adic or 3-adic solubility of the necessary quartics.
(a) $y^2 = (x-1)(x^2-14x+1)$: show that $|\alpha(E(\mathbb{Q}))| = 2$ and $|\widehat{\alpha}(\widehat{E}(\mathbb{Q}))| = 2$, hence $r(E) = 0$.
(b) $y^2 = (x+1)(x^2+14x+1)$: show that $|\alpha(E(\mathbb{Q}))| = 4$ and $|\widehat{\alpha}(\widehat{E}(\mathbb{Q}))| = 2$, so that $r(E) = 1$, and give explicit generators.
(c) $y^2 = (x-1)(x^2-4)$: show that $|\alpha(E(\mathbb{Q}))| = 4$ and $|\widehat{\alpha}(\widehat{E}(\mathbb{Q}))| = 1$, so that $r(E) = 0$.
(d) $y^2 = x^3 - 8$: show that one can reduce to the equation studied in (a), hence that $r(E) = 0$.
(e) $y^2 = x(x^2-9)$: show that $|\alpha(E(\mathbb{Q}))| = 4$ and $|\widehat{\alpha}(\widehat{E}(\mathbb{Q}))| = 1$, so that $r(E) = 0$.
(f) $y^2 = 9x^4+18x^2+1$: show that this curve is isomorphic to $y^2 = x(x^2-9)$ hence that $r(E) = 0$.
(g) $y^2 = 12x^4+1$: setting $y = 1+xY$ and using the algorithm described in Section 7.2.4 and Proposition 8.2.15 show that $r(E) = 0$.

15. Continue the study of 3-descent by first proving an analogue of Proposition 8.2.4 (3) and (4). You will need in particular to work with prime *ideals* of K_d. Prove also an analogue of Proposition 8.2.8.

16. Let E be an elliptic curve defined over a field K of characteristic 0. It is clear (and we have used this fact in 2-descent) that if E has a rational point of order 2 its equation can be taken of the form $y^2 = x^3 + ax^2 + bx$ (here and afterwards the parameters a and b are implicitly assumed to be in K).
(a) Using Proposition 8.4.2, show that if E has a rational point of order 3 its equation can be taken of the form

$$y^2 + by = x^3 + a^2x^2 + abx \ .$$

(b) By writing $2[0,0] = -2[0,0]$, show that if E has a rational point of order 4 its equation can be taken of the form

$$y^2 + 2aby = x^3 + (a+b^2)x^2 + 2ab^2x\ .$$

(c) By writing $3[0,0] = -2[0,0]$, show that if E has a rational point of order 5 its equation can be taken of the form

$$y^2 + (2a-b)b^2y = x^3 + (a^2+2ab-b^2)x^2 + (2a-b)ab^2x$$

(hint: transform the polynomial relation between a_2, a_3, and a_4 obtained from $3[0,0] = -2[0,0]$ by setting $a_4 = ta_3$, dividing by a_3^6, setting $z = a_2 - t^2$, solving in t, and simplifying the resulting equation).

(d) Using practically the same method as for order 5, show that if E has a rational point of order 6 its equation can be taken of the form

$$y^2 - 2a(a-b)(2a-b)y = x^3 - (2a^2 - 6ab + 3b^2)x^2 - 2ab(a-b)(2a-b)x\ .$$

Note that since these equations are not unique, your results may be a little different.

17. Using Legendre symbols or otherwise, prove that if E_1 is the elliptic curve with affine equation $y^2 = x^3 + 1$ we have $a_p(E_1) \equiv 0 \pmod 2$. Using Propositions 2.5.20 and 8.5.3, deduce Corollary 8.5.4.

18. The aim of this exercise is to study the decomposition of 22 as a sum of two rational cubes.

(a) Let x, y, z be pairwise coprime integers such that $x^3 + y^3 = 22z^3$ (since 22 is cubefree, it is clear that we can reduce to this case). Show that $66 \mid x+y$ and that x and y are odd.

(b) Using this and making a systematic search with $|y| \leqslant x$, show that 22 is the sum of two rational cubes by giving explicitly x, y and z.

(c) Thanks to Proposition 7.2.3, we can also study the rational points on the elliptic curve E whose Weierstrass equation is $y^2 = x^3 - 432 \cdot 22^2$ or, more simply $y^2 = x^3 - 27 \cdot 11^2$ by changing (x,y) to $(4x, 8y)$. Using Proposition 8.5.6 and the remark that follows, show that $\varepsilon(E) = -1$, hence that under the BSD conjecture the rank of E is odd, hence at least equal to 1, so that 22 is indeed a sum of two rational cubes.

(d) Show that $L'(E,1) \neq 0$, hence that the analytic rank of E is equal to 1. By the *proven* results of Gross–Zagier et al, this shows that the rank of E is equal to 1.

(e) By performing a general 2-descent, find explicitly a rational point on E, and hence a decomposition of 22 as a sum of two rational cubes.

(f) Do the same, but now using the Heegner point method, since we know that E has rank 1.

19. Set

$$f(x) = xe^x E_1(x) = xe^x \int_x^\infty \frac{e^{-t}}{t}\,dt\ .$$

(a) Show that if we set $y_0(t) = f(1/t)$ then y_0 is a solution of the differential equation $t^2y' + (1+t)y - 1 = 0$.

(b) Prove that y_0 is a C^∞ function around $t = 0$, and that it has the (nonconvergent) series expansion $y_0(t) = \sum_{n \geqslant 0}(-1)^n n! t^n$.

(c) Consider the differential equation $t^2y' + (1+at)y + bty^2 - c = 0$, where a, b, and c are parameters. Prove that there is a unique solution of this equation which is C^∞ around $t = 0$ and that its value at $t = 0$ is equal to c.

(d) Let y_n be a the C^∞ function which is a solution of $t^2y'+(1+a_nt)y+b_nty^2-c_n = 0$. Prove that if we set $y_n = c_n/(1+ty_{n+1})$ then y_{n+1} is the C^∞ function that is a solution of $t^2y' + (1+a_{n+1}t)y + b_{n+1}ty^2 - c_{n+1} = 0$ with $a_{n+1} = 1 - a_n$, $b_{n+1} = 1$, and $c_{n+1} = a_n + b_nc_n$.

(e) By proving the convergence of the continued fraction, deduce that

$$E_1(x) = \cfrac{e^{-x}}{x + \cfrac{1}{1 + \cfrac{1}{x + \cfrac{2}{1 + \cfrac{2}{x + \ddots}}}}} .$$

(f) By contracting this fraction, deduce finally that

$$E_1(x) = \Gamma_1(1,x) = \cfrac{e^{-x}}{x + 1 - \cfrac{1^2}{x + 3 - \cfrac{2^2}{x + 5 - \cfrac{3^2}{x + 7 - \ddots}}}} .$$

20. (Continuation of the preceding exercise.)

(a) Denote by p_n/q_n the nth convergent of the continued fraction for $E_1(x)$ obtained at the end of the preceding exercises (so that $p_0 = 0$, $p_1 = e^{-x}$, $q_0 = 1$, $q_1 = x + 1$). Show by induction that

$$q_n = \sum_{j=0}^{n} \binom{n}{j}^2 (n-j)!x^j .$$

(b) Show that the largest summand in this sum is obtained for j_0 equal to one of the two integers closest to

$$j_0 = -1 - x/2 + \sqrt{nx + x + x^2/4} ,$$

and using Stirling's formula show that as $n \to \infty$ this summand is asymptotic to

$$\frac{n!e^{2\sqrt{nx}}e^{-x/2}}{2\pi\sqrt{nx}} .$$

(c) By setting $j = j_0 + \lambda n^{1/4}$ and approximating the sum by an integral, show that as $n \to \infty$ we have

$$q_n \sim \frac{n!e^{2\sqrt{nx}}e^{-x/2}}{2\sqrt{\pi}(nx)^{1/4}} \quad \text{and} \quad p_n \sim \frac{n!e^{2\sqrt{nx}}e^{x/2}E_1(x)}{2\sqrt{\pi}(nx)^{1/4}} .$$

(d) Deduce that

$$E_1(x) - \frac{p_n}{q_n} \sim 2\pi e^{-4\sqrt{nx}} .$$

21. Prove completely similar results to those of Exercises 19 and 20 for the incomplete gamma function $\Gamma(s,x) = \int_x^\infty e^{-t}t^{s-1}\,dt$. In particular, show that

$$\Gamma(s,x) = \cfrac{x^s e^{-x}}{x+1-s-\cfrac{1(1-s)}{x+3-s-\cfrac{2(2-s)}{x+5-s-\ddots}}}$$

and that if p_n/q_n is the nth convergent of this continued fraction, then as $n \to \infty$ we have

$$\Gamma(s,x) - \frac{p_n}{q_n} \sim \frac{2\pi}{\Gamma(1-s)} e^{-4\sqrt{nx}}$$

(when $s \in \mathbb{Z}_{\geqslant 1}$ this means that the left hand side is equal to 0, due to the fact that the continued fraction terminates).

22. Assume that E is an elliptic curve defined over $\mathbb{Q}$ of rank 1 and that one knows a point of infinite order in $E(\mathbb{Q})$. Explain how to find a generator for the torsionfree part of $E(\mathbb{Q})$.

23. Prove Proposition 8.6.2.

24. Prove Proposition 8.6.6.

25. (Atkin–Lehner.) Let $N \geqslant 1$ be an integer, and let Q be a (positive) divisor of N such that $\gcd(Q, N/Q) = 1$.

(a) Prove that there exist x, y, z, and w in $\mathbb{Z}$ such that if we set

$$W_Q = \begin{pmatrix} Qx & y \\ Nz & Qw \end{pmatrix},$$

then $\det(W_Q) = Q$. Such a matrix W_Q will be called an Atkin–Lehner matrix for the divisor Q of N.

(b) Prove that W_Q is unique up to left multiplication by an element of $\Gamma_0(N)$, in other words that if $\gamma \in \Gamma_0(N)$ then γW_Q is again an Atkin–Lehner matrix for Q, and conversely that if W_Q and W'_Q are two such matrices there exists $\gamma \in \Gamma_0(N)$ such that $W'_Q = \gamma W_Q$.

(c) Prove that $W_Q^2 = Q\gamma$ for some $\gamma \in \Gamma_0(N)$, hence that the action of W_Q via linear fractional transformations is an *involution* on $\Gamma_0(N)$-invariant functions.

26. (Continuation of the previous exercise.) Let τ be a Heegner point of level N, and let $(A,B,C) = 0$ be the corresponding primitive positive definite quadratic form, hence by Proposition 8.6.3 such that $N \mid A$ and $\gcd(A/N, B, CN) = 1$ (or $\gcd(N, B, AC/N) = 1$). Let $W_Q = \left(\begin{smallmatrix} Qx & y \\ Nz & Qw \end{smallmatrix}\right)$ be an Atkin–Lehner matrix corresponding to some $Q \mid N$ such that $\gcd(Q, N/Q) = 1$. We set $\tau_1 = (Qx\tau + y)/(Nz\tau + Qw)$, which we write as $\tau_1 = W_Q(\tau)$, and let (A_1, B_1, C_1) be the corresponding primitive quadratic form.

(a) Compute explicitly A_1, B_1, and C_1 in terms of A, B, and C (and of course of the matrix W_Q), and conversely compute explicitly A, B, and C in terms of A_1, B_1, and C_1 (hint: this second computation is immediate from the first).

(b) It is immediately seen from the formulas that $N \mid A_1$, so the first condition for a Heegner point of level N is satisfied. Using $\gcd(A/N, B.CN) = 1$, prove that if p is a prime such that $p \mid N/Q$ then $p \nmid \gcd(A_1/N, B_1, C_1 N)$.

(c) Using now $\gcd(N, B, AC/N) = 1$, prove that if p is a prime such that $p \mid Q$ then again $p \nmid \gcd(A_1/N, B_1, C_1 N)$, so that $\tau_1 = W_Q(\tau)$ is a Heegner point of level N.

27. Compute all the integral points on the elliptic curves $y^2 = x^3 + t$ for $t = -26$, -29, -38, -39, -53, -59, -61, -83, -89, and $t = 17$, which are needed for Theorem 6.7.14 and Exercise 34 of Chapter 6. For instance, first show that a basis of the Mordell–Weil group is given by $(P, Q) = ((5, 6), (153/4, 1891/8))$ for $t = -89$, $(P, Q) = ((4, 5), (10, 31))$ for $t = -39$, and $(P, Q) = ((-2, 3), (4, 9))$ for $t = 17$, and proceed similarly for the other values of t.
28. The reader may have noticed that not only the denominator, but also the numerator of the x-coordinate found in the example of Section 8.6.5 is the square of an integer. Explain and generalize this phenomenon.
29. Compute a rational point on the elliptic curve $y^2 = x^3 - 157^2 x$ considered in Section 8.6.5, but now using the 2-descent method (hint: cheat and start from the point found in the text to see on which quartics to look, and at what height).
30. Using the Heegner point method, compute rational numbers u and v such that $u^3 + v^3 = 697$. For this, first show that the minimal Weierstrass model of the corresponding elliptic curve is $y^2 + y = x^3 - 3279211$. You will have to perform all the subsequent computations with reasonably small accuracy (66 to 75 decimal digits), but you will need several hundred million coefficients of the L-series, so these will have to be computed on the fly. The smallest denominators for u and v have 50 decimal digits.
31. (Bremner–Cassels [Bre-Cas].) Using the Heegner point method, find a nontorsion rational point on the elliptic curve $y^2 = x(x^2 + 877)$ (again, this is a large computation).
32. Let Q be the matrix of a positive definite quadratic form, and let λ be its smallest eigenvalue. By diagonalizing Q on an orthonormal basis of eigenvectors, show that $X^t Q X \geqslant \lambda X^t X$.
33. Prove that there are exactly 20 integral points on the elliptic curve with equation $y^2 + y = x^3 + x^2 - 2x$ (this is the curve of rank 2 having smallest conductor, equal to 389).

14. The Super-Fermat Equation

14.1 Preliminary Reductions

The general super-Fermat equation is the equation $Ax^p + By^q + Cz^r = 0$ for given nonzero integers A, B, C and integral exponents p, q and r greater or equal to 2 (otherwise the equation would have little interest). The number of integers less than or equal to some large X of the form Ax^p is $O(X^{1/p})$, and similarly for By^q and Cz^r. Thus, to be able to obtain 0 as a sum of such quantities by something else than pure accident, it is reasonable to believe that we must have $X \leqslant O(X^{1/p+1/q+1/r})$, in other words $1/p+1/q+1/r \geqslant 1$. Thus, we *expect* (of course we have no proof) that when $1/p+1/q+1/r < 1$ (the so-called *hyperbolic case*), we will have only finitely many solutions. On the other hand, when $1/p + 1/q + 1/r > 1$ (the so-called *elliptic case* or *spherical case*), we expect an infinity of solutions. Finally, we cannot say anything for the moment about the intermediate case $1/p + 1/q + 1/r = 1$ (the so-called *parabolic case*).

This heuristic reasoning is almost correct, but not quite. Indeed, I claim that for many triples (p, q, r) it is easy to construct an infinite number of "nontrivial" solutions. Assume for instance that $A = B = 1$ and $C = -1$ and that (p, q, r) are pairwise coprime. Let a and b be integers strictly greater than 1, and set $c = a + b$. Multiplying this equation by $a^{uqr}b^{vpr}c^{wpq}$ for some integers u, v and w we obtain

$$a^{uqr+1}b^{vpr}c^{wpq} + a^{uqr}b^{vpr+1}c^{wpq} = a^{uqr}b^{vpr}c^{wpq+1} .$$

This is a "nontrivial" solution to our equation if we choose $u \equiv (qr)^{-1} \pmod{p}$, $v \equiv (pr)^{-1} \pmod{q}$ and $w \equiv (pq)^{-1} \pmod{r}$. Therefore it is necessary to add a further condition to exclude this type of solutions, and the natural choice is to ask that x, y and z be pairwise coprime. With that additional restriction, our heuristic reasoning is correct.

A second reduction can be made most of the time. Assume that two among p, q and r are coprime. Without loss of generality, assume for example that $\gcd(p, q) = 1$. There exist unique positive integers u and v such that that $up - vq = 1$ and $1 \leqslant u \leqslant p$, $1 \leqslant v \leqslant q$. Multiplying our equation by $A^{vq}B^{pq-up}$ gives the equation $x_1^p + y_1^q + C_1 z^r = 0$ with $x_1 = (AB)^u x$, $y_1 = A^v B^{p-v} y$ and $C_1 = A^{vq}B^{pq-up}C$. We may thus in that case assume that $A = B = 1$.

Note, however, that the coprimality of the solutions may be destroyed by this transformation.

In this chapter, we will in fact often consider the case $A = B = 1$ and $C = \pm 1$. It is easy to see that we can then reduce to the case $C = -1$: indeed, if $C = 1$ and if $x^p + y^q + z^r = 0$, then if p, q and r are all three even it is clear by positivity that there are no nontrivial solutions, or else at least one of them, say r, is odd, and then the equation can be written $x^p + y^q - (-z)^r = 0$, thus with $C = -1$. Therefore we will consider mainly the equations $x^p + y^q = z^r$, as usual with $\gcd(x, y) = 1$.

Finally, given a triple (p, q, r) up to permutation, if we want to fix the right hand side, say z^r, then we must consider the 4 equations $-x^p - y^q = z^r$, $x^p - y^q = z^r$, $-x^p + y^q = z^r$ and $x^p + y^q = z^r$. If p (resp., q, resp., r) is odd, we may change x into $-x$ (resp., y into $-y$, resp., z into $-z$). Then it is easily seen by examination of cases that we can reduce to the examination of a smaller number of equations. More precisely, if at least two of p, q and r are odd, it is sufficient to consider the equation $x^p + y^q = z^r$; if exactly one is odd, we must in addition consider the equation $x^p - y^q = z^r$ if p or r is odd, and the equation $-x^p + y^q = z^r$ if q is odd. Finally, if p, q and r are even, we must consider the three equations $x^p + y^q = z^r$, $x^p - y^q = z^r$ and $-x^p + y^q = z^r$, except if $p = q$ in which case it is enough to consider the first two.

We will begin by considering the elliptic case. Up to permutation of (p, q, r), this corresponds to the cases $(p, q, r) = (2, 2, r)$ for $r \geqslant 2$, $(2, 3, 3)$, $(2, 3, 4)$, $(2, 3, 5)$, which for reasons which will be seen below can be called the dihedral, tetrahedral, octahedral and icosahedral cases respectively.

14.2 The Dihedral Cases $(2, 2, r)$

This case is the simplest. We must consider the two equations $x^2 - y^2 = z^r$ and $x^2 + y^2 = z^r$.

14.2.1 The Equation $x^2 - y^2 = z^r$

We set $a = x + y$, $b = x - y$, so that $ab = z^r$. Since x and y are coprime, there are two cases. Either $x \not\equiv y \pmod 2$, in which case a and b are coprime and z is odd, hence $a = \pm s_1^r$, $b = \pm t_1^r$ for coprime odd integers s_1 and t_1, so that $x = \pm(s_1^r + t_1^r)/2$, $y = \pm(s_1^r - t_1^r)/2$ and $z = s_1 t_1$ (and also $-s_1 t_1$ if r is even). If we insist in not having denominators, we set $s = (s_1 + t_1)/2$, $t = (s_1 - t_1)/2$ which are coprime integers of different parity, hence we obtain the parametrization

$$(x, y, z) = (\pm((s+t)^r + (s-t)^r)/2, \pm((s+t)^r - (s-t)^r)/2, s^2 - t^2)$$

(and also $z = t^2 - s^2$ if r is even). Note that here we can either insist that the $\pm$ signs are the same (this is how they have been obtained), or that they are independent, since a change of t in $-t$ changes only y into $-y$.

Or else $x \equiv y \equiv 1 \pmod 2$, in which case a and b are even but $a/2$ and $b/2$ are coprime of opposite parity. Changing y into $-y$ if necessary, we may therefore assume that $a/2$ is even and $b/2$ is odd. Since $(a/2)(b/2) = 2^{r-2}(z/2)^r$, we have $a = \pm 2^{r-1}s^r$, $b = \pm 2t^r$ for coprime integers s and t with t odd if $r \geqslant 3$, $t \not\equiv s \pmod 2$ if $r = 2$, so that we obtain

$$(x, y, z) = (\pm(2^{r-2}s^r + t^r), \pm(2^{r-2}s^r - t^r), 2st)$$

(and also $z = -2st$ if r is even).

We thus obtain the following special cases, where we always assume that s and t are coprime, plus indicated additional conditions modulo 2. Often the additional sign of x, y or z when r is even can be absorbed by changing s into $-s$, t into $-t$ or by exchanging s and t.

$r = 2$: $(x, y, z) = (\pm(s^2 + t^2), 2ts, (s - t)(s + t))$, where $s \not\equiv t \pmod 2$, up to exchange of y and z.

$r = 3$: $(x, y, z) = (s(s^2 + 3t^2), t(3s^2 + t^2), (s - t)(s + t))$, where $s \not\equiv t \pmod 2$, or $(x, y, z) = (\pm(2s^3 + t^3), 2s^3 - t^3, 2ts)$, where $2 \nmid t$.

$r = 4$: $(x, y, z) = (\pm(s^4 + 6t^2s^2 + t^4), 4ts(s^2 + t^2), (s - t)(s + t))$, where $s \not\equiv t \pmod 2$, or $(x, y, z) = (\pm(2s^2 - 2st + t^2)(2s^2 + 2st + t^2), \pm(2s^2 - t^2)(2s^2 + t^2), 2ts)$, where $2 \nmid t$.

$r = 5$: $(x, y, z) = (s(s^4 + 10t^2s^2 + 5t^4), t(5s^4 + 10t^2s^2 + t^4), (s - t)(s + t))$, where $s \not\equiv t \pmod 2$, or $(x, y, z) = (\pm(8s^5 + t^5), 8s^5 - t^5, 2ts)$, where $2 \nmid t$.

14.2.2 The Equation $x^2 + y^2 = z^r$

Here we set $a = x + iy$, $b = x - iy$ so that $ab = z^r$. If we had $x \equiv y \equiv 1 \pmod 2$, we would have $z^r \equiv 2 \pmod 8$, which is impossible since $r \geqslant 2$. Thus since x and y are coprime, x and y have opposite parity and a and b are coprime in the principal ideal domain $\mathbb{Z}[i]$. It follows that there exist $\alpha = s + it \in \mathbb{Z}[i]$ and some $v = 0$, 1, 2, or 3 such that $x + iy = i^v\alpha^r$, hence $x - iy = i^{-v}\overline{\alpha}^r$, $z = \alpha\overline{\alpha}$ (and also $z = -\alpha\overline{\alpha}$ if r is even). Clearly multiplication by i^v corresponds to changing signs of x and/or y and exchange of x and y, so that up to exchange of x and y we obtain the parametrization

$$\begin{cases} x &= \pm\sum_{0 \leqslant k \leqslant \lfloor r/2 \rfloor} (-1)^k \binom{r}{2k} t^{2k} s^{r-2k} \\ y &= \pm\sum_{0 \leqslant k \leqslant \lfloor (r-1)/2 \rfloor} (-1)^k \binom{r}{2k+1} t^{2k+1} s^{r-2k-1} \\ z &= s^2 + t^2 \quad \text{(and also } -(s^2 + t^2) \text{ if } r \text{ is even).} \end{cases}$$

Furthermore, the condition $\gcd(x, y) = 1$ of course implies that s and t are coprime, and since $r \geqslant 2$, if s and t were both odd we would have $\alpha^r \equiv$

$(1+i)^r \equiv 0 \pmod{2\mathbb{Z}[i]}$, so that x and y would both be even. It follows that in addition s and t have opposite parity. Conversely, it is easy to see that if this is the case then x and y are coprime.

We thus obtain the following special cases, where we assume that s and t are coprime of opposite parity. Again the additional sign of x, y or z when r is even, or the exchange of x and y can be absorbed by changing s into $-s$, t into $-t$ or by exchanging s and t, or a combination.

$r = 2$: $(x, y, z) = (2ts, s^2 - t^2, \pm(s^2 + t^2))$, up to exchange of x and y.

$r = 3$: $(x, y, z) = (s(s^2 - 3t^2), t(3s^2 - t^2), s^2 + t^2)$.

$r = 4$: $(x, y, z) = (\pm(s^2-2st-t^2)(s^2+2st-t^2), 4ts(s-t)(s+t), \pm(s^2+t^2))$, up to exchange of x and y.

$r = 5$: $(x, y, z) = (s(s^4 - 10t^2s^2 + 5t^4), t(5s^4 - 10t^2s^2 + t^4), s^2 + t^2)$.

14.2.3 The Equations $x^2 + 3y^2 = z^3$ and $x^2 + 3y^2 = 4z^3$

As additional examples of dihedral equations we prove the following:

Proposition 14.2.1. (1) *The equation $x^2 + 3y^2 = z^3$ in nonzero integers x, y and z with x and y coprime can be parametrized by*

$$(x, y, z) = (s(s - 3t)(s + 3t), 3t(s - t)(s + t), s^2 + 3t^2) ,$$

where s and t denote coprime integers of opposite parity such that $3 \nmid t$.

(2) *The equation $x^2 + 3y^2 = 4z^3$ in nonzero integers x, y and z with x and y coprime has the two disjoint parametrizations*

$$(x, y, z) = ((s + t)(s - 2t)(2s - t), 3st(s - t), s^2 - st + t^2) ,$$
$$(x, y, z) = (\pm(s^3 + 3s^2t - 6st^2 + t^3), s^3 - 3s^2t + t^3, s^2 - st + t^2) ,$$

where in both cases s and t are coprime integers such that $3 \nmid s + t$. The first parametrization corresponds to the case where $6 \mid y$, and the second to the case where y is coprime to 6.

Proof. For (1) we set $x_1 = x+3y$ and the equation becomes $x_1^2 - 3x_1(2y) + 3(2y)^2 = z^3$. Thanks to Proposition 6.4.4 of Chapter 6 we know that this equation has three disjoint parametrizations. Among these only the first gives an even value for the second variable, hence $x_1 = s^3 + 3s^2t - 6st^2 + t^3$, $y = 3st(s-t)/2$, and $z = s^2 - st + t^2$. If s is even we set $S = t - s/2$, $T = s/2$, if t is even we set $S = s - t/2$, $T = t/2$, and if s and t are both odd we set $S = (s + t)/2$ and $T = (s - t)/2$. In all three cases we check that up to sign we obtain the given parametrizations and the conditions at the primes 2 and 3.

For (2) we note that x and y are both odd, so we set $x_1 = (x + 3y)/2$, and the equation is $x_1^2 - 3x_1y + 3y^2 = z^3$. By Proposition 6.4.4 once again we

obtain three parametrizations, but it is immediate that (up to the sign of x which does not matter) the last two are interchanged by exchanging s and t, so we have only the two parametrizations given above. Note that because of this sign change in the interchange of the last two parametrizations we have to add a $\pm$ sign for the parametrization of x. □

Note that by looking modulo 8 it is clear that the equation $x^2+3y^2=2z^3$ is impossible in coprime x, y.

14.3 The Tetrahedral Case $(2,3,3)$

14.3.1 The Equation $x^3+y^3=z^2$

Thanks to the reductions made above, for $(p,q,r)=(2,3,3)$ it is sufficient to consider the single equation $x^3+y^3=z^2$. We will imitate what we did in the case of FLT, by factoring x^3+y^3 in $\mathbb{Z}[\zeta]$, where ζ is a primitive cube root of unity. Thus, we write

$$(x+y)(x+\zeta y)(x+\zeta^2 y)=z^2\ .$$

Case 1: $3\nmid z$

If $\pi\in\mathbb{Z}[\zeta]$ is a prime element which divides two distinct factors on the left, then $\pi\mid 1-\zeta$, hence $\pi=1-\zeta$, which is excluded since $3\nmid z$. Thus the factors are coprime in $\mathbb{Z}[\zeta]$, and each one is equal to a unit multiplied by a square. If we had factored directly in $\mathbb{Z}$, we would have obtained that $x+y=\pm a^2$ for $a\in\mathbb{Z}$, and since the cofactor x^2-xy+y^2 is always positive and $z^2>0$, we necessarily have $x+y=a^2$. Thus our equation implies that $x+y=a^2$ with $a\in\mathbb{Z}$ and $x+\zeta y=(-\zeta)^k\alpha^2$ for some integer k, and conversely this implies also $x+\zeta^2 y=(-\zeta^2)^k\overline{\alpha}^2$, hence $z=\pm a\alpha\overline{\alpha}$. In addition, since $\zeta=\zeta^4$ is a square, we may write $(-\zeta)^k\alpha^2=(-1)^k(\alpha\zeta^{2k})^2$. Thus finally our equation is thus equivalent to the equations $x+y=a^2$, $x+\zeta y=\varepsilon\alpha^2$, $z=\pm a\alpha\overline{\alpha}$, where $a\in\mathbb{Z}$, $\alpha\in\mathbb{Z}[\zeta]$ and $\varepsilon=\pm1$.

If we set $\beta=\zeta^2\alpha$ then

$$\beta^2+\overline{\beta}^2=\zeta\alpha^2+\zeta^2\overline{\alpha}^2=\varepsilon(\zeta(x+\zeta y)+\zeta^2(x+\zeta^2 y))=\varepsilon(-x-y)=-\varepsilon a^2\ .$$

Conversely, if $\beta\in\mathbb{Z}[\zeta]$ satisfies $\beta^2+\overline{\beta}^2=-\varepsilon a^2$ and if we set $\alpha=\zeta\beta$, then one checks that

$$\frac{\varepsilon\overline{\alpha}^2-a^2}{\varepsilon\alpha^2-a^2}=-\zeta^2=\frac{\overline{\zeta}-1}{\zeta-1}$$

so that $y=(\varepsilon\alpha^2-a^2)/(\zeta-1)\in\mathbb{Q}$. However $3\nmid a$, so that $a^2\equiv 1\pmod 3$, and also $(1-\zeta)\nmid\beta$ so that $\alpha^2\equiv\pm\varepsilon\pmod{1-\zeta}$. However if $\alpha^2\equiv-\varepsilon\pmod{1-\zeta}$, we would have $-a^2\equiv\varepsilon(-\varepsilon)(\zeta+\zeta^2)\equiv 1\pmod{1-\zeta}$, which is

absurd. Thus $\alpha^2 \equiv \varepsilon \pmod{1-\zeta}$, hence in fact $y \in \mathbb{Z}$. Thus our equation is now equivalent to the single simpler equation $a^2 = -\varepsilon(\beta^2 + \overline{\beta}^2)$. If we write $\beta = u + v\zeta$ with u and v in $\mathbb{Z}$, this gives finally the equation

$$a^2 = \varepsilon(v^2 + 2uv - 2u^2) \ .$$

Note that the condition $\gcd(x,y) = 1$ implies that a and β are coprime in $\mathbb{Z}[\zeta]$, hence that $\gcd(u,v) = 1$. Note also for future reference that this implies that $u+v$ and a are coprime (easy exercise left to the reader). Also since we are in the case $3 \nmid z$, we have $3 \nmid a$ hence $3 \nmid u+v$. Thus

$$1 \equiv a^2 \equiv \varepsilon((u+v)^2 - 3u^2) \equiv \varepsilon(u+v)^2 \equiv \varepsilon \pmod{3} \ ,$$

so that we must have $\varepsilon = 1$.

We have thus reduced our problem to the solution of a Diophantine equation of degree 2, for which an algorithmic solution is always possible.

We can do one more important reduction. It is clear that exchanging x and y is equivalent to changing β into $\overline{\beta}$, or in other words the pair (u,v) into the pair $(u-v,-v)$. Note that $v \equiv a \pmod 2$. Thus, if a is odd, v is odd, so either u or $u-v$ is odd. If a is even, then v is even, hence u is odd since it is coprime to v. Thus in all cases we may assume, possibly after exchanging x and y, that $u + v \not\equiv a \pmod 2$.

We write $3u^2 = (u+v)^2 - a^2 = (u+v-a)(u+v+a)$. Since $3 \nmid a$ and $3 \nmid (u+v)$, if necessary by changing β into $-\beta$ (or a into $-a$) we may assume that $3 \mid u+v-a$, and then $3 \nmid u+v+a$. Since $u+v$ and a are coprime, and since we have reduced above to the case where they do not have the same parity, it follows that $u+v-a$ and $u+v+a$ are coprime. Thus $u+v-a = 3\varepsilon_1 s_1^2$, $u+v+a = \varepsilon_1 t_1^2$, hence $u = \varepsilon_2 s_1 t_1$ with s_1 and t_1 coprime and odd and with $\varepsilon_1 = \pm 1$ and $\varepsilon_2 = \pm 1$. If we change simultaneously u, v and a into their opposites, we may assume that $\varepsilon_1 = 1$. Changing s_1 into $-s_1$ we may also assume that $\varepsilon_2 = 1$. Finally we set $s = s_1$, $t = (t_1 - s_1)/2$, which are coprime with s odd, which gives $u = s(s+2t)$, $v = s^2 + 2t^2$, $a = -s^2 + 2st + 2t^2$). The condition $3 \nmid u+v$ (or $3 \mid a$) is equivalent to $3 \nmid (s^2 + st + t^2)$, hence (since s and t are coprime) to $s \not\equiv t \pmod 3$. Replacing everywhere gives the first parametrization

$$\begin{cases} x = s(s+2t)(s^2 - 2ts + 4t^2) \\ y = -4t(s-t)(s^2 + ts + t^2) \\ z = \pm(s^2 - 2ts - 2t^2)(s^4 + 2ts^3 + 6t^2s^2 - 4t^3s + 4t^4) \ , \end{cases}$$

where s is odd and $s \not\equiv t \pmod 3$, up to exchange of x and y.

Note that if we had $s \equiv t \pmod 3$ we would have $3 \mid \gcd(x,y)$, contrary to our assumption. Note also that if we had not done the reduction equivalent to exchanging x and y, we would have obtained a second parametrization, which would have been equivalent to the first one where x and y are exchanged.

Case 2: $3 \mid z$

In this case $x+y$, $x+\zeta y$ and $x+\zeta^2 y$ are all three divisible by $1-\zeta$, and their quotient by $1-\zeta$ are pairwise coprime. Thus

$$\frac{x+y}{3}\frac{x+\zeta y}{1-\zeta}\frac{x+\zeta^2 y}{1-\zeta^2} = (z/3)^2$$

with the three factors on the left pairwise coprime, hence as above our equation is equivalent to $x+y = 3a^2$, $x+\zeta y = \varepsilon(1-\zeta)\alpha^2$, $z = \pm 3a\alpha\overline{\alpha}$, with $\varepsilon = \pm 1$. We note that since $3 \nmid xy$ (otherwise $3 \mid \gcd(x,y)$) then $v_{\mathfrak{p}}(x+\zeta y) = v_{\mathfrak{p}}(x+y+(\zeta-1)y) = 1$ where $\mathfrak{p} = (1-\zeta)\mathbb{Z}[\zeta]$, so that α is coprime to $1-\zeta$.

We have $(1-\zeta)y = 3a^2 - \varepsilon(1-\zeta)\alpha^2$, hence $y = (1-\zeta^2)a^2 - \varepsilon\alpha^2$, and since $y \in \mathbb{Q}$ we obtain $\alpha^2 - \overline{\alpha}^2 = \varepsilon a^2(\zeta - \zeta^2)$. Conversely, if this is satisfied for some $\alpha \in \mathbb{Z}[\zeta]$, then we can take $y = (1-\zeta^2)a^2 - \varepsilon\alpha^2 \in \mathbb{Z}$. Thus as before our equation is equivalent to the single simpler equation $a^2(\zeta - \zeta^2) = \varepsilon(\alpha^2 - \overline{\alpha}^2)$. If we write $\alpha = u + v\zeta$ with u and v in $\mathbb{Z}$, this gives finally the equation

$$a^2 = \varepsilon v(2u - v)\ .$$

We have already mentioned that α is coprime to $1-\zeta$, which is equivalent to $3 \nmid u+v$. In addition, the condition $\gcd(x,y) = 1$ implies that a and α are coprime in $\mathbb{Z}[\zeta]$, hence that $\gcd(u,v) = 1$. Thus the GCD of v and $2u-v$ is equal to 1 if v is odd, and to 2 if v is even.

It is easily seen that exchanging x and y is here equivalent to simultaneously changing α into $\overline{\alpha}$ and ε into $-\varepsilon$. Thus, we may assume that $\varepsilon = 1$. Thus we have two possibilities according to the parity of v.

• If v is odd, then $v = \varepsilon_1 s_1^2$, $2u - v = \varepsilon_1 t_1^2$, hence $a = \varepsilon_2 s_1 t_1$ with s_1 and t_1 odd and $\varepsilon_1 = \pm 1$. Changing α into $-\alpha$, we may assume that $\varepsilon_1 = 1$, and changing s_1 into $-s_1$ that $\varepsilon_2 = 1$. We set $s = (s_1+t_1)/2$, $t = (s_1-t_1)/2$ which are coprime integers of opposite parity, so that $v = (s+t)^2$, $u = s^2+t^2$, $a = s^2 - t^2$. The condition $3 \nmid u+v$ is again equivalent to $s \not\equiv t \pmod 3$. Replacing everywhere gives the second parametrization, where the sign of z can be absorbed by exchanging s and t.

$$\begin{cases} x = s^4 - 4ts^3 - 6t^2s^2 - 4t^3s + t^4 \\ y = 2(s^4 + 2ts^3 + 2t^3s + t^4) \\ z = 3(s-t)(s+t)(s^4 + 2s^3t + 6s^2t^2 + 2st^3 + t^4)\ , \end{cases}$$

where $s \not\equiv t \pmod 2$ and $s \not\equiv t \pmod 3$, up to exchange of x and y.

• If v is even, then $v = 2\varepsilon_1 s^2$, $2u - v = 2\varepsilon_1 t^2$, hence $u = \varepsilon_1(s^2+t^2)$ and $a = 2\varepsilon_2 st$, where s and t are coprime integers of opposite parity. As before, we may reduce to the case $\varepsilon_1 = \varepsilon_2 = 1$. The condition $3 \nmid u+v$ is now equivalent to $3 \nmid t$. Replacing everywhere gives the third and final parametrization, where the sign of z can be absorbed by changing s into $-s$.

$$\begin{cases} x = -3s^4 + 6t^2s^2 + t^4 \\ y = 3s^4 + 6t^2s^2 - t^4 \\ z = 6st(3s^4 + t^4) \ , \end{cases}$$

where $s \not\equiv t \pmod 2$ and $3 \nmid t$, up to exchange of x and y.

We have thus shown the following theorem.

Theorem 14.3.1. *The equation $x^3 + y^3 = z^2$ in integers x, y, z with $\gcd(x, y) = 1$ can be parametrized by one of the above three parametrizations, up to exchange of x and y, where s and t denote coprime integers satisfying the given congruences modulo 2 and 3. In addition these parametrizations are disjoint, in that any solution to our equation belongs to a single parametrization (up to exchange of x and y).*

14.3.2 The Equation $x^3 + y^3 = 2z^2$

This equation is very similar to the preceding one, and will be needed in the octahedral case. Thus we only give a brief sketch. We can factor $x^3 + y^3$ as usual, and we use the fact that 2 is inert in $\mathbb{Z}[\zeta]$. As usual we distinguish two cases.

Case 1: $3 \nmid z$

Using the same technique as above, it is easily seen that our equation is equivalent to the equations $x + y = 2a^2$, $z = \pm a\beta\overline{\beta}$, and $2a^2 = -(v^2 + 2uv - 2u^2)$, where $\beta = u + v\zeta$, and u and v are coprime. Thus $v = 2w$ must be even, hence u is odd so we obtain $(u - w - a)(u - w + a) = 3w^2$. It follows that $a^2 = (u-w)^2 - 3w^2 \equiv (1-w)^2 - 3w^2 \equiv 1 \pmod 2$, hence a is odd. Since $3 \mid a$ and $3 \nmid u + v \equiv u - w \pmod 3$, we may assume that $3 \mid (u - w - a)$. Thus, we have two different cases (where as usual we can get rid of the signs):

Case 1.1: $2 \nmid w$

Here $u - w - a = 3s_1^2$, $u - w + a = t_1^2$ with s_1 and t_1 odd and coprime, hence setting $s = s_1$, $t = (t_1 - s_1)/2$ coprime with s odd and with $s \not\equiv t \pmod 3$, we obtain $w = s(s + 2t)$, $a = -s^2 + 2st + 2t^2$, $u = 3s^2 + 4st + 2t^2$. Replacing gives the first parametrization, where the exchange of x and y can be absorbed by the exchange of s and t.

$$\begin{cases} x = -(s^2 + 4ts - 2t^2)(3s^2 + 4ts + 2t^2) \\ y = (s^2 + 2t^2)(5s^2 + 8ts + 2t^2) \\ z = \pm(s^2 - 2ts - 2t^2)(7s^4 + 20ts^3 + 24t^2s^2 + 8t^3s + 4t^4) \ , \end{cases}$$

where s is odd and $s \not\equiv t \pmod 3$.

Case 1.2: $2 \mid w$

Here $u - w - a = 6s^2$, $u - w + a = 2t^2$, $w = 2st$, hence $a = t^2 - 3s^2$, $u = 3s^2 + 2st + t^2$, and s and t are coprime integers of opposite parity with

$3 \nmid t$. Replacing gives the second parametrization, where the exchange of x and y can be absorbed by changing s into $-s$.

$$\begin{cases} x = (3s^2 - 6ts + t^2)(3s^2 + 2ts + t^2) \\ y = (3s^2 - 2ts + t^2)(3s^2 + 6ts + t^2) \\ z = \pm(3s^2 - t^2)(9s^4 + 18t^2s^2 + t^4) \ , \end{cases}$$

where $s \not\equiv t \pmod 2$ and $3 \nmid t$.

Case 2: $3 \mid z$

Using the same technique as above, it is easily seen that our equation is equivalent to the equations $x + y = 6a^2$, $z = \pm 3a\alpha\overline{\alpha}$, $y = 2(1-\zeta^2)a^2 - \varepsilon\alpha^2$, and $2a^2 = \varepsilon v(2u - v)$, where $\alpha = u + v\zeta$ and u and v are coprime, and α is coprime to $1-\zeta$. Thus $v = 2w$ must be even, hence u is odd so we obtain that a is even and $\varepsilon w(u - w)/2 = (a/2)^2$. Since exchanging x and y is equivalent to changing α into $\overline{\alpha}$ and ε into $-\varepsilon$, we may assume that $\varepsilon = 1$. Once again we have two cases, where as usual we can get rid of the signs.

Case 2.1: $2 \nmid w$

Here $w = s^2$, $u - w = 2t^2$, $a = 2st$, hence $u = s^2 + 2t^2$, $v = 2s^2$, where s and t are coprime with s odd. Replacing, we obtain the third parametrization

$$\begin{cases} x = -3s^4 + 12t^2s^2 + 4t^4 \\ y = 3s^4 + 12t^2s^2 - 4t^4 \\ z = 6ts(3s^4 + 4t^4) \ , \end{cases}$$

where s is odd and $3 \nmid t$, up to exchange of x and y.

Case 2.2: $2 \mid w$

Here $w = 2s^2$, $u - w = t^2$, $a = 2st$, hence $u = 2s^2 + t^2$, $v = 4s^2$, where s and t are coprime with t odd. Replacing, we obtain the fourth and final parametrization

$$\begin{cases} x = -12s^4 + 12t^2s^2 + t^4 \\ y = 12s^4 + 12t^2s^2 - t^4 \\ z = 6ts(12s^4 + t^4) \ , \end{cases}$$

where t is odd and $3 \nmid t$, up to exchange of x and y.

We have thus shown the following theorem.

Theorem 14.3.2. *The equation $x^3 + y^3 = 2z^2$ in integers x, y, z with $\gcd(x,y) = 1$ can be parametrized by one of the above four parametrizations, up to exchange of x and y, where s and t denote coprime integers with the indicated congruence conditions modulo 2 and 3. In addition these parametrizations are disjoint, in that any solution to our equation belongs to a single parametrization (up to exchange of x and y).*

14.3.3 The Equation $x^3 - 2y^3 = z^2$

We will also need this equation in the octahedral case. Note first that z is necessarily odd, otherwise x is even, hence y is even, contradiction. Similarly, it is easy to check that the congruence $x^3 - 2y^3 \equiv 0 \pmod 9$ implies that $x \equiv y \equiv 0 \pmod 3$, which is impossible. Thus we must have $3 \nmid z$, i.e., the "second case" does not occur.

We now work in the number field $K = \mathbb{Q}(\theta)$, where $\theta^3 = 2$, whose ring of integers is $\mathbb{Z}[\theta]$ and is a principal ideal domain. Note also that 3 is totally ramified in $\mathbb{Z}[\theta]$. Our equation is a *norm equation* of the type $\mathcal{N}(\alpha) = z^2$, for $\alpha = x - y\theta \in \mathbb{Z}[\theta]$. We factor our equation as $(x - y\theta)(x^2 + xy\theta + y^2\theta^2) = z^2$. Since $3 \nmid z$, as usual it is easily seen that the two factors on the left are coprime in $\mathbb{Z}[\theta]$, hence $x - y\theta = \pm\varepsilon^k\beta^2$ for $\varepsilon = \theta - 1$ the fundamental unit, and some $\beta \in \mathbb{Z}[\theta]$. We may of course assume that $k = 0$ or 1. Taking norms and using the fact that $\mathcal{N}(\varepsilon) = 1$ gives $z^2 = \pm\mathcal{N}(\beta)^2$, so that the sign must be $+$, and then $z = \pm\mathcal{N}(\beta)$. The only condition is thus that $\varepsilon^k\beta^2$ have no terms in θ^2. Writing $\beta = u + v\theta + w\theta^2$, we thus have two cases.

Case 1: $k = 0$

Then we obtain the equations $v^2 + 2uw = 0$, $x = u^2 + 4vw$, $y = -2(w^2 + uv)$, $z = \pm(u^3 + 2v^3 + 4w^3 - 6uvw)$. Thus $v = 2v_1$ is even, hence u is odd. Since x and y are coprime, so are u and w. Thus the equation $uw = -2v_1^2$ implies that $u = \varepsilon_1 s^2$, $w = -\varepsilon_1 2t^2$, $v = \varepsilon_2 2st$ for some ε_1 and ε_2 equal to ± 1, with s and t coprime and s odd. As usual changing if necessary β into $-\beta$, and s into $-s$, we may assume that $\varepsilon_1 = \varepsilon_2 = 1$. Replacing gives the first parametrization

$$\begin{cases} x = s(s^3 - 16t^3) \\ y = -4t(s^3 + 2t^3) \\ z = \pm(s^6 + 40t^3s^3 - 32t^6)\ , \end{cases}$$

where s is odd and $s \not\equiv t \pmod 3$.

Case 2: $k = 1$

Here we obtain the equations $(2v - 2w)u - v^2 + 2w^2 = 0$, $x = -u^2 + 4wu + 2v^2 - 4wv$, $y = -u^2 + 2vu - 4wv + 2w^2$. The first equation can be written $(u - w)^2 + w^2 = (v - u)^2$. Since $\gcd(u, v, w) = 1$, the solution to the Pythagorean triple equation gives the parametrizations $u - w = 2st$, $w = s^2 - t^2$, $v - u = \varepsilon_1(s^2 + t^2)$ or $w = 2st$, $u - w = s^2 - t^2$, $v - u = \varepsilon_1(s^2 + t^2)$ for $\varepsilon_1 = \pm 1$, where s and t are coprime integers of opposite parity. Since we can change β into $-\beta$, we may assume that $\varepsilon_1 = 1$. Replacing gives the following two further parametrizations:

$$\begin{cases} x = 3s^4 + 12ts^3 + 6t^2s^2 + 4t^3s + 3t^4 \\ y = -3s^4 + 6t^2s^2 + 8t^3s + t^4 \\ z = \pm(9s^6 + 18ts^5 + 45t^2s^4 + 60t^3s^3 + 15t^4s^2 - 6t^5s - 5t^6)\ , \end{cases}$$

where $s \not\equiv t \pmod 2$ and $3 \nmid t$.

$$\begin{cases} x = 7s^4 + 4ts^3 + 6t^2s^2 - 4t^3s - t^4 \\ y = 3s^4 - 8ts^3 - 6t^2s^2 - t^4 \\ z = \pm(17s^6 + 30ts^5 - 15t^2s^4 + 20t^3s^3 + 15t^4s^2 + 6t^5s - t^6)\,, \end{cases}$$

where $s \not\equiv t \pmod 2$ and $s \not\equiv t \pmod 3$.

We have thus shown the following theorem:

Theorem 14.3.3. *The equation $x^3 - 2y^3 = z^2$ in integers x, y, z with $\gcd(x,y) = 1$ can be parametrized by one of the above three parametrizations, where s and t denote coprime integers with the indicated congruence conditions modulo 2 and 3. In addition these parametrizations are disjoint, in that any solution to our equation belongs to a single parametrization.*

14.4 The Octahedral Case $(2,3,4)$

According to the reductions made above, this case reduces to the two equations $x^2 \pm y^4 = z^3$. We consider both separately.

14.4.1 The Equation $x^2 - y^4 = z^3$

Factoring gives $(x-y^2)(x+y^2) = z^3$. Since x and y are coprime, either $x-y^2$ and $x+y^2$ are coprime, or x and y are odd and $(x-y^2)/2$ and $(x+y^2)/2$ are coprime.

Case 1: $2 \nmid z$

Here $x-y^2$ and $x+y^2$ are coprime, so that $x-y^2 = a^3$, $x+y^2 = b^3$, $z = ab$ (the possible sign can be removed by changing the sign of a). This is equivalent to $x = y^2 + a^3$, $z = ab$ and $2y^2 + a^3 = b^3$. Changing variable names, we are thus reduced to the equation $x^3 + y^3 = 2z^2$ with x and y odd, which we have studied above. Note that the exchange of x and y in this latter equation is equivalent to the exchange of b with $-a$, hence to the exchange of x with $-x$ in our initial equation. Thus after replacing we obtain the following four different parametrizations of our equation, where in each case s and t are coprime integers satisfying the indicated additional congruence conditions modulo 2 and 3.

$$\begin{cases} x = 4s(s+2t)(s^2+ts+t^2)(s^4+4ts^3+16t^2s^2+24t^3s+12t^4) \\ \qquad\qquad (19s^4 - 4ts^3 + 8t^3s + 4t^4) \\ y = \pm(s^2-2ts-2t^2)(7s^4+20ts^3+24t^2s^2+8t^3s+4t^4) \\ z = (s^2+2t^2)(s^2+4ts-2t^2)(3s^2+4ts+2t^2)(5s^2+8ts+2t^2)\,, \end{cases}$$

where s is odd and $s \not\equiv t \pmod 3$.

Note that changing t into $-s-t$ changes x into $-x$, hence we do not need to put a $\pm$ sign in front of x.

$$\begin{cases} x = 4ts(3s^2+t^2)(3s^4-2t^2s^2+3t^4)(81s^4-6t^2s^2+t^4) \\ y = \pm(3s^2-t^2)(9s^4+18t^2s^2+t^4) \\ z = -(3s^2-6ts+t^2)(3s^2-2ts+t^2)(3s^2+2ts+t^2)(3s^2+6ts+t^2)\ , \end{cases}$$

where $s \not\equiv t \pmod 2$ and $3 \nmid t$.

$$\begin{cases} x = \pm(3s^4-4t^4)(9s^8+408t^4s^4+16t^8) \\ y = 6ts(3s^4+4t^4) \\ z = (3s^4-12t^2s^2-4t^4)(3s^4+12t^2s^2-4t^4)\ , \end{cases}$$

where s is odd and $3 \nmid t$.

$$\begin{cases} x = \pm(12s^4-t^4)(144s^8+408t^4s^4+t^8) \\ y = 6ts(12s^4+t^4) \\ z = (12s^4-12t^2s^2-t^4)(12s^4+12t^2s^2-t^4)\ , \end{cases}$$

where t is odd and $3 \nmid t$.

Note that the exchange of x and y in the parametrizations of $x^3+y^3=2z^3$ correspond only to the exchange of x and $-x$ in the present ones.

Case 2: $2 \mid z$

Here we must have $2 \mid ((x-y^2)/2)(x+y^2)/2$, so that changing x into $-x$ if necessary, we may assume that $4 \mid x-y^2$. It follows that $x-y^2=4a^3$, $x+y^2=2b^3$, $z=2ab$. This is equivalent to $x=y^2+4a^3$, $z=2ab$ and $y^2+2a^3=b^3$, with y odd. We are thus reduced to the equation $x^3-2y^3=z^2$, which we have studied above. We thus obtain three parametrizations, which after replacing gives the following three additional parametrizations of our equation, for a total of seven:

$$\begin{cases} x = \pm(s^6-176t^3s^3-32t^6)(s^6+32t^6) \\ y = \pm(s^6+40t^3s^3-32t^6) \\ z = -8ts(s^3-16t^3)(s^3+2t^3)\ , \end{cases}$$

where s is odd and $s \not\equiv t \pmod 3$.

$$\begin{cases} x = \pm(-27s^{12}+324ts^{11}+1782t^2s^{10}+3564t^3s^9+3267t^4s^8 \\ \qquad +2376t^5s^7+2772t^6s^6+3960t^7s^5+4059t^8s^4 \\ \qquad +2420t^9s^3+726t^{10}s^2+156t^{11}s+29t^{12}) \\ y = \pm(9s^6+18ts^5+45t^2s^4+60t^3s^3+15t^4s^2-6t^5s-5t^6) \\ z = -2(3s^4-6t^2s^2-8t^3s-t^4)(3s^4+12ts^3+6t^2s^2+4t^3s+3t^4)\ , \end{cases}$$

where $s \not\equiv t \pmod 2$ and $3 \nmid t$.

$$\begin{cases} x = \pm(397s^{12} + 156ts^{11} + 2046t^2s^{10} + 1188t^3s^9 - 1485t^4s^8 - 2376t^5s^7 \\ \qquad - 924t^6s^6 - 792t^7s^5 + 99t^8s^4 + 44t^9s^3 - 66t^{10}s^2 - 12t^{11}s - 3t^{12}) \\ y = \pm(17s^6 + 30ts^5 - 15t^2s^4 + 20t^3s^3 + 15t^4s^2 + 6t^5s - t^6) \\ z = 2(3s^4 - 8ts^3 - 6t^2s^2 - t^4)(7s^4 + 4ts^3 + 6t^2s^2 - 4t^3s - t^4)\ , \end{cases}$$

where $s \not\equiv t \pmod 2$ and $s \not\equiv t \pmod 3$.

Remark. We could have used the parametrizations of the dihedral equation $x^2 - y^2 = z^3$, but it would not have been really simpler. The same is true for the next equation.

We have thus shown the following theorem:

Theorem 14.4.1. *The equation $x^2 - y^4 = z^3$ in integers x, y, z with $\gcd(x,y) = 1$ can be parametrized by one of the above seven parametrizations, where s and t denote coprime integers with the indicated congruence conditions modulo 2 and 3. In addition these parametrizations are disjoint, in that any solution to our equation belongs to a single parametrization.*

14.4.2 The Equation $x^2 + y^4 = z^3$

We note that here we cannot have x and y both odd, otherwise $z^3 \equiv 2 \pmod 8$, absurd. We work in $\mathbb{Z}[i]$ and factor the equation as $(x + iy^2)(x - iy^2) = z^3$. Since x and y are coprime and not both odd, $x + iy^2$ and $x - iy^2$ are coprime in $\mathbb{Z}[i]$. Thus there exists $\alpha \in \mathbb{Z}[i]$ such that $x + iy^2 = \alpha^3$, hence $x - iy^2 = \overline{\alpha}^3$, $z = \alpha\overline{\alpha}$, where the possible power of i can be absorbed in α. We write $\alpha = u + iv$, so that $z = u^2 + v^2$, $x = u^3 - 3uv^2$, and $y^2 = 3u^2v - v^3$. Thus, we must solve this equation. Note that since x and y are coprime, we have $\gcd(u,v) = 1$ and u and v have opposite parity. We write $y^2 = v(3u^2 - v^2)$ and consider two cases.

Case 1: $3 \nmid v$

Then v and $3u^2 - v^2$ are coprime, hence $v = \varepsilon a^2$, $3u^2 - v^2 = \varepsilon b^2$, $y = \pm ab$ with $\varepsilon = \pm 1$, and then a and b are coprime, b is odd, and $3 \nmid ab$. We note that $3u^2 - v^2 \equiv -(u^2 + v^2) \equiv -1 \pmod 4$ since u and v have opposite parity, hence we must have $\varepsilon = -1$, so the equations to be solved are $v = -a^2$ and $3u^2 = v^2 - b^2$. Since $3 \nmid v$ and $3 \nmid b$, changing if necessary b into $-b$, we may assume that $3 \mid v - b$, so the second equation is $u^2 = ((v-b)/3)(v+b)$. Note that v and b are coprime. I claim that v is odd. Indeed, otherwise a is even, hence $4 \mid v = -a^2$, hence $v^2 - b^2 \equiv 7 \pmod 8$, while $3u^2 \equiv 3 \pmod 8$, a contradiction. Thus v is indeed odd, so u is even and $v - b$ and $v + b$ are even with $(v-b)/2$ and $(v+b)/2$ coprime. Thus we can write $v - b = 6\varepsilon_1 c^2$, $v + b = 2\varepsilon_1 d^2$, $u = 2cd$ (where the sign of u can be removed by changing c into $-c$) with c and d coprime, and $3 \nmid d$. Thus $v = \varepsilon_1(3c^2 + d^2)$,

$b = \varepsilon_1(d^2 - 3c^2)$, and since $v = -a^2$ we have $\varepsilon_1 = -1$, the last remaining equation to be solved is the second degree equation $d^2 + 3c^2 = a^2$. Corollary 6.3.15 gives us à priori the two parametrizations $d = \pm(s^2 - 3t^2)$, $c = 2st$, $a = \pm(s^2 + 3t^2)$ with coprime integers s and t of opposite parity such that $3 \nmid s$, and $d = \pm(s^2+4st+t^2)$, $c = s^2-t^2$, $a = \pm 2(s^2+st+t^2)$, with coprime integers s and t of opposite parity such that $s \not\equiv t \pmod 3$. However, since $v = -a^2$ is odd, a is odd hence this second parametrization is impossible. Thus there only remains the first one, so replacing everywhere gives the first parametrization

$$\begin{cases} x = 4ts(s^2 - 3t^2)(s^4 + 6t^2s^2 + 81t^4)(3s^4 + 2t^2s^2 + 3t^4) \\ y = \pm(s^2 + 3t^2)(s^4 - 18t^2s^2 + 9t^4) \\ z = (s^4 - 2t^2s^2 + 9t^4)(s^4 + 30t^2s^2 + 9t^4)\ , \end{cases}$$

where $s \not\equiv t \pmod 2$ and $3 \nmid s$.

Case 2: $3 \mid v$

Set $w = v/3$. Then $3 \nmid u$, w and $u^2 - 3w^2$ are coprime, hence $v = \varepsilon 3a^2$, $u^2 - 3w^2 = \varepsilon b^2$, $y = \pm 3ab$ with $\varepsilon = \pm 1$, and then a and b are coprime and b is odd. Since u and v (hence w) have opposite parity, we have $u^2 - 3w^2 \equiv u^2 + w^2 \equiv 1 \pmod 4$, hence we must have $\varepsilon = 1$, so the equations to be solved are $w = a^2$ and $u^2 - 3w^2 = b^2$. Corollary 6.3.15 tells us that there exist coprime integers c and d of opposite parity such that either $u = c^2 + 3d^2$, $w = 2cd$, $b = c^2 - 3d^2$ with $3 \nmid c$, or $u = 2(c^2 + cd + d^2)$, $w = c^2 - d^2$, $b = c^2 + 4cd + d^2$ with $c \not\equiv d \pmod 3$, where the signs can be absorbed as usual either by changing x into $-x$ or b into $-b$. Thus in the first case the final equation to be solved is $2cd = a^2$, so that there exists coprime s and t with $3 \nmid s$ such that either $c = 2s^2$, $d = t^2$, $a = \pm 2st$ and t odd, or $c = s^2$, $d = 2t^2$, $a = \pm 2st$ and s odd. Replacing everywhere gives the second and third parametrizations:

$$\begin{cases} x = \pm(4s^4 + 3t^4)(16s^8 - 408t^4s^4 + 9t^8) \\ y = 6ts(4s^4 - 3t^4) \\ z = 16s^8 + 168t^4s^4 + 9t^8\ , \end{cases}$$

where t is odd and $3 \nmid s$.

$$\begin{cases} x = \pm(s^4 + 12t^4)(s^8 - 408t^4s^4 + 144t^8) \\ y = 6ts(s^4 - 12t^4) \\ z = s^8 + 168t^4s^4 + 144t^8\ , \end{cases}$$

where s is odd and $3 \nmid s$.

In the second case the final equation to be solved is $c^2 - d^2 = a^2$ with c and d of opposite parity, hence with a odd, so that by the solution to the Pythagorean equation there exists coprime integers s and t of opposite parity

such that $c = s^2 + t^2$, $d = 2st$, $a = s^2 - t^2$ with $s \not\equiv t \pmod 3$ Replacing everywhere gives the fourth and final parametrization:

$$\begin{cases} x = \pm 2(s^4 + 2ts^3 + 6t^2s^2 + 2t^3s + t^4)(23s^8 - 16ts^7 - 172t^2s^6 - 112t^3s^5 \\ \qquad\qquad - 22t^4s^4 - 112t^5s^3 - 172t^6s^2 - 16t^7s + 23t^8) \\ y = 3(s-t)(s+t)(s^4 + 8ts^3 + 6t^2s^2 + 8t^3s + t^4) \\ z = 13s^8 + 16ts^7 + 28t^2s^6 + 112t^3s^5 + 238t^4s^4 \\ \qquad\qquad + 112t^5s^3 + 28t^6s^2 + 16t^7s + 13t^8 \ , \end{cases}$$

where $s \not\equiv t \pmod 2$ and $s \not\equiv t \pmod 3$.

We have thus shown the following theorem:

Theorem 14.4.2. *The equation $x^2 + y^4 = z^3$ in integers x, y, z with $\gcd(x, y) = 1$ can be parametrized by one of the above four parametrizations, where s and t denote coprime integers with the indicated congruence conditions modulo 2 and 3. In addition these parametrizations are disjoint, in that any solution to our equation belongs to a single parametrization.*

14.5 Invariants, Covariants and Dessins d'Enfants

There is a completely different way of attacking the super-Fermat equation in the elliptic case, which is based on geometrical methods. This is an alternate way for the tetrahedral and octahedral cases, but is the only known way of solving the icosahedral case. The reason is that in the tetrahedral case $(2, 3, 3)$ and the octahedral case $(2, 3, 4)$, we can *factor* the equation (possibly in some number field), hence reduce to a simpler equation, and we treated these cases with complete success. On the other hand in the icosahedral case $(2, 3, 5)$, it is not possible to factor the equation. Thus another approach is needed, which will be given by the considerations of the present section.

14.5.1 Dessins d'Enfants, Klein Forms and Covariants

The present subsection will serve as a motivation for the results which will be given without proof below, and we refer to [Edw] for details. For the moment we ignore all rationality questions and we look for one-variable polynomials P, Q and R with complex coefficients satisfying $P^3 + Q^k = R^2$ for $k = 3$, 4 and 5. We could try to solve this by indeterminate coefficients, but there is no guarantee that we will succeed. However, we can use a very important theorem due to Belyi, which tells us (in our special case) that for any graph inscribed in the Riemann sphere (a "dessin d'enfant", name coined by A. Grothendieck), there exists a rational function ϕ from the sphere to $\mathbb{P}_1$ such that the zeros of ϕ have order equal to the number of edges meeting at

the vertices V of the graph, the poles of ϕ have order equal to the number of vertices along the faces F of the graph, and finally the values where $\phi = -1$ have order 2, one for each edge E of the graph, and the coefficients of ϕ may be chosen in a number field.

We apply this to the 5 platonic solids, and we index the polynomials according to their degrees.

• For the tetrahedron, we have $\phi = P_4^3/Q_4^3$ and $\phi + 1 = R_6^2/Q_4^3$, so that $P_4^3 + Q_4^3 = R_6^2$.

• For the cube, we have $\phi = P_8^3/Q_6^4$ and $\phi+1 = R_{12}^2/Q_6^4$, so that $P_8^3+Q_6^4 = R_{12}^2$.

• For the octahedron, we have $\phi = P_6^4/Q_8^3$ and $\phi + 1 = R_{12}^2/Q_8^3$, so that $P_6^4 + Q_8^3 = R_{12}^2$. This is exactly the same equation as for the cube (coming from the fact that the cube and the octahedron are dual), hence we do not need to consider the cube.

• For the dodecahedron, we have $\phi = P_{20}^3/Q_{12}^5$ and $\phi + 1 = R_{30}^2/Q_{12}^5$, so that $P_{20}^3 + Q_{12}^5 = R_{30}^2$.

• For the icosahedron, we have $\phi = P_{12}^5/Q_{20}^3$ and $\phi+1 = R_{30}^2/Q_{20}^3$, so that $P_{12}^5 + Q_{20}^3 = R_{30}^2$. This is exactly the same equation as for the dodecahedron (coming from the fact that the dodecahedron and the icosahedron are dual), hence we do not need to consider the dodecahedron.

This geometric interpretation explains the origin of the tetrahedral, octahedral and icosahedral terminology, which is always used when considering finite subgroups of $\mathrm{PSL}_2(\mathbb{C})$.

Almost a century before Belyi, Klein had already shown the existence of the Belyi functions ϕ in the case of platonic solids. More precisely, he showed the following:

Theorem 14.5.1. *Let G be the vertices of a regular tetrahedron, octahedron or icosahedron inscribed in the Riemann sphere, let N be the north pole of the sphere, and for $g \in G$ let $(\alpha_g : \beta_g) \in \mathbb{P}_1(\mathbb{C})$ be the point obtained by stereographic projection from N (if $g = N$, choose the point at infinity $(1:0)$). Let $k = |G|$ be the number of vertices (4, 6 or 12 respectively), let r be the number of edges meeting at each vertex (3, 4, or 5 respectively), and set*

$$f_G(s,t) = \prod_{g\in G}(\beta_g s - \alpha_g t),$$

$$h_G(s,t) = \frac{1}{k^2(k-1)^2}\left(\frac{\partial^2 f_G}{\partial s^2}\frac{\partial^2 f_G}{\partial t^2} - \left(\frac{\partial^2 f_G}{\partial s \partial t}\right)^2\right),$$

$$j_G(s,t) = \frac{1}{2k(k-2)}\left(\frac{\partial f_G}{\partial s}\frac{\partial h_G}{\partial t} - \frac{\partial f_G}{\partial t}\frac{\partial h_G}{\partial s}\right).$$

Then after a suitable rotation of the sphere there exists a constant $u_G \in \mathbb{C}$ such that

$$j_G^2 + h_G^3 + f_G^r/u_G = 0\,.$$

Although for the moment the polynomials are with coefficients in $\mathbb{C}$, this is exactly what we need for solving the $(2,3,r)$ equation in the elliptic case. To make this clearer, we look at all three cases. Consider first the regular tetrahedron. Up to rescaling and rotation we can choose $f_G(s,t) = t(s^3 - t^3)$ (the factor t corresponds to the north pole N, and the roots of $s^3 - t^3$ to the cube roots of unity, i.e., to the face of the tetrahedron opposite to N). A short computation shows that $j_G^2 + h_G^3 + f_G^3/64 = 0$, so that $u_G = 64$. Similarly, consider the regular octahedron. Clearly we can choose $f_G(s,t) = st(s^4 - t^4)$ (draw a picture!), and a short computation shows that $j_G^2 + h_G^3 + f_G^4/432 = 0$, so that $u_G = 432$. Finally, consider the regular icosahedron. Here the geometry is slightly more complicated, but after a little work it can be seen that we may choose $f_G(s,t) = st(s^{10} - 11s^5t^5 - t^{10})$ (Exercise 1), and a short computation shows that $j_G^2 + h_G^3 + f_G^5/1728 = 0$, so that $u_G = 1728$.

Starting from these basic solutions, if we apply an element of $\mathrm{GL}_2(\mathbb{C})$ we obtain a new relation of the same type (this is in fact the meaning of the word covariant), hence as many as we want. The basic problem is now to obtain polynomials with coefficients in $\mathbb{Q}$, or even in $\mathbb{Z}$, and to separate equivalent parametrizations under $\mathrm{GL}_2(\mathbb{Z})$. This can be done using a suitable *reduction* theory, see [Edw].

14.5.2 The Icosahedral Case (2, 3, 5)

It can be checked that up to signs, *all* the parametrizations that we have given in the preceding sections correspond to special cases of Klein's theorem: let us introduce a convenient shorthand, copied from [Edw]. We simply write $f = [a_k, \ldots, a_0]$ as an abbreviation for

$$f(s,t) = \sum_{0 \leqslant i \leqslant k} \binom{k}{i} a_i s^i t^{k-i} .$$

The inclusion of the binomial coefficient is natural and simplifies the formulas. Starting from f we define h and j as in the theorem, and since we now want arithmetic solutions, we will impose $u_G = \pm 1$, so that the parametrizations of $x^2 + y^3 \pm z^r = 0$ will be $x = \pm j$, $y = h$ and $z = \pm f$ for any sign in x and any sign in z if $r = 4$.

So that the reader can relate to what we have done in the cases $r = 3$ and $r = 4$, we give in abbreviated form the results that we have obtained, in the same order.

For $x^2 + y^3 - z^3 = 0$ the 3 parametrizations are $f_1 = [1,0,0,2,0]$, $f_2 = [2,1,0,1,2]$, and $f_3 = [3,0,1,0,-1]$.

For $x^2+y^3-z^4 = 0$ the 7 parametrizations are $f_1 = [7,1,-2,-4,-4,-4,-8]$, $f_2 = [27,0,3,0,-1,0,-1]$, $f_3 = [0,3,0,0,0,4,0]$, $f_4 = [0,12,0,0,0,1,0]$, $f_5 = [1,0,0,2,0,0,-32]$, $f_6 = [9,3,3,3,1,-1,-5]$, and $f_7 = [17,5,-1,1,1,1,-1]$.

For $x^2+y^3+z^4 = 0$ the 4 parametrizations are $f_1 = [1,0,-1,0,-3,0,27]$, $f_2 = [0,4,0,0,0,-3,0]$, $f_3 = [0,1,0,0,0,-12,0]$, and $f_4 = [3,4,1,0,-1,-4,-3]$.

We can now give without proof Edwards's result on the $(2,3,5)$ equation.

Theorem 14.5.2. *Up to changing x into $-x$ there are exactly 27 distinct parametrizations of $x^2+y^3+z^5=0$ given by*

$$f_1 = [0,1,0,0,0,0,-144/7,0,0,0,0,-20736,0]$$
$$f_2 = [-1,0,0,-2,0,0,80/7,0,0,640,0,0,-102400]$$
$$f_3 = [-1,0,-1,0,3,0,45/7,0,135,0,-2025,0,-91125]$$
$$f_4 = [1,0,-1,0,-3,0,45/7,0,-135,0,-2025,0,91125]$$
$$f_5 = [-1,1,1,1,-1,5,-25/7,-35,-65,-215,1025,-7975,-57025]$$
$$f_6 = [3,1,-2,0,-4,-4,24/7,16,-80,-48,-928,-2176,27072]$$
$$f_7 = [-10,1,4,7,2,5,80/7,-5,-50,-215,-100,-625,-10150]$$
$$f_8 = [-19,-5,-8,-2,8,8,80/7,16,64,64,-256,-640,-5632]$$
$$f_9 = [-7,-22,-13,-6,-3,-6,-207/7,-54,-63,-54,27,1242,4293]$$
$$f_{10} = [-25,0,0,-10,0,0,80/7,0,0,128,0,0,-4096]$$
$$f_{11} = [6,-31,-32,-24,-16,-8,-144/7,-64,-128,-192,-256,256,3072]$$
$$f_{12} = [-64,-32,-32,-32,-16,8,248/7,64,124,262,374,122,-2353]$$
$$f_{13} = [-64,-64,-32,-16,-16,-32,-424/7,-76,-68,-28,134,859,2207]$$
$$f_{14} = [-25,-50,-25,-10,-5,-10,-235/7,-50,-49,-34,31,614,1763]$$
$$f_{15} = [55,29,-7,-3,-9,-15,-81/7,9,-9,-27,-135,-459,567]$$
$$f_{16} = [-81,-27,-27,-27,-9,9,171/7,33,63,141,149,-67,-1657]$$
$$f_{17} = [-125,0,-25,0,15,0,45/7,0,27,0,-81,0,-729]$$
$$f_{18} = [125,0,-25,0,-15,0,45/7,0,-27,0,-81,0,729]$$
$$f_{19} = [-162,-27,0,27,18,9,108/7,15,6,-51,-88,-93,-710]$$
$$f_{20} = [0,81,0,0,0,0,-144/7,0,0,0,0,-256,0]$$
$$f_{21} = [-185,-12,31,44,27,20,157/7,12,-17,-76,-105,-148,-701]$$
$$f_{22} = [100,125,50,15,0,-15,-270/7,-45,-36,-27,-54,-297,-648]$$
$$f_{23} = [192,32,-32,0,-16,-8,24/7,8,-20,-6,-58,-68,423]$$
$$f_{24} = [-395,-153,-92,-26,24,40,304/7,48,64,64,0,-128,-512]$$
$$f_{25} = [-537,-205,-133,-123,-89,-41,45/7,41,71,123,187,205,-57]$$
$$f_{26} = [359,141,-1,-21,-33,-39,-207/7,-9,-9,-27,-81,-189,-81]$$
$$f_{27} = [295,-17,-55,-25,-25,-5,31/7,-5,-25,-25,-55,-17,295]$$

For instance, one of the simplest parametrizations, given by f_{20}, is explicitly

$$\begin{cases} x = \pm(81s^{10}+256t^{10})(6561s^{20}-6088608t^5s^{15}-207484416t^{10}s^{10} \\ \qquad\qquad +19243008t^{15}s^5+65536t^{20}) \\ y = -6561s^{20}-2659392t^5s^{15}-10243584t^{10}s^{10}+8404992t^{15}s^5-65536t^{20} \\ z = 12st(81s^{10}-1584t^5s^5-256t^{10})\ . \end{cases}$$

14.6 The Parabolic and Hyperbolic Cases

14.6.1 The Parabolic Case

We now consider the parabolic case $1/p+1/q+1/r=1$. Up to permutation of (p,q,r), this corresponds to the three cases $(p,q,r)=(2,3,6)$, $(2,4,4)$ and $(3,3,3)$. The result is then simply as follows.

Proposition 14.6.1. *In the parabolic case $1/p+1/q+1/r=1$, the equation $x^p+y^q=z^r$ has no solutions in nonzero coprime integers, except that the equation $x^3+y^6=z^2$ has the solutions $(x,y,z)=(2,\pm1,\pm3)$, and the equation $x^3+y^2=z^6$ has the solutions $(x,y,z)=(-2,\pm3,\pm1)$.*

Proof. The $(3,3,3)$ case is FLT for exponent 3, which has been proved in Section 6.9. The $(2,4,4)$ case corresponds to the equations $x^4\pm y^4=z^2$ which have also been treated in that section (Proposition 6.6.14). We are left with the $(2,3,6)$ case which, thanks to the reductions made above, reduces to the equations $x^3\pm y^6=z^2$. Setting $X=x/y^2$, $Y=z/y^3$, our equations are thus equivalent to finding rational points on the curves $Y^2=X^3\pm1$. This is done by the 2-descent technique, explained in Chapter 8, which is here very easy to apply since the 2-torsion point $(\mp1,0)$ has rational coordinates. We have treated this example in Proposition 8.2.14, but we can of course be lazy and use Cremona's `mwrank` program which tells us that both curves have rank 0. The curve $Y^2=X^3-1$ has only the point $(1,0)$ as torsion point (in addition to the point at infinity). On the other hand, the curve $Y^2=X^3+1$ has a torsion subgroup of order 6, and apart from the point at infinity the torsion points are $(-1,0)$, $(0,\pm1)$ and $(2,\pm3)$. The points $(-1,0)$ and $(0,\pm1)$ correspond to $z=0$ and $x=0$, respectively, while the points $(2,\pm3)$ give $x=2y^2$, $z=\pm3y^3$. Since x and y are coprime, we must have $y=\pm1$, hence $x=2$ and $z=\pm3$, proving the proposition. □

Thus in the parabolic case there are only finitely many nonzero coprime solutions. Note however that this is because we only consider the super-Fermat equation with coefficients ±1. In case of general coefficients, the equation may have finitely or infinitely many coprime solutions, depending on whether the rank of the corresponding elliptic curve is zero or not. For instance the equations $x^2+y^4=2z^4$ and $x^4+8y^4=z^2$ have infinitely many coprime solutions, see Exercise 12 of Chapter 8 and Exercise 2.

14.6.2 General Results in the Hyperbolic Case

We finally consider what is by far the most difficult case, the hyperbolic case $1/p + 1/q + 1/r < 1$. Proving all that is known would require a book in itself, so we will only give a survey with little proofs. Note that when we talk of solutions to our equations, we always mean integral nonzero coprime solutions.

First, there is a beautiful theorem of Darmon and Granville [Dar-Gra] as follows.

Theorem 14.6.2. *For fixed p, q, and r such that $1/p + 1/q + 1/r < 1$ and fixed nonzero integers A, B, and C, there exist only finitely many solutions to the equation $Ax^p + By^q + Cz^r = 0$ in integers x, y, and z with x and y coprime.*

To prove this theorem, they succeed in reducing it to Faltings's famous theorem on the finiteness of the number of rational points on a curve of genus greater than or equal to 2 (Mordell's conjecture), which is not a trivial task since $Ax^p + By^q + Cz^r = 0$ does not a priori represent a curve.

Second, we recall the very important *abc conjecture* of Masser–Oesterlé, which implies many results or other conjectures in number theory (for instance Elkies has proved that it implies Faltings's result above: *abc* implies Mordell, see [Elk]). There are several possible statements of this conjecture, but the following is sufficient.

Definition 14.6.3. *For a nonzero natural integer N we define the* radical $\mathrm{rad}(N)$ *of N as the product of the prime numbers dividing N, i.e.,* $\mathrm{rad}(N) = \prod_{p|N} p$.

The *abc* conjecture is then as follows.

Conjecture 14.6.4. *Let $\varepsilon > 0$. If a, b, and c are three nonzero pairwise coprime integers such that $a + b + c = 0$ then*

$$\max(|a|, |b|, |c|) = O_\varepsilon(\mathrm{rad}(abc)^{1+\varepsilon}) .$$

We then have the following result:

Proposition 14.6.5. *The abc conjecture implies that the* total *number of nonzero coprime solutions to $x^p \pm y^q \pm z^r = 0$ with $1/p + 1/q + 1/r < 1$ is finite, even allowing p, q and r to vary. Here, if $x = \pm 1$ (resp., $y = \pm 1$, resp., $z = \pm 1$), we identify solutions having the same value of x^p (resp., y^q, resp., z^r).*

Proof. Order p, q and r such that $p \leqslant q \leqslant r$. Then the hyperbolic cases correspond to the triples $(2,3,r)$ for $r \geqslant 7$, $(2,4,r)$ for $r \geqslant 5$, $(2,q,r)$ for $r \geqslant q \geqslant 5$, $(3,3,r)$ for $r \geqslant 4$, $(3,q,r)$ for $r \geqslant q \geqslant 4$, or (p,q,r) with $r \geqslant q \geqslant p \geqslant 4$. In all these cases one checks immediately that $1/p + 1/q + 1/r \leqslant 41/42$,

attained for $(p,q,r) = (2,3,7)$. We apply the *abc* conjecture to $a = x^p$, $b = \pm y^q$ and $c = \pm z^r$, and choose $\varepsilon = 1/42$. Note that $\mathrm{rad}(abc) = \mathrm{rad}(xyz) \leqslant xyz$. If we set $M = \max(|x^p|, |y^q|, |z^r|)$, we thus have

$$\begin{aligned} M &= O((xyz)^{1+\varepsilon}) = O(M^{(1/p+1/q+1/r)(1+\varepsilon)}) \\ &= O(M^{(41/42)(43/42)}) = O(M^{1763/1764}) , \end{aligned}$$

which is impossible if M is sufficiently large. Thus M is bounded, hence so are x, y. z, p, q and r (except in the special case $\min(|x|, |y|, |z|) = 1$), proving the proposition. □

A stronger statement is given in Exercise 3.

Remark. As already mentioned in Chapter 1, it has been proved by P. Mihăilescu in 2002 that Catalan's conjecture is true, i.e., that $x^p \pm y^q = 1$ is possible only if $x^p = 9$ and $y^q = 8$, and I refer the reader to Section 6.11 and Chapter 16 for a detailed description of the proof (see also [Bilu] and [Mis]). Thus the special case mentioned in the proposition occurs only (up to ordering of p, q and r) for $p = 2$, $q = 3$, $r \geqslant 7$, with $(\pm 3)^p - 2^q = 1^r$ (and also $(-1)^r$ when r is even).

A computer search gives the following 10 essentially different solutions (where as above the first one is only counted once, and we also count once solutions differing only by sign changes).

$$\begin{aligned} 1^r + 2^3 &= (\pm 3)^2 \quad (\text{for } r \geqslant 7, \text{ with also } (-1)^r \text{ for } r \text{ even}) \\ (\pm 3)^4 + (-2)^5 &= (\pm 7)^2 \\ 2^9 + (-7)^3 &= (\pm 13)^2 \\ 2^7 + 17^3 &= (\pm 71)^2 \\ 3^5 + (\pm 11)^4 &= (\pm 122)^2 \\ 15613^3 - (\pm 33)^8 &= (\pm 1549034)^2 \\ 65^7 + (-1414)^3 &= (\pm 2213459)^2 \\ 113^7 + (-9262)^3 &= (\pm 15312283)^2 \\ 17^7 + 76271^3 &= (\pm 21063928)^2 \\ (\pm 43)^8 + 96222^3 &= (\pm 30042907)^2 \end{aligned}$$

These solutions can easily be found in a few seconds by a systematic search on a fast PC. A search for several weeks has not revealed any additional solutions. There may be no more, and on probabilistic grounds one would expect at most 2 or 3 more. Note also that the number of solutions found decreases with $\chi = 1/p + 1/q + 1/r - 1$, as can be expected: counting the

first one when possible, we have 5 solutions for $\chi = -1/42$, 3 solutions for $\chi = -1/24$, 2 solutions for $\chi = -1/20$, 1 solution for $\chi = -1/18$ and no solution for other χ (apart from the first when applicable).

14.6.3 The Equation $x^6 - y^4 = z^2$

We now study a few hyperbolic equations. In each case, we proceed as follows. We reduce the equation to finding integral or rational points on curves. We then use general methods to find this set of points. When the curve is an elliptic curve, we use Cremona's `mwrank` program, which does all the work for us, or the methods explained in Chapter 8. When the curve is a curve of higher genus, or an elliptic curve of nonzero rank, the problem becomes more difficult and we will only mention the known results.

Proposition 14.6.6. *The equation $x^6 - y^4 = z^2$ has no solution in nonzero coprime integers x, y, z.*

Proof. Although we could use the solution of the elliptic equation $x^2+y^4 = z^3$ given in Section 14.4.2, it is much simpler to use only the solution to the dihedral equation $x^2 + y^2 = z^3$. Indeed, we obtain that $x^6 - y^4 = z^2$ is equivalent to $x^2 = s^2 + t^2$, $y^2 = s(s^2 - 3t^2)$, $z = t(3s^2 - t^2)$ where s and t are coprime with $s \not\equiv t \pmod 2$. The first equation is equivalent to $s = 2uv$, $t = u^2 - v^2$, $x = \pm(u^2 + v^2)$, up to exchange of s and t, where u and v are coprime integers of opposite parity. We consider both cases.

Case 1: $2 \mid s$

Set $a = u + v$, $b = u - v$, which are coprime and both odd. Then $s = (a^2 - b^2)/2$ and $t = ab$, so the last equation to be solved can be written $8y^2 = (a^2 - b^2)(a^4 - 14a^2b^2 + b^4)$. Since b is odd, we can set $Y = y/b^3$, $X = a^2/b^2$, and we obtain the elliptic curve $8Y^2 = (X - 1)(X^2 - 14X + 1)$, which can be given in reduced Weierstrass form as $y^2 = (x+2)(x^2-2x-11)$. In any case, the `mwrank` program tells us that (outside the point at infinity) the only rational point has $y = 0$, which does not correspond to a solution of our equation.

Case 2: $2 \nmid s$

Here $s = u^2 - v^2$, $t = 2uv$, so that the last equation to be solved can be written $y^2 = (u^2 - v^2)(u^4 - 14u^2v^2 + v^4)$. We cannot have $v = 0$, otherwise $t = 0$ hence $z = 0$, which is impossible. Thus, we can set $Y = y/v^3$, $X = u^2/v^2$ and we obtain the elliptic curve $Y^2 = (X - 1)(X^2 - 14X + 1)$, which can be given in reduced Weierstrass form as $y^2 = (x + 4)(x^2 - 4x - 44)$. In any case the `mwrank` program again tells us that the only rational point has $y = 0$, which again does not correspond to a solution. □

14.6.4 The Equation $x^4 - y^6 = z^2$

Proposition 14.6.7. *The equation $x^4 - y^6 = z^2$ has no solution in nonzero coprime integers x, y, z.*

Proof. Once again, we use the solution to the dihedral equation. We obtain that our equation is equivalent to $x^2 = s(s^2+3t^2)$, $z = t(3s^2+t^2)$, $y^2 = s^2-t^2$ with s and t coprime of opposite parity, or to $x^2 = \pm(2s^3+t^3)$, $z = 2s^3-t^3$, $y^2 = 2ts$ with s and t coprime and t odd. We consider both cases separately.

Case 1: $2 \nmid y$

This corresponds to the first parametrization. Since $y^2+t^2 = s^2$ and y is odd, there exist coprime u and v of opposite parity such that $y = u^2-v^2$, $t = 2uv$ and $s = \pm(u^2+v^2)$. Since $x^2 > 0$, we have $s > 0$ so the $\pm$ is $+$. The last equation to be solved is thus is $x^2 = (u^2+v^2)(u^4+14u^2v^2+v^4)$. Note for future reference that since u and v have opposite parity, x is odd. We have $v \neq 0$ otherwise $t = 0$ hence $z = 0$, which is impossible. Thus we set $Y = z/v^3$, $X = u^2/v^2$ and obtain the elliptic curve $Y^2 = (X+1)(X^2+14X+1)$, which can be given in reduced Weierstrass form as $y^2 = (x-4)(x^2+4x-44)$. However here the `mwrank` program tells us that this is a curve of rank 1, hence we must proceed differently. Note that when we set $X = u^2/v^2$, we implicitly forget the information that X is a square. In order to keep it, we must return to the equation $x^2 = (u^2+v^2)(u^4+14u^2v^2+v^4)$. First, we set $a = u+v$, $b = u-v$, which are coprime and both odd. We obtain $2x^2 = (a^2+b^2)(a^4-a^2b^2+b^4)$. Since $a^4-a^2b^2+b^4 = (a^2+b^2)^2-3a^2b^2$, it follows that the only possible common prime divisor of a^2+b^2 and $a^4-a^2b^2+b^4$ is $p = 3$. But this is impossible, since $a^2+b^2 \equiv 0 \pmod 3$ if and only if $a \equiv b \equiv 0 \pmod 3$, which is excluded since a and b are coprime. Thus the factors are coprime, and by positivity we obtain that there exist integers c and d such that $a^2+b^2 = 2c^2$, $a^4-a^2b^2+b^4 = d^2$ and $x = \pm cd$, and c and d are both odd since x is odd.

We consider only the second equation. Setting $D = d/b^2$, $A = a/b$ we obtain the hyperelliptic quartic curve of genus 1 $D^2 = A^4-A^2+1$. Corollary 7.2.2 tells us that if we set $X = 2A^2-2D-1$, $Y = 2A(2A^2-D-1)$ this is a birational transformation whose inverse is $A = Y/(2X)$, $D = Y^2/(4X^2)-(X+1)/2$ and which transforms our genus 1 curve into the Weierstrass equation $Y^2 = X(X^2+2X-3)$, and now the `mwrank` program tells us that the rank is zero, but there are 8 rational torsion points on the curve: not counting the point at infinity, they are $(-3,0)$, $(-1,\pm 2)$, $(0,0)$, $(1,0)$ and $(3,\pm 6)$. Because of our birational transformation, we cannot have $Y = 0$. It is easy to check that the other 4 points $(X,Y) = (-1,\pm 2)$ and $(3,\pm 6)$ correspond to the 4 points $(A,D) = (\pm 1,\pm 1)$. Since $A = a/b$ and a and b are coprime, we must have therefore $a = \pm 1$ and $b = \pm 1$, hence $a = \pm b$. Now recall that $a = u+v$ and $b = u-v$. It follows that $a = \pm b$ is equivalent to $uv = 0$, hence to $t = 0$, which is impossible since this implies $z = 0$, so that there are no solutions in this case as claimed.

Case 2: $2 \mid y$

This corresponds to the second parametrization $x^2 = \pm(2s^3+t^3)$, $z = 2s^3-t^3$, $y^2 = 2ts$ with s and t coprime and t odd. Thus there exist coprime a and b with a odd and $\varepsilon = \pm 1$ such that $t = \varepsilon a^2$, $s = 2\varepsilon b^2$ and $y = \pm 2ab$. The last equation to be solved is thus $x^2 = \pm\varepsilon(a^6+16b^6)$. Since a is odd, we

have $\varepsilon = \pm$ hence the equation is $x^2 = a^6 + 16b^6$. We have $b \neq 0$, otherwise $y = 0$, hence setting $Y = x/b^3$ and $X = a^2/b^2$ we obtain the elliptic curve $Y^2 = X^3+16$, whose minimal Weierstrass equation is $y^2+y = x^3$, and `mwrank` tells us that the only rational points outside the point at infinity of this curve are those with $x = 0$, hence $X = 0$, hence $a = 0$, which is impossible since a is odd. □

14.6.5 The Equation $x^6 + y^4 = z^2$

Proposition 14.6.8. *The equation $x^6 + y^4 = z^2$ has no solution in nonzero coprime integers x, y, z.*

Proof. Once again, we use the solution to the dihedral equation. We obtain that our equation is equivalent to $z = s(s^2+3t^2)$, $y^2 = t(3s^2+t^2)$, $x^2 = s^2-t^2$ with s and t coprime of opposite parity, or to $z = \pm(2s^3 + t^3)$, $y^2 = 2s^3 - t^3$, $x^2 = 2ts$ with s and t coprime and t odd. We consider both cases separately.
Case 1: $2 \nmid x$

This corresponds to the first parametrization. Since $x^2 + t^2 = s^2$ and x is odd, there exist coprime u and v of opposite parity such that $x = u^2 - v^2$, $t = 2uv$, $s = \pm(u^2 + v^2)$. The last equation to be solved is thus $y^2 = 2uv(3u^4 + 10u^2v^2 + 3v^4)$. We set $a = u + v$, $b = u - v$ which are both odd, and this gives $2y^2 = (a^2-b^2)(a^4+a^2b^2+b^4)$. We set $Y = y/b^3$, $X = a^2/b^2$ and we obtain the elliptic curve $2Y^2 = (X-1)(X^2+X+1) = X^3-1$, whose reduced Weierstrass equation is $y^2 = x^3 - 8$. Once again `mwrank` tells us that this equation has no solutions with $y \neq 0$.
Case 2: $2 \mid x$

This corresponds to the second parametrization. Since t is odd, s is even, and since s and t are coprime the equation $x^2 = 2ts$ gives $t = \varepsilon u^2$, $s = 2\varepsilon v^2$ and $x = \pm 2uv$ with u and v coprime, u odd and $\varepsilon = \pm 1$. The last equation to be solved is thus $y^2 = \varepsilon(16v^6 - u^6)$. Since u is odd, y is odd, hence $y^2 \equiv 1 \pmod 8$ while $16v^6 - u^6 \equiv -1 \pmod 8$. Thus $\varepsilon = -1$, and we have $y^2 = u^6 - 16v^6$. We have $v \neq 0$, otherwise $s = 0$ hence $z = 0$, which is impossible. Thus setting $Y = y/v^3$ and $X = u^2/v^2$ gives the elliptic curve $Y^2 = X^3 - 16$ in reduced Weierstrass form, and once again `mwrank` tells us that this curve has no solutions with $y \neq 0$. □

Putting together the three equations above, we obtain the following

Corollary 14.6.9. *The equations $\pm x^6 \pm y^4 = z^2$ have no solutions in nonzero coprime integers x, y, z.*

14.6.6 The Equation $x^4 + y^4 = z^5$

Proposition 14.6.10. *The equation $x^4+y^4 = z^5$ has no solution in nonzero coprime integers x, y, z.*

Proof. Once again we use the solution to the dihedral equation. Our equation is thus equivalent to $x^2 = s(s^4 - 10t^2s^2 + 5t^4)$, $y^2 = t(5s^4 - 10t^2s^2 + t^4)$, and $z = s^2 + t^2$, where s and t are coprime integers of opposite parity. I claim that $5 \mid st$. Indeed, if s and t are not divisible by 5, then the factors in the expressions for x^2 and y^2 are coprime, hence in particular there exist integers u and v such that $s^4 - 10t^2s^2 + 5t^4 = \pm u^2$ and $5s^4 - 10t^2s^2 + t^4 = \pm v^2$. Then if t is even s is odd, and the second equation gives a contradiction modulo 8, and similarly if t is odd then s is even and now the first equation gives a contradiction modulo 8, proving my claim. Thus $5 \mid st$, and exchanging x and y, hence s and t if necessary we may assume that $5 \mid s$. Writing $s = 5s_1$, we thus have in particular $(x/5)^2 = s_1(125s_1^4 - 50t^2s_1^2 + t^4)$, hence $125s_1^4 - 50t^2s_1^2 + t^4 = \pm u^2$ for some integer u. If t is even s_1 is odd, and this gives a contradiction modulo 8. Thus $s = 5s_1$ is even, and since t is coprime to 5 the equation for y^2 gives $5s^4 - 10t^2s^2 + t^4 = \pm v^2$, and since s is even and t is odd, again looking modulo 8 we see that the sign must be $+$, hence we finally obtain the hyperelliptic quartic of genus 1 with equation $V^2 = T^4 - 10T^2 + 5$, with $V = v/s^2$ and $T = t/s$. Corollary 7.2.2 tells us that if we set $X = 2(T^2 - V - 5)$ and $Y = 4T(T^2 - V - 5)$ this is a birational transformation whose inverse is $T = Y/(2X)$ and $V = Y^2/(4X^2) - X/2 - 5$, and which transforms our genus 1 curve into the Weierstrass equation in minimal form $Y^2 = X(X^2 + 20X + 80)$. This curve has a rational point of order 2, hence the 2-descent method of Section 8.2.4 is easily applicable and shows that our curve has rank 0 (or we can be lazy and use `mwrank`). The only nontrivial torsion point has $X = 0$, hence $V = 5 - T^2$, but replacing in the quartic we obtain the contradiction $25 = 5$, proving the proposition. □

Remark. The equation $x^4 - y^4 = z^5$ leads to elliptic curves of nonzero rank, and I do not know whether it can be treated by similar methods (although the nonexistence of nontrivial solutions follows from the $(2, 4, 5)$ case treated by Bruin, see below).

14.6.7 Further Results

The reason for which it has not been difficult to treat the $(2, 4, 6)$ cases and one of the $(4, 4, 5)$ cases is that we have always been able to reduce to curves of genus 1 with only a finite number of rational points. In only one case, we had a curve of genus 1 with infinitely many rational points, but we were able to bypass it by using additional information given by the elliptic parametrizations. Unfortunately, in other hyperbolic cases, when reducing to finding rational points on curves, some of these curves will have infinitely many rational points, and some will be of genus greater than or equal to 2, and our knowledge of algorithmic methods for finding all rational points on such curves is much smaller. One of the only general methods, due to Chabauty, unfortunately works only in certain cases, see Chapter 13. In other cases, such as FLT itself, one can also use the method of Ribet–Wiles for finding all the

solutions. Thus, we give a brief survey of known results. For equations with fixed small exponents (p, q, r), one method is to find covering curves for the solutions. These curves may be of genus 1, as we have seen in the $(2, 4, 6)$ and $(4, 4, 5)$ examples, but are in general of higher genus. We summarize below the known results, including the highest genus which is necessary and the name of the authors. Recall that we only consider nonzero coprime solutions.

Equation	Solutions	Genus	Author(s)
$\pm x^6 \pm y^4 = z^2$	none	1	Bruin
$x^2 + y^4 = z^5$	none	2	Bruin
$x^2 - y^4 = z^5$	$(\pm 7, \pm 3, -2)$, $(\pm 122, \pm 11, 3)$	2	Bruin
$x^2 + y^8 = z^3$	$(\pm 1549034, \pm 33, 15613)$	2	Bruin
$x^2 - y^8 = z^3$	$(\pm 3, \pm 1, 2)$, $(\pm 30042907, \pm 43, 96222)$	2	Bruin
$x^2 + y^3 = z^7$	$(\pm 3, -2, 1)$, $(\pm 71, -17, 2)$, $(\pm 2213459, 1414, 65)$, $(\pm 15312283, 9262, 113)$, $(\pm 21063928, -76271, 17)$	3	Poonen–Schaefer–Stoll
$x^2 + y^3 = z^9$	$(\pm 3, -2, 1)$, $(\pm 13, 7, 2)$	3	Bruin

The results of N. Bruin can be found in [Bru1] and [Bru2]. The $(2, 3, 7)$ result, which is very recent (2004, see [Poo-Sch-Sto]), deserves special mention. Using Galois representation techniques and level lowering à la Ribet–Wiles (see Chapter 15), the authors show that solutions come from rational points on twists of the modular curve $X(7)$ that come from a finite list of elliptic curves, and this leads to finding the rational points satisfying congruence conditions modulo 2 and 3 on precisely 10 curves of genus 3 defined over $\mathbb{Q}$, which over $\mathbb{C}$ are all isomorphic to the so-called Klein quartic curve whose projective equation is $x^3y + y^3z + z^3x = 0$.

Using known techniques it is possible to find the rational points satisfying the congruence conditions on 9 of the 10 curves, leading to the given solutions. To prove that the tenth curve does not have any rational point is more difficult, but has been achieved by the authors. It is interesting to note that the large solutions for the $(2, 3, 7)$ come from extremely small solutions on the twisted Klein curves.

Once again we note that the large number of solutions in this case is (heuristically) due to the fact that $\chi = 1/p + 1/q + 1/r - 1 = -1/42$ is as close to zero as it can be in the hyperbolic case.

All the other results on the super-Fermat equation (including the original Fermat equation itself) have also been proved using Galois representation techniques. We refer to Chapter 15, written by S. Siksek, for a black box

explanation of this method, and we also refer to the excellent papers [Kra2] and [Ben2] for surveys, details and references. Among the results obtained to date (2006) using this method we cite the following.

equation	conditions	author(s)
$x^n + y^n = z^n$	$3 \leqslant n$	Ribet–Taylor–Wiles
$x^3 + y^3 = z^n$	$17 \leqslant n \leqslant 10000$ or z even	Kraus
$x^5 + y^5 = z^n$	$3 \leqslant n$ and z even	Darmon–Kraus
$x^n + y^n = z^2$	$4 \leqslant n$	Darmon–Merel, Poonen
$x^n + y^n = z^3$	$3 \leqslant n$	Darmon–Merel, Poonen
$x^4 + y^n = z^4$	$2 \leqslant n$	Darmon
$x^2 + y^4 = z^n$	$211 \leqslant n$	Ellenberg, Ramakrishnan
$x^2 - y^4 = z^n$	$5 \leqslant n$	Bennett–Skinner
$x^2 + y^{2n} = z^3$	$11 \leqslant n \leqslant 1000$ and $n \neq 31$, or y even	Chen
$x^4 + y^{2n} = z^3$	$2 \leqslant n$	Bennett–Chen
$x^2 + y^{4n} = z^3$	$2 \leqslant n$	Bennett–Chen
$x^{2n} + y^{2n} = z^5$	$2 \leqslant n$	Bennett

14.7 Applications of Mason's Theorem

It is interesting to note that most of the important Diophantine problems that we have met in this book, such as Fermat's last theorem, Catalan's equation, the super-Fermat equation, and others, have a very simple answer if we look at them in the context of *polynomials*, in other words if we look for polynomial, as opposed to rational or integral, solutions. This essentially follows from a single, elementary, result, due to Mason. It should be emphasized that these results have no use whatsoever for the initial Diophantine equations to be solved over $\mathbb{Q}$. Nonetheless I believe that it has a place in this book.

14.7.1 Mason's Theorem

The reader should compare with Definition 14.6.3 and Conjecture 14.6.4.

Definition 14.7.1. *For a nonzero polynomial P in one variable, we define* $\mathrm{rad}(P)$ *to be the monic polynomial with no multiple roots having the same roots as P, in other words* $\mathrm{rad}(P) = \prod_{P(\alpha)=0}(X - \alpha)$.

Proposition 14.7.2 (Mason). *Let A, B, C be pairwise coprime polynomials in one variable, not all constant and such that $A + B + C = 0$. Then*

$$\max(\deg(A), \deg(B), \deg(C)) \leqslant \deg(\mathrm{rad}(ABC)) - 1\,.$$

In other words, the *abc* conjecture is true for polynomials.

Proof. Let $f = A/C$ and $g = B/C$, so that f and g are rational functiona such that $f + g + 1 = 0$. Note that g is not constant, otherwise f would also be constant and A, B, and C would be proportional hence constant since they are pairwise coprime. Differentiating, it follows that $f' = -g'$, hence

$$\frac{B}{A} = \frac{g}{f} = -\frac{f'/f}{g'/g} .$$

If we write

$$A(X) = a\prod_i (X-\alpha_i)^{a_i}, \quad B(X) = b\prod_j (X-\beta_j)^{b_j}, \quad C(X) = c\prod_k (X-\gamma_k)^{c_k}$$

we have

$$\frac{f'}{f}(X) = \sum_i \frac{a_i}{X-\alpha_i} - \sum_k \frac{c_k}{X-\gamma_k} \quad \text{and} \quad \frac{g'}{g}(X) = \sum_j \frac{b_j}{X-\beta_j} - \sum_k \frac{c_k}{X-\gamma_k} .$$

Thus if we multiply f'/f and g'/g by $N = \mathrm{rad}(ABC)$ we obtain polynomials, and the degree of these polynomials is at most equal to $\deg(N) - 1$. From the equality

$$\frac{B}{A} = -\frac{Nf'/f}{Ng'/g}$$

and the fact that A and B are coprime we deduce that B divides Nf'/f and A divides Ng'/g, hence that $\max(\deg(A), \deg(B)) \leqslant \deg(N) - 1$, so $\deg(C) = \deg(-A - B) \leqslant \deg(N) - 1$, proving the proposition. □

14.7.2 Applications

Corollary 14.7.3. *FLT is true for polynomials in one variable which are not all constant, in other words if f, g, and h are nonzero polynomials, not all constant and such that $f^n + g^n = h^n$ then $n \leqslant 2$.*

Proof. Dividing the equation by $\gcd(f, g)^n$ we may assume that f, g, and h are pairwise coprime. Setting $A = f^n$, $B = g^n$, $C = -h^n$ we have $A + B + C = 0$ and $\mathrm{rad}(ABC) \mid fgh$. Thus by the above proposition we have

$$n\max(\deg(f), \deg(g), \deg(h)) \leqslant \deg(fgh) - 1 = \deg(f) + \deg(g) + \deg(h) - 1 .$$

Adding the corresponding inequalities for f, g, and h we obtain

$$n(\deg(f) + \deg(g) + \deg(h)) \leqslant 3(\deg(f) + \deg(g) + \deg(h)) - 3 ,$$

hence $n < 3$ as claimed. □

Note that since we have a two-parameter coprime integer solution to FLT for $n = 2$, a fortiori there exists a solution with polynomials in one variable, for instance $f = 2x$, $g = x^2 - 1$, and $h = x^2 + 1$.

More generally, a similar proof shows that the super-Fermat equation can have solutions only in the elliptic case:

Corollary 14.7.4. *Let p, q, r be integers such that $2 \leqslant p \leqslant q \leqslant r$, and assume that f, g, and h are pairwise coprime polynomials, not all constant and satisfying the super-Fermat equation $f^p + g^q = h^r$. We are then in the elliptic case, in other words $(p,q,r) = (2,2,r)$ for some $r \geqslant 2$, $(2,3,3)$, $(2,3,4)$, or $(2,3,5)$.*

Proof. Once again we have $A + B + C = 0$ with $A = f^p$, $B = g^q$, and $C = -h^r$, which are pairwise coprime by assumption, and $\mathrm{rad}(ABC) \mid fgh$. If we denote by a, b, and c respectively the degrees of f, g, and h, the above proposition tells us that $\max(pa, qb, rc) \leqslant a + b + c - 1$. Since $p \leqslant q \leqslant r$ we have $p(a+b+c) \leqslant pa + qb + rc \leqslant 3(a+b+c) - 3$, hence as for FLT we deduce that $p < 3$, hence $p = 2$ and the inequality $pa \leqslant a + b + c - 1$ gives $a \leqslant b + c - 1$. If $q = 2$ we are in the dihedral case $(2,2,r)$. Otherwise, assume that $q \geqslant 3$. Our basic inequality now gives $2a + qb + rc \leqslant 3a + 3b + 3c - 3$, hence since $q \leqslant r$

$$q(b+c) \leqslant qb + rc \leqslant a + 3b + 3c - 3 \leqslant 4(b+c) - 4\ ,$$

so that $q < 4$, hence $q = 3$. Finally, for $p = 2$ and $q = 3$ the inequality for qb gives $2b \leqslant a + c - 1 \leqslant b + 2c - 2$, so that $b \leqslant 2c - 2$, hence $a \leqslant b + c - 1 \leqslant 3c - 3$. Thus $rc \leqslant a + b + c - 1 \leqslant 6(c-1)$, hence $r < 6$, so $r = 3$, 4, or 5, proving the corollary. □

Note that we have seen in Sections 14.2, 14.3, 14.4, and 14.5.2, that in all the elliptic cases we have a two-variable parametrization, hence in the given cases of the corollary, solutions do indeed exist.

14.8 Exercises for Chapter 14

1. Show that, as claimed in the text, in Theorem 14.5.1 we can choose $f_G(s,t) = st(s^{10} - 11s^5t^5 - t^{10})$ in the case of the regular icosahedron.
2. As a numerical sequel of Exercise 12 of Chapter 8, compute all coprime integral solutions of $x^2 + y^4 = 2z^4$ with $|x| \leqslant 10^{100}$.
3. (M. Stoll.) Assume that the following weaker form of the *abc* Conjecture 14.6.4 is valid: there exists $\varepsilon < 1/5$ such that for all nonzero pairwise coprime integers a, b, c with $a + b + c = 0$ we have $\max(|a|,|b|,|c|) = O(\mathrm{rad}(abc)^{1+\varepsilon})$.

(a) Prove that there are in total only finitely many solutions to the super-Fermat equations with $1/p + 1/q + 1/r < 5/6 + \delta$ for some $\delta > 0$ depending on ε.

(b) Deduce from the Darmon–Granville Theorem 14.6.2 that there are in total only finitely many solutions in the hyperbolic case.

4. Let p and q be integers such that $p \geqslant 2$ and $q \geqslant 2$. Using Mason's theorem (Proposition 14.7.2), prove that if f and g are nonconstant coprime polynomials then
$$\deg(f^p - g^q) \geqslant (p - 1 - p/q)\deg(f) + 1 .$$
The special case $\deg(f^3 - g^2) \geqslant (\deg(f)/2) + 1$ is due to Davenport and is the polynomial analogue of *Hall's conjecture*, which states that if a, b are coprime positive integers different from 1 then for every $\varepsilon > 0$ we have $|a^3 - b^2| \geqslant a^{1/2-\varepsilon}$ except for finitely many (a, b).
5. Let p, q, and r be strictly positive integers. Show that there do not exist any solutions to the *negative* super-Fermat equation $x^{-p} + y^{-q} = z^{-r}$ with x, y, and z pairwise coprime.