4.1 Hensel's Analogy: Prime and Space

Hensel conceived of an analogy in which integers could be viewed as "functions" on the "space" of prime numbers (this would be much much more broadly generalized in modern algebraic geometry). To understand this analogy, we compare $\mathbb{Z}$ to the ring of polynomials $\mathbb{C}[x]$, which is a ring of functions on the affine line $\mathbb{A}^1_{\mathbb{C}}$ (this is an algebro-geometric notation for the space of complex numbers $\mathbb{C}$, thought of as a one-dimensional "line" since it has dimension 1 over $\mathbb{C}$). We detail the facets of this analogy in the following table:

Hensel's analogy	
$\mathbb{C}[x]$, as functions on $\mathbb{A}^1_{\mathbb{C}}$	$\mathbb{Z}$, as functions on $\{p \in \mathbb{N} : p \text{ is prime}\}$
Evaluation: given $f \in \mathbb{C}[x]$ and $c \in \mathbb{C}$, $f(c)$ can be identified with the image of x under the quotient $\mathbb{C}[x] \to \mathbb{C}[x]/(x-c) \cong \mathbb{C}$.	The "evaluation" of $n \in \mathbb{Z}$ at the "point" p is its image under the quotient $\mathbb{Z} \to \mathbb{Z}/p$
$\mathbb{C}(x) = \{\frac{f}{g} : f, g \in \mathbb{C}[x]\}$, as *rational* functions on $\mathbb{A}^1_{\mathbb{C}}$.	$\mathbb{Q} = \{\frac{n}{m} : n, m \in \mathbb{Z}\}$, as "rational functions" on $\{p \in \mathbb{N} : p \text{ is prime}\}$
Laurent series expansion of a rational function $h = \frac{f}{g}$ around a point $c \in \mathbb{C}$, of the form $\sum_{i=n_0}^{\infty} b_i(x-c)^i$.	p-adic expansion of a rational number $a = \frac{n}{m}$ around a "point" p prime, of the form $\sum_{i=n_0}^{\infty} b_i p^i \in \mathbb{Q}_p$
The nth partial sums of the Laurent series of h is the best approximation of h around c by a rational function of degree n.	The nth partial sum of the p-adic expansion of a is congruent to a mod p^n.
If $\sum_{i=n_0}^{\infty} b_i(x-c)^i$ is the Taylor expansion of h, with $b_{n_0} \neq 0$, then h vanishes at c with order n_0.	If $\sum_{i=n_0}^{\infty} b_i p^i$ is the p-adic expansion of a with $b_{n_0} \neq 0$, then a vanishes at p with order n_0.

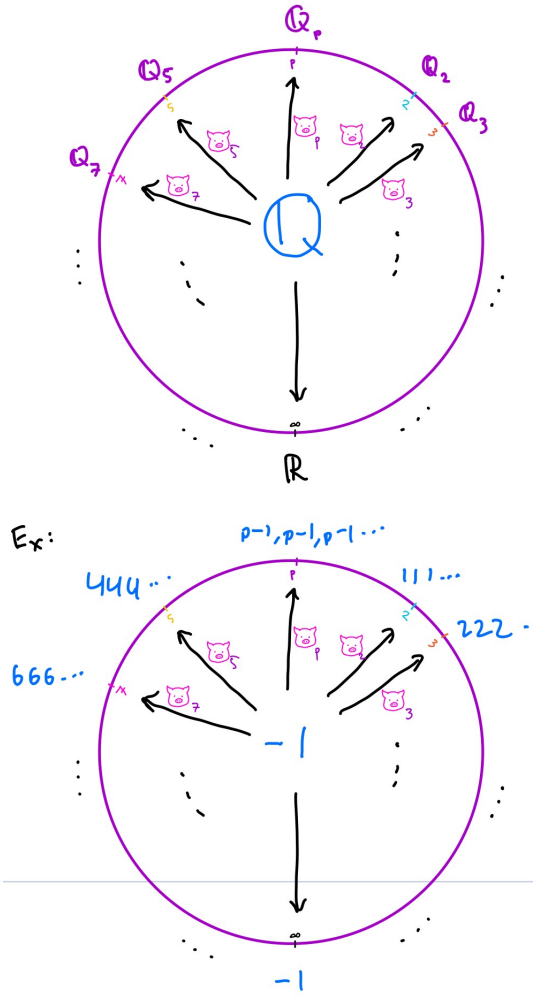
To add to this analogy, we think of ∞ as another place on which elements of $\mathbb{Q}$ can be evaluated, and of the embedding $\mathbb{Q} \to \mathbb{R}$ as the expansion around infinity. We use p to refer to either a prime number or infinity.

4.2 Local-to-global

Along these lines, we can think of the natural map

$$loc : \mathbb{Q} \to \prod_{p \leq \infty} \mathbb{Q}_p$$

as recording the "local behavior" of "functions" $a \in \mathbb{Q}$ at all "points" p, including $p = \infty$.

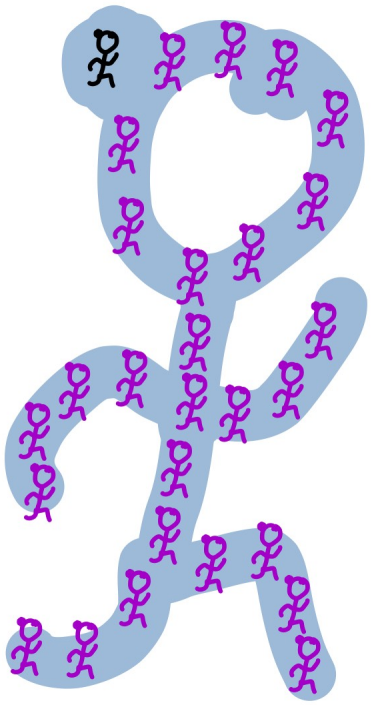


Similarly, if $f \in \mathbb{Q}[X_1, ..., X_n]$ and there is some $v = (x_1, ..., x_n) \in \mathbb{Q}^n$ such that $f(v) = 0$, then $f(v_p) = 0$ for all $p \leq \infty$, where v_p is the image of v in $\mathbb{Q}_p^n$. So a "global" root of f gives "local" roots of f for all p. But can we go the other way around? This is the philosophy of the Local-Global Principle:

Principle 4.1 Local-Global Principle

The existence of solutions in $\mathbb{Q}$ of $f \in \mathbb{Q}[X_1, ..., X_n]$ can be determined by studying solutions of f in $\mathbb{Q}_p \forall p \leq \infty$.

Can we always piece together the p-atalantas into a $\mathbb{Q}$-atalanta?



There are many reasons we would like to be able to do this, aside from just drawing fun pictures. We now have many tools to determine if there are solutions over $\mathbb{R}$ or over $\mathbb{Q}_p$. Over $\mathbb{R}$, we can look at things like discriminant of a quadratic equation, degree, sign, etc. And over $\mathbb{Q}_p$, we can scale so that the coefficients are in $\mathbb{Z}_p$ and use Hensel's lemma to reduce to studying roots over $\mathbb{Z}/p\mathbb{Z}$.

Unfortunately, as you will see in the problem set, the local-global principle does not hold in general...

4.3 Salvaging Local-Global

We start by introducing a useful tool that relates $\mathbb{Q}$ and $\mathbb{Q}_p$ for $p \leq \infty$.

Theorem 4.2 (Weak) Approximation Theorem

Let $V \in \{p \in \mathbb{Z} : p \text{ prime }\} \cup \{\infty\}$ and let S be a finite subset of V. Then the image of $\mathbb{Q}$ in

$$loc_S : \mathbb{Q} \to \prod_{p \in S} \mathbb{Q}_p$$

is dense.
That is, for any $(x_p)_{p\in S} : x_p \in \mathbb{Q}_p$ and any $(\epsilon_p)_{p\in S} : \epsilon_p \in \mathbb{R}_{>0}$, there exists $x \in \mathbb{Q}$: $|x_{xp}|_p < \epsilon_p$ for all $p \in S$.

Proof: Suppose $S = \{\infty, p_1, ..., p_n\}$ with p_i distinct, and let $(x_\infty, x_1, ..., x_n) \in \mathbb{R} \times \mathbb{Q}_{p_1} \times ... \times \mathbb{Q}_{p_n}$. By scaling by an appropriate integer (product of powers of p_is) we may assume that $x_i \in \mathbb{Z}_{p_i}$ for all $1 \leq i \leq n$.

We want to show that for all $\epsilon > 0$ and $\in \mathbb{N}$ there exists $x \in \mathbb{Q}$ such that

$$|x - x_\infty|_\infty \leq \epsilon \text{ and } v_{p_i}(x - x_i) \geq N \quad \forall 1 \leq i \leq n.$$

By Sun Tzu Remainder Theorem (commonly referred to as Chinese Remainder Theorem), there exists $\tilde{x} \in \mathbb{Z}$ such that $\tilde{x} \equiv \bar{x_i} \pmod{p_i^N}$ for all $1 \leq i \leq n$. This $\tilde{x}$ is sufficiently close to the elements x_i for the finite primes, but we need to adjust it so it is sufficiently close to x_∞ in the archimedean metric.

Let $q \in \mathbb{Z}_{>0}$ such that $p_i \nmid q$ for any i. Choose $a, m \in \mathbb{Z}$ such that

$$|\tilde{x} - x_\infty + \frac{a}{q^m} p_1^N \cdots p_n^N| \leq \epsilon$$

and let $x = \tilde{x} + \frac{a}{q^m} p_1^N \cdots p_n^N$. □

Now for some great news!

Theorem 4.3 Hasse–Minkowski Theorem

Let $F(X_1, ..., X_n) \in \mathbb{Q}[X_1, ..., X_n]$ be a quadratic form. Then

$$F(X_1, ..., X_n) = 0$$

has nontrivial solutions in $\mathbb{Q}$ if and only if it has nontrivial solutions in $\mathbb{Q}_p$ for all $p \leq \infty$.

Before we get into the proof, we present an application:

Question 4.4

For which $a, b, c, \in \mathbb{Q}$ does

$$aX^2 + bY^2 + cZ^2 = 0$$

have a nontrivial solution?

By Hasse–Minkowski, it suffices to determine for which a, b, c the form has nontrivial roots locally for all p.

To start putting some constraints on a, b, c, we simplify the polynomial. Let

$$f(X, Y, Z) = aX^2 + bY^2 + cZ^2$$

Then if $d \neq 0$, $f(x, y, z) = 0$ if and only if $d \cdot f(x, y, z) = 0$ so we can assume $a, b, c \in \mathbb{Z}$ with no common factors. We can even assume that a, b, c are pairwise relatively prime–check this! The proof has some elements in common with irrationality of root 2, so don't try this on a boat!

Next, if $a = a_1 a_2^2$, then (x, y, z) is a root of f if and only if $(a_2 x, y, z)$ is a root of $a_1 X^2 + bY^2 + cZ^2$, so we can assume a, b, c are squarefree.

So now lets consider some local cases. Since negative numbers don't have square roots in $\mathbb{R}$, there is a root of f if and only if a, b, c do not all have the same sign.

Now suppose p is an odd prime not dividing a, b, or c. We look at this equation mod p and use Hensel's lemma.

Lemma 4.5

If p is an odd prime not dividing a, b, or c, there exist integers x_0, y_0, z_0 not all divisible by p such that

$$ax_0^2 + by_0^2 + cz_0^2 \equiv 0 \pmod{p}.$$

Proof of lemma: in fact, we will find a solution with $z_0 = 1$, so a solution to

$$ax_0 + by_0^2 + c \equiv 0 \pmod{p}.$$

This is equivalent to solving

$$ax_0 = -by_0^2 - c \equiv 0 \pmod{p}.$$

Since there are $(p + 1)/2$ squares mod p and a, b are invertible mod p, there are $(p + 1)/2$ possible congruence classes for the left side of the above equation as x_0 ranges over elements

of $\mathbb{Z}/p\mathbb{Z}$ and $(p+1)/2$ congruence classes that can occur on the right. Hence there must be some overlap, proving the lemma $\square$

Now I claim we can lift this to a root of f in $\mathbb{Z}_p$. We can use Hensel's Lemma, but that's only for single variable polynomials, so we suppose WLOG that $x_0 \neq 0 \pmod{p}$ and define

$$g(X) = aX^2 + by_0^2 + cz_0^2.$$

Then Hensel's lemma applied to g (check the conditions for this!!) implies there exists $x \in \mathbb{Z}_p$ such that $g(x) = 0$, so (x, y_0, z_0) is a root of f in $\mathbb{Q}_p$.

Now let's find sufficient conditions for existence of a root in $\mathbb{Q}_2$, and suppose we are in the case where a, b, c are all odd.

If we have a root $(x, y, z) \in \mathbb{Q}_2^3$ of f, we can suppose $x, y, z, \in \mathbb{Z}_p$ and one of x, y, z has absolute value 1, scaling by the appropriate power of 2 if necessary. So we may now look at f mod 2; we see that

$$0 \equiv ax^2 + by^2 + cz^2 \equiv x^2 + y^2 + z^2 \pmod{2}.$$

WLOG, suppose $y \equiv z \equiv 1 \pmod{2}$ and $x \equiv 0 \pmod{2}$. Then $y^2 \equiv z^2 \equiv 1 \pmod{4}$ and $x^2 \equiv 0 \pmod{4}$. So

$$b + c \equiv 0 \pmod{4}.$$

Hence, if there is a root of f over $\mathbb{Q}_2$, two of a, b, c sum to 0 mod 4.

The rest of the classification can be stated as follows, and its completion is an exercise in this week's problem set:

Theorem 4.6

Suppose $a, b, c \in \mathbb{Z}$ are relatively prime and squarefree. Then

$$aX^2 + bY^2 + cZ^2 = 0$$

has a nontrivial solution in $\mathbb{Q}$ if and only if all of the following hold:

1. a, b, c do not all have the same sign
2. if $p \mid a$ and $p \neq 2$, there exists $r \in \mathbb{Z}$ such that $b + r^2 c \equiv 0 \pmod{p}$ (similarly for b, c)
3. if $2 \nmid abc$, then two of a, b, c sum to 0 mod 4
4. if $2 \mid a$ then $8 \mid b + c$ or $8 \mid a + b + c$ (similarly for b, c)

4.4 Proof of Hasse–Minkowski

Quadratic forms of rank 2 and 4 were covered in Professor Chan's lecture. We begin by proving the theorem for rank 3 quadratic forms, following a proof due to Legendre.

Arizona Winter School is all about acquainting students with cutting-edge research; in the spirit of this, here is a result from 2005. For centuries it was conjectured (actually assumed!) that the mathematician Adrien-Marie Legendre was this guy:

You may see his picture in many textbooks! In 2005, this conjecture was shown to be false (the above guy is just an unrelated French politician whose last name is Legendre); the only known depiction left of our very own Legendre is the following:

by caricature artist Julien-Léopold Boilly, whose other delightful caricatures you should defintely check out.

Back to the proof for when $n = 3$: suppose that f is of the form $aX^2 + bY^2 + cZ^2$ with $a, b, c \in \mathbb{Q}^\times$, and suppose that for each $p \leq \infty$, there exists $v_p := (x_p, y_p, z_p) \in (\mathbb{Q}_p)^3$ such that $f_p(x_p, y_p, z_p) = 0$.

First, a couple simplifications: since $f_p(v_p) = 0$ if and only if $a^{-1}f_p(v_p) = 0$, we may assume $a = 1$, that is, $f = X^2 - bY^2 - cZ^2$ Also, if $b = b_1 b_2^2$ for some $b_1, b_2 \in \mathbb{Q}$, then

$$f_p(v_p) = (x_p)^2 + b(y_p)^2 + c(z_p)^2 = (x_p)^2 + b_1(b_2 y_p)^2 + c(z_p)^2$$

so we may replace b by b_1 and thus assume b, and similarly c, are squarefree integers. Without loss of generality, assume also that $|b| \leq |c|$.

We now induct on $m = |b| + |c|$. The base case is $m = 2$, meaning $f = X^2 \pm Y^2 \pm Z^2$.

We can ignore the case $f = X^2 + Y^2 + Z^2$ since it has no nonzero root over $\mathbb{R} = \mathbb{Q}_\infty$. We are left with two cases up to symmetry: $f = X^2 + Y^2 - Z^2$ and $f = X^2 - Y^2 - Z^2$, both of which have a zero at $(X, Y, Z) = (1, 0, 1)$ over any field.

Now suppose $m > 2$. We will reduce the problem to one with a smaller value of m. First note that, since $m > 2$ and $|b| \leq |c|$, we must have $|c| \geq 2$. Let p be a prime dividing c. We

will show that b is a square mod p. Indeed, suppose we have a nontrivial zero (x_p, y_p, z_p) of f_p in $\mathbb{Q}_p$. We can assume that b is not 0 mod p, otherwise it is trivially a square mod p. We can further assume by scaling (x_p, y_p, z_p) by an appropriate scalar that $x_p, y_p, z_p \in \mathbb{Z}_p$ and that one of these numbers has absolute value 1 in $\mathbb{Q}_p$. We now consider the equation $f(x_p, y_p, z_p) = 0 \bmod p\mathbb{Z}_p$, which gives us

$$x_p^2 - by_p^2 \equiv 0 \pmod{p}$$

We note that y_p is not divisible by p. If it were, then x_p would be divisible by p, hence cz_p^2 must be divisible by p^2. Since c is squarefree, z_p would need to be divisible by p, contradicting our assumption that one of x_p, y_p, z_p has absolute value 1. Thus y_p is invertible mod p and we have

$$b \equiv (\frac{x_p}{y_p})^2 \pmod{p}$$

showing that b is indeed a square mod p.

Now, since c is squarefree, it follows from the Sun Tzu Remainder Theorem that $\mathbb{Z}/c\mathbb{Z} \cong \Pi_i(\mathbb{Z}/p_i\mathbb{Z})$, where this product ranges over all prime factors p_i of c. Since b is a square mod each of these primes, it must therefore be a square mod c.

So we can write $b = t^2 - c\tilde{c}$ for some $t, \tilde{c}$ with $|t| \leq \frac{|c|}{2}$. So $\tilde{c}c = t^2 - b$. Let k denote a field which is either $\mathbb{Q}$ or $\mathbb{Q}_p$, for $p \leq \infty$. Using the Hilbert symbol notation from (Chan 3.4), we see that $(b, \tilde{c}c) = 1$ in k, since $(t, 1, 1)$ is a zero of f. By the bimultiplicative property of the Hilbert symbol, $(b, \tilde{c})(b, c) = 1$. By definition of the Hilbert symbol, this means that the original quadratic form f has a nontrivial zero in k if and only if the modified quadratic form

$$h = X^2 - bY^2 - \tilde{c}Z^2$$

has a nontrivial zero in k.

Note that $|\tilde{c}| = \frac{t^2-b}{c} \leq \frac{|c|}{4} + 1 < |c|$ since $|c| \geq 2$.
Finally, we let $\tilde{c} = \gamma u^2$ with γ square-free. Then the quadratic form

$$g = X^2 - bY^2 - \gamma Z^2$$

has a nontrivial root in k if and only if g does if and only if f does, for $k = \mathbb{Q}$ or $\mathbb{Q}_p$ for any $p \leq \infty$.
Thus, by assumption g has nontrivial roots over $\mathbb{Q}_p$ for any p, and so by induction it has a nontrivial root over $\mathbb{Q}$, so that f has a nontrivial root over $\mathbb{Q}$, as desired.

Now suppose that the rank of f is greater than or equal to 5. We now proceed by induction on the rank.

We write $f = h - g$, where $h = a_1X_1^2 + a_2X_2^2$ and $g = -(a_3X_3^2 + \cdots + a_nX_n^2)$. Let S be the set of places $S = \{\infty\} \cup \{2\} \cup \{p \text{ prime} : |a_i|_p \neq 1 \text{ for some } i \geq 3\}$. Importantly, S is finite.

Let p be a prime or ∞. By our hypothesis there exists some choice $x_{1,p}, \ldots, x_{n,p} \in \mathbb{Q}_p$ and some $c_p \in \mathbb{Q}_p$ such that

$$h(x_{1,p}, x_{2,p}) = c_p = g(x_{3,p}, \ldots, x_{n,p})$$

Let $\mathbb{Q}_p^{\times 2}$ denote $\{y^2 : y \in \mathbb{Q}_p^\times\}$. It is an exercise to check that $\mathbb{Q}_p^{\times 2}$ is open in $\mathbb{Q}_p$ (Hint: Hensel's lemma). Thus, the weak approximation Theorem, together with the continuity of h, guarantees that there exist some $(x_1, x_2) \in \mathbb{Q}$ such that $\frac{h(x_1,x_2)}{c_p} \in \mathbb{Q}_p^{\times 2}$ for all $p \in S$. Given such a choice of x_1, x_2, let $c = h(x_1, x_2)$. Then $h = c$ has a nontrivial solution in $\mathbb{Q}_p$ for all $p \in S$.

Let $f_1 := cZ^2 - g$. Then $f_1 = 0$ has a nontrivial root in $\mathbb{Q}_p$ for $p \in S$. And if $p \notin S$, the coefficients of the discriminant $d_p(g)$ are units, so $\epsilon_p(g) = 1$ (See Chan for definitions of the discriminant and Hasse invariant ϵ)

Hence f_1 has a nontrivial zero in $\mathbb{Q}_p$ for ALL $p \leq \infty$!

By induction, f_1 has a nontrivial 0 in $\mathbb{Q}$ so $g = c$ has a nontrivial solution in $\mathbb{Q}$, so $f = 0$ has a nontrivial solution in $\mathbb{Q}$.