Explicit Methods for Solving Diophantine Equations

by Henri Cohen

The aim of this course is to show through examples the wide variety of methods with which Diophantine equations can be attacked, most of which being amenable to computer implementation.

• We will begin by local methods, which have several advantages: they give an easy way to see whether an equation has no solutions at all, they give information on possible solutions, and they are algorithmically implementable. As interesting examples of these methods we will consider Fermat quartics and the first case of Fermat's last theorem. As prerequisite it would be useful to have a small amount of familiarity with p-adic numbers.

• Naïve factorization over $\mathbb{Z}$: this rarely works, but we will show on the example of the first case of Fermat's last theorem and on Catalan's equation that it can give highly nontrivial results.

• Factorization of the equation over a number field. This is the most classical method, originating with Kummer, and we will spend some time on it. The prerequisites are here the basics of algebraic number theory: ring of integers, prime ideal factorization, and Dirichlet's theorems on the class and unit groups. A huge amount of examples can be treated, but we will choose them among Fermat's last theorem for regular exponents, the super-Fermat equation, the equation $y^2 = x^n + t$, and Fermat quartics.

• Descent on elliptic curves: both 2 and 3-descent can be treated explicitly. Time permitting, I would like to explain 3-descent and its application to Fermat cubics.

• The search for integral points on elliptic curves has now become almost algorithmic if the *rational* points are known, through the use of elliptic logarithms. This topic will be mentioned if there is time.

• The use of L functions, and especially the Heegner point method for finding rational points on elliptic curves. This is one of the most fascinating algorithms since it enables to find points of very large height quite easily, in a manner analogous to the resolution of the Pell–Fermat equation. Although everything will be defined and theorems stated, it will be useful to have some additional prerequisites for this: imaginary quadratic fields, modular functions, the Weierstrass $\wp$-function, some basic knowledge of complex multiplication.

• "Modern" methods such as the resolution of Thue equations, finding rational points on curves of higher genus, or the Ribet–Wiles modular method for solving Fermat-type equations will be briefly mentioned, but it will be impossible to go into these subjects.

Of course, many projects can be suggested in the wide domain of Diophantine equations. I suggest a project centered around the Heegner point techniques. This is the object of current research by John Cremona, Christophe Delaunay, and Mark Watkins, among others. As mentioned above, this quite "magical" method is essentially the only one known for *constructing* from scratch solutions to a Diophantine equation (together with the much more down to earth continued fraction method for solving Pell–Fermat equations). This project involves the following:

• Elementary aspects of the theory of complex multiplication, and in particular of Shimura's reciprocity law.

• Basic theory of modular forms over $\Gamma_0(N)$, and in particular of their associated L-functions.

• The modular parametrization of an elliptic curve defined over $\mathbb{Q}$.

• The theorem of Gross–Zagier.

For all the above, only the results and their uses will be necessary, and evidently none of the proofs.

• Writing a detailed algorithm for finding Heegner points based on the above theoretical material.

• A detailed analysis of the running time of this algorithm, of the necessary accuracy for the computations, of the bottlenecks, and of the numerous tricks which can be used to remove the bottlenecks as much as possible.

• For the computationally oriented students, an actual computer implementation of the algorithm, together with large examples and time comparisons using some of the tricks mentioned above.

As literature for the course and the project I will distribute extracts from a 1100 page book that will be published by Springer in 2006. Most of the prerequisites are very classical and can be found in any good number theory book, for instance Borevitch–Shafarevitch.

Specifically for the project, I suggest the following reading matter (in which there is much more than necessary):

J. Cremona, *Computing the degree of the modular parametrization of a modular elliptic curve*, Math. Comp. **64** (1995), 1235–1250.

H. Darmon, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Math. **101** (2004), American Math. Soc., also available on the author's web page.

B. Gross, *Heegner points on* $X_0(N)$, in Modular forms, edited by R. Rankin (1984), 87–105.

D. Zagier, *Modular parametrizations of elliptic curves*, Canad. Math. Bull. **28** (1985), 372–384.