The complexity of Diophantine equations

Colloquium
McMaster University
Hamilton, Ontario
April 2005

The basic question

A Diophantine equation is a polynomial equation $f(x_1, \ldots, x_n) = 0$ with integer coefficients, for which one seeks rational or *integer* solutions.

Question. Given a diophantine equation, how hard is it to find a solution?

Matijasevich. This problem of determining the *existence* of a solution is undecidable in general.

It is natural to try to develop theories for more restricted classes.

The size of a Diophantine equation

If $a/b \in \mathbf{Q}$, $\mathsf{Height}(a/b) := \mathsf{h}(a/b) = \log(ab)$.

$$\mathsf{h}((x_1, \ldots, x_n)) = \mathsf{h}(x_1) + \cdots + \mathsf{h}(x_n).$$

If $f = \sum_J a_J x^J$ is a diophantine equation,

$$\mathsf{h}(f) = \sum_J \mathsf{h}(a_J).$$

The height of an equation is, roughly speaking, the amount of paper required to write it down.

Complexity

Definition A class $\mathcal{C}$ of equations is said to be *strictly polynomial* if there is an $n \geq 1$ and an algorithm which for each equation $E \in \mathcal{C}$ produces a solution to E in at most $\mathsf{h}(E)^n$ operations.

Less formally: the time required to find a solution for E is *roughly equivalent* to the time it takes to write E down.

Some examples

The following (not very interesting!) classes of Diophantine equations are strictly polynomial:

$$\mathcal{C} = \{\text{Equations in one variable}\}$$

$$\mathcal{C} = \{\text{ systems of linear equations}\}$$

Question. Are there *any* other naturally occuring classes of non-linear Diophantine equations in more than one variable which are strictly polynomial?

Factorisation

Consider

$$\text{FACT} := \{xy = n,\ x, y \neq \pm 1; \quad \text{as } n \in \mathbf{Z}\}.$$

Conjecture The class FACT is *not* strictly polynomial.

Much of modern cryptography rides on this conjecture, although it seems difficult to prove.

Conics

Consider

CONICS $= \{ax^2 + by^2 + cz^2 = 0, \text{ as } a, b, c \in \mathbf{Z}\}$

Theorem (Hasse-Minkowski) Suppose given an *oracle* for extracting the square root of m modulo n in time which is polynomial in $\log(n)$. Then CONICS is strictly polynomial.

Sketch of proof

1. Find $\lambda_a, \lambda_b, \lambda_c \in \mathbf{Z}$ such that

$$\lambda_a^2 = -b/c \pmod{a}, \quad \lambda_b^2 = -a/c \pmod{b},$$

$$\lambda_c^2 = -a/b \pmod{c}.$$

2. Let $\Lambda =$ set of $(x, y, z) \in \mathbf{Z}^3$ with

$$z = \lambda_a y \pmod{a}, \quad z = \lambda_b x \pmod{b},$$

$y = \lambda_c x \pmod{c}$, plus parity conditions.

$$(x, y, z) \in \Lambda \Rightarrow ax^2 + by^2 + cz^2 = 0 \pmod{4abc}.$$

Sketch of proof (cont'd)

3. Find a short vector $(x_0, y_0, z_0) \in \Lambda$.

This is similar to a gcd calculation, and can be done very fast (in polynomial time).

4. Geometry of numbers:

$$4abc \text{ divides } |ax_0^2 + by_0^2 + cz_0^2| < 4abc$$

hence $ax_0^2 + by_0^2 + cz_0^2 = 0$.

This algorithm for finding (x_0, y_0, z_0) works in time which is polynomial in $\log(abc)$.

Applications

Theorem The classes

•$\text{CONICS}_{a,b} := \{ax^2 + by^2 + pz^2 = 0, \quad p \text{ prime}\}$

•$\text{2SQUARES} := \{x^2 + y^2 = p, \quad p \text{ prime}\}$;

are strictly polynomial.

Question. Are there classes of Diophantine equations which can be proved to *not* be strictly polynomial?

Pell's Equation

Fermat's "favorite" Diophantine equation:

$$\text{PELL} := \{x^2 - dy^2 = 1, \text{ as } d \in \mathbf{Z}\}.$$

Group law:

$$(x_1, y_1) \star (x_2, y_2) := (x_1x_2 + dy_1y_2, x_1y_2 + y_1x_2).$$

Fundamental solution: $(\pm x, \pm y) = (x_*, y_*)^{\star k}$.

Theorem. The class PELL is not strictly polynomial.

“Proof”

Here are some fundamental solutions.

$d = 2$. $x = 3$, $y = 2$.

$d = 61$.
$x = 1766319049$,
$y = 226153980$.

$d = 109$.
$x = 158070671985249$,
$y = 15140424455100$.

$d = 991$.
$x = 379516400906811930638014896080$,
$y = 12055735790331359447442538767$.

Induction (à la Fermat): $\mathrm{h}(x_0, y_0)$ can be as large as $\sqrt{d}$.

Hence merely writing down the fundamental solution can take as many as $\sqrt{d} >> \log(d)^n$ operations.

Polynomial complexity

Problem P(E,h). Given $E \in \mathcal{C}$ and $h >> \mathrm{h}(E)$, (more precisely: $h > \exp(\mathrm{h}(E))$) find a solution x of E with $\mathrm{h}(x) < h$, if it exists, or terminate with an appropriate message, otherwise.

Obvious algorithm: run over all solutions with height $\leq h$ until a solution is found (or not).

This requires a number of operations which is *exponential* in h.

Definition. A class $\mathcal{C}$ of Diophantine equations is said to be *solvable in polynomial time* if there is $n \in \mathbf{N}$ and an algorithm that solves $P(E, h)$ in at most h^n operations.

Less formally: the time required to find a *large* solution for E is *roughly equivalent* to the time it takes to write the solution down.

Caveat: FACT is *trivially* solvable in polynomial time according to this definition.

Pell's equation

Theorem The class PELL is solvable in polynomial time.

Algorithm for computing (x_*, y_*): the *continued fraction method*.

$$\sqrt{d} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}$$

$$\frac{x_n}{y_n} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots + \frac{1}{a_n}}}.$$

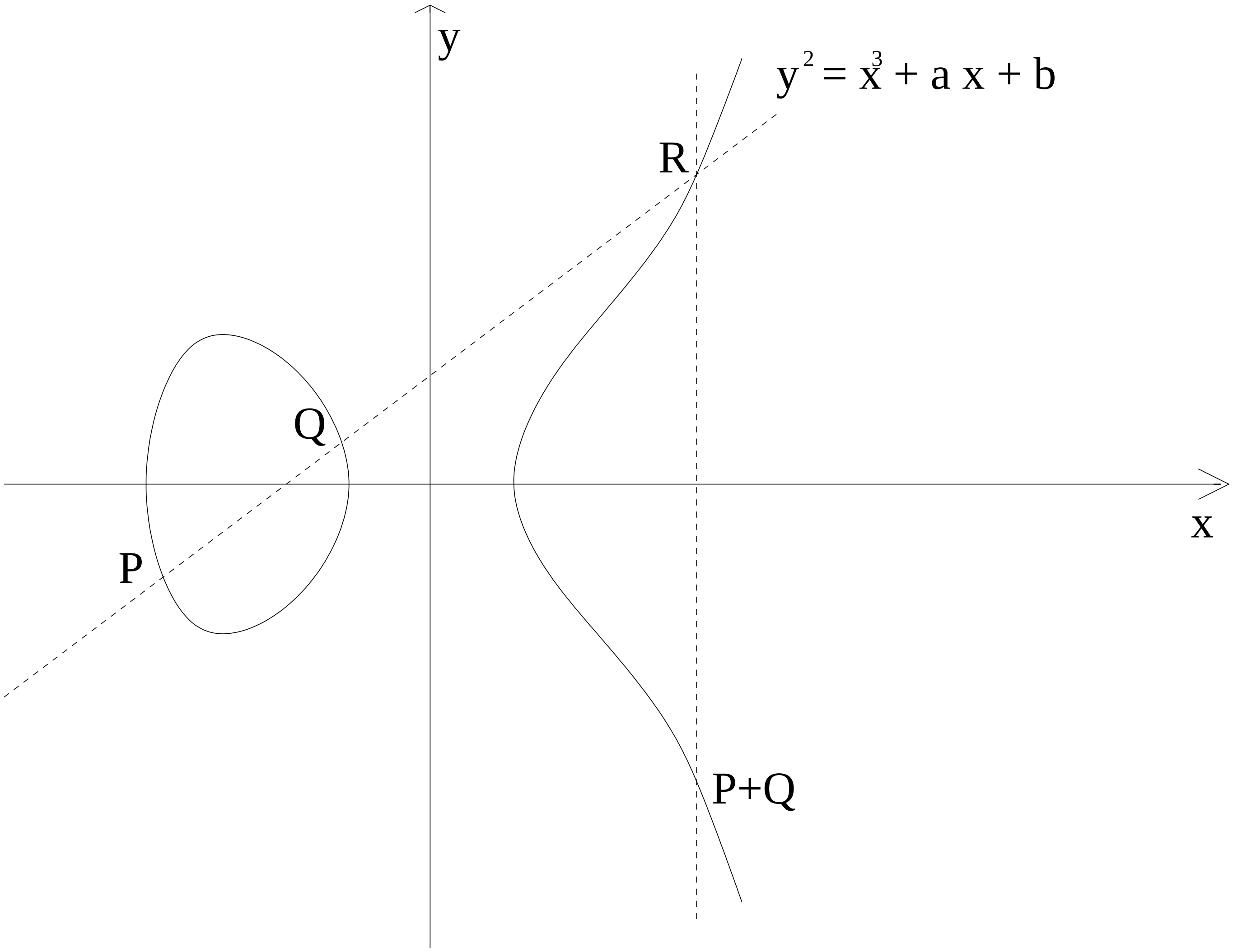
For $n >> 0$, $(x_n, y_n) = (x_*, y_*)$.

This approach requires $O(\log(x_*))$ operations.

Elliptic curves

The class

$$\mathsf{ELL} := \{y^2 = x^3 + ax + b, \quad a, b \in \mathbf{Q}\}.$$



The addition law on an elliptic curve

The Mordell-Weil theorem

Theorem. The set $E(\mathbf{Q})$ is a *finitely generated* abelian group.

$$E(\mathbf{Q}) = T \oplus \mathbf{Z}^r, \quad r \geq 0.$$

Question. Is there an algorithm to compute $E(\mathbf{Q})$ given E?

The answer is not known! (It is related to the Shafarevich-Tate conejcture, and the Birch and Swinnerton-Dyer conjecture.)

Related Question Is ELL solvable in polynomial time?

This question might seem more approachable to the uninitiated.

A conjecture/provocation

Conjecture The class ELL of elliptic curve equations is solvable in polynomial time.

This conjecture asserts that it should be possible to "zero in" on solutions to elliptic curve equations much more rapidly than by performing an exhaustive search.

It appears to be intimately connected to the Birch and Swinnerton-Dyer conjecture.

An example of Bremner and Cassels

The elliptic curve

$$E : y^2 = x^3 + 877x$$

has rank one and generator given by:

$$x = \frac{612776083187947368101^2}{7884153586068390021 0^2}$$

$$y = \frac{\begin{array}{r}256256267988926809388 77\\ 6834045513089648669 1\\ 5320435660346478694 9\end{array}}{7884153586068390021 0^3}$$

Another example

Consider the equation

$$101y^2 = x^3 - x^2 - 10x - 19/4.$$

The smallest solution has

$$x = \frac{10816241366446925396670846851 16849}{246846541822770321447579971520100}$$

This solution was found on a computer in a few seconds.

The Hasse-Weil L-series

Let N :=Conductor(E), and define

$$a_p := \begin{cases} p+1-\#E(\mathbf{Z}/p\mathbf{Z}) & \text{if } p \not| N; \\ 0,1, \text{ or } -1 & \text{if } p|N. \end{cases}$$

$$a_{p^n} = a_p a_{p^{n-1}} - p a_{p^{n-2}},$$

$$a_{rs} := a_r a_s, \quad (r,s) = 1.$$

Hasse-Weil L-function attached to E:

$$L(E,s) = \sum_n a_n n^{-s} = \prod_p (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

$$L(E,1) \text{``}=\text{''} \prod_p \frac{p}{\#E(\mathbf{Z}/p\mathbf{Z})}.$$

The Hasse-Weil L-series is expected to encode arithmetic information about E, notably its rank.

The Birch and Swinnerton-Dyer conjecture

Conjecture. The L-function $L(E,s)$ extends to an analytic function of $s \in \mathbf{C}$, and

$$\text{rank}(E(\mathbf{Q})) = \text{ord}_{s=1} L(E,s).$$

The leading term of $L(E,s)$ is also expected to be expressible in terms of the heights of the generators of $E(\mathbf{Q})$, and of the *conjecturally finite* Shafarevich-Tate group.

Tate (1974) "... this remarkable conjecture relates the behaviour of a function L at a point where it is at present not known to be defined to the order of a group $Ш$ which is not known to be finite."

Modularity

Problem: Give a "closed formula" for the a_n?

Consider the generating series:

$$f_E(q) := \sum_{n=1}^{\infty} a_n q^n, \quad q := e^{2\pi i \tau}.$$

Hecke's congruence group:

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbf{Z}) \ \text{ s.t. } N|c \right\}.$$

Definition. A *modular form* of weight k and level N is a function

$$f(z) = \sum_{n=0}^{\infty} b_n e^{2\pi i n z}$$

such that

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z),$$

$$\text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

Wiles' Theorem

Theorem (Wiles) The generating function $f_E(z)$ is a modular form of weight 2 and level N.

First consequence:

The Hasse-Weil L-series

$$L(E,s) = (2\pi)^s \Gamma(s)^{-1} \int_0^\infty f(it) t^s \frac{dt}{t}$$

extends to an analytic function of $s \in \mathbf{C}$. Hence the left-hand side of the BSD conjecture makes sense!

Modular parametrisations

Second consequence:

Let

$$\exp_E : \mathbf{C} \longrightarrow E(\mathbf{C})$$

be the Lie exponential. There exists $\lambda \in \mathbf{C}^\times$ such that

$$\Phi(\tau) := \exp_E \left(\lambda \int_{i\infty}^{\tau} f(z) dz \right)$$

descends to a well-defined analytic map

$$\boxed{\Phi : \mathcal{H}/\Gamma_0(N) \longrightarrow E(\mathbf{C}),}$$

called the *modular parametrisation*.

$\mathcal{H} := \{z \in \mathbf{C} \text{ s.t. } \Im(z) > 0\}$ (the Poincaré upper half-plane.)

Key remark. The map Φ can be calculated in polynomial time, in the sense that d digits of accuracy can be obtained in $O(d^n)$ operations.

The Heegner point construction

Let $\mathcal{H}'$ be a the set of $\tau \in \mathcal{H}$ which generate a *quadratic imaginary field* K: $\tau = a + b\sqrt{d}$, with $a, b, d \in \mathbf{Q}$.

Theorem. If τ belongs to $\mathcal{H} \cap K$, then $\Phi(\tau)$ belongs to $E(K^{\text{ab}})$.

$K^{\text{ab}} =$ maximal abelian extension of K.

In fact, the smallest abelian extension H_τ over which $\Phi(\tau)$ is defined can be specified explicitly.

For $\tau \in \mathcal{H}'$, define

$P_\tau := \text{trace}_{H_\tau/\mathbf{Q}}(\Phi(\tau))$

The point P_τ is called the *Heegner point* attached to τ.

Theorem. If $\text{h}(P_\tau) < h$, then P_τ can be computed in poly($\log(h)$) operations.

Main Properties

Theorem (Kolyvagin)

If $r = \text{rank}(E(\mathbf{Q})) \neq 1$, then P_τ is torsion for all τ.

Theorem (Gross-Zagier).

If $\text{ord}_{s=1} L(E, s) = 1$, then P_τ is of infinite order for infinitely many τ.

Corollary Let

$$\text{ELL}_1 := \{E \in \text{ELL s.t. } \text{ord}_{s=1} L(E, s) \leq 1\}.$$

The class ELL_1 is solvable in polynomial time.

The number field case

In contrast with ELL_1, the complexity of ELL seems very hard to study, and we find ourselves with little of interest to say about it.

We seek refuge in the *number field case*.

Let F=finite extension of $\mathbf{Q}$.

•$\mathsf{ELL}(F) :=$ {Elliptic curves over F};

•$E \in \mathsf{ELL}_1(F) \Leftrightarrow \mathrm{ord}_{s=1} L(E/F, s) \leq 1$.

Hard conjecture The class $\mathsf{ELL}(F)$ is solvable in polynomial time.

Easier conjecture The class $\mathsf{ELL}_1(F)$ is solvable in polynomial time.

Thesis. This last conjecture, while seemingly not out of reach, is worthwhile and presents many interesting challenges.

Real quadratic fields

Let F=real quadratic field.

Assume all elliptic curves over F are modular.

$\mathsf{ELL}'_1(F)$ = set of elliptic curves $E \in \mathsf{ELL}_1(F)$ such that there is a prime p of $\mathcal{O}_F$ which divides $N(E)$ exactly.

Theorem (Matt Greenberg, 2005) The class $\mathsf{ELL}'_1(F)$ is solvable in polynomial time.

The proof uses ideas arising from the theory of p-adic integration and the theory of *over-convergent p-adic modular forms* (attached to definite quaternion algebras).

What about $\mathsf{ELL}_1(F)$?

The class $\mathsf{ELL}_1(F)$

There is a *conjectural algorithm* for solving *any* equation in $\mathsf{ELL}_1(F)$ in polynomial time, which *works reasonably well in practice*.

Darmon, Logan. *Periods of Hilbert modular forms and rational points on elliptic curves.* IMRN (2003) no. 40, 2153-2180.

Useful theoretical insights about elliptic curves are to be gained by carefully considering $\mathsf{ELL}_1(F)$ for other fields F, such as the *imaginary quadratic fields*.