Modular forms and Diophantine equations

Colloquium

University of Maryland
College Park
April 2004

Pell's Equation

Fermat's "favorite" Diophantine equation:

Pell's equation $\boxed{x^2 - dy^2 = 1.}$

Group law:

$(x_1, y_1) \star (x_2, y_2) := (x_1 x_2 + d y_1 y_2, x_1 y_2 + y_1 x_2).$

Fundamental solution: $(\pm x, \pm y) = (x_0, y_0)^{\star k}$.

1. How big can (x_0, y_0) be?

2. Can one compute (x_0, y_0) efficiently?

Some fundamental solutions

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

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

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

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

Algorithms

There is a good algorithm for computing (x_0, y_0): the *continued fraction method*.

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

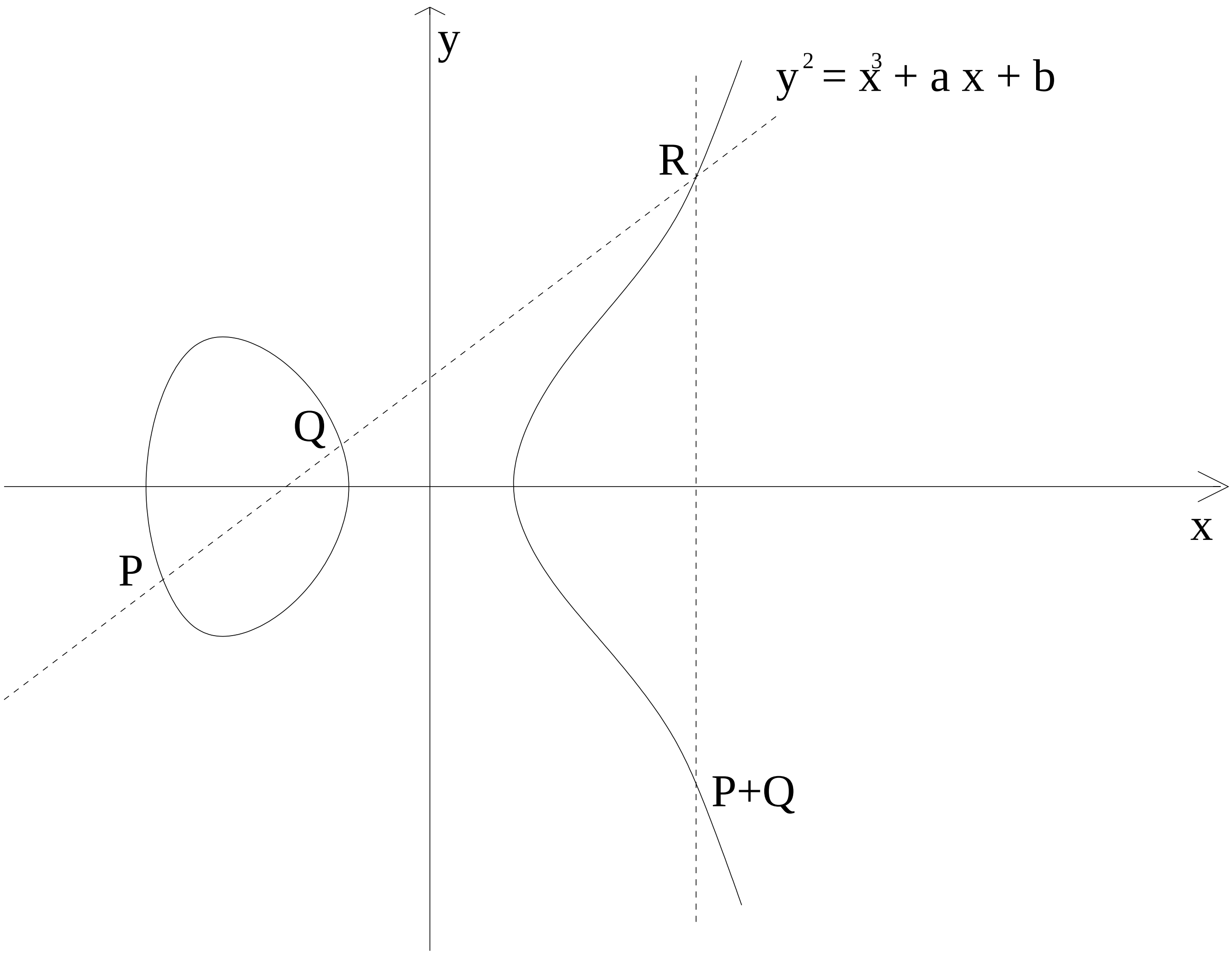
$$\frac{x_n}{y_n} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots + \frac{1}{a_n}}}.$$

For $n >> 0$, $(x_n, y_n) = (x_0, y_0)$.

This approach requires $O(\log(x_0))$ operations; since $\log x_0$ is a good measure of the size of the problem, this algorithm runs in *polynomial time*.

Elliptic curves

$$E : y^2 = x^3 + ax + b.$$



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.)

A more tractable question

Question. Given (E, M), with $M \in \mathbf{R}^{>0}$, print a point on $E(\mathbf{Q})$ of logarithmic height less than M, if such a point exists, or print "there is none" if no such point exists.

Obvious algorithm: Run over all x with $ht(x) < M$.

Complexity: exponential time!

An example of Bremner and Cassels

The elliptic curve

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

has rank one and generator given by:

$$x = \frac{612776083187947368101^2}{78841535860683900210^2}$$

$$y = \frac{\begin{array}{r}256256267988926809388776834045513089648669153204356603464786949\end{array}}{78841535860683900210^3}$$

Modularity

N :=Conductor(E).

Define

$$a_p := \begin{cases} p+1-\#E(\mathbf{Z}/p\mathbf{Z}) & \text{if } p \nmid N; \\ 0, 1, \text{ or } -1 & \text{if } p \mid N. \end{cases}$$

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

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

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

Consider the generating series:

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

Modular forms

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.

Complementary statement: 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.)

Complex Multiplication

Let $K = \mathbf{Q}(\sqrt{-D}) \subset \mathbf{C}$ be a *quadratic imaginary field*.

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.

More precise version: Given $\tau \in \mathcal{H}$ with quadratic coordinates, let

$$F_\tau(x, y) = Ax^2 + Bxy + Cy^2$$

be the smallest primitive binary quadratic form with

$$F_\tau(\tau, 1) = 0, \qquad N|A.$$

Define $\text{Disc}(\tau) := \text{Disc}(F_\tau)$.

$$\mathcal{H}^D := \{\tau \text{ s.t. } \text{Disc}(\tau) = D.\}.$$

Class Field Theory

$$G_D := \left\{ \begin{array}{c} \text{Primitive binary quadratic forms} \\ \text{of discriminant } D \end{array} \right\}.$$

This set is an *abelian group* under Gaussian composition.

Class field Theory produces a map

$$\text{rec} : G_D \longrightarrow \text{Gal}(H_D/K),$$

where

$H_D =$ ring class field of K attached to D.

The Heegner point construction

Theorem If τ belongs to $\mathcal{H}^D$, then $\Phi(\tau)$ belongs to $E(H_D)$, and the maps are compatible with the actions in the following diagram:

$$\begin{array}{ccc} G_D & \stackrel{\text{rec}}{\longrightarrow} & \mathrm{Gal}(H_D/K) \\ \circlearrowleft & & \circlearrowleft \\ \mathcal{H}^D/\Gamma_0(N) & \stackrel{\Phi}{\longrightarrow} & E(H_D) \end{array}$$

The interests of this construction

$\boxed{\text{1. Constructing points on } E(\mathbf{Q})}$

$$P_D := \text{Trace}_{H_D/\mathbf{Q}}(\Phi(\tau)), \quad \tau \in \mathcal{H}^D.$$

Theorem (Kolyvagin) If $r = \text{rank}(E(\mathbf{Q})) \neq 1$, then P_D is torsion.

Theorem (Gross-Zagier). Assume the Birch and Swinnerton-Dyer conjecture. If $r = 1$, then P_D is of infinite order.

$\boxed{\text{2. Constructing abelian extensions}}$

$\mathbf{Q}^{\text{ab}} = \cup_{\alpha \in \mathbf{Q}} \mathbf{Q}(e^{2\pi i \alpha})$,

$K^{\text{ab}} \simeq \cup_{\substack{\alpha \in \mathbf{Q} \\ \tau \in \mathcal{H} \cap K}} K(e^{2\pi i \alpha}, j(\tau))$,

where j= the j-function on $\mathcal{H}/\mathbf{SL}_2(\mathbf{Z})$.

Natural question: What if K is *real* quadratic?

Real quadratic fields

There is no known "explicit class field theory" for real quadratic fields.

Goal: To extend, at least *conjecturally*, the theory of complex multiplication, and the Heegner point construction, to real quadratic fields.

Ingredients:

1. p-adic analysis.

2. p-adic variation of modular forms ("Hida theory").

p-adic analysis

Assume E has conductor $N = pM$, with $p \nmid M$.

$\mathbf{Q}_p :=$ completion of $\mathbf{Q}$ for the p-adic metric.

$\mathbf{C}_p :=$ completion of $\bar{\mathbf{Q}}_p$.

$\mathcal{H}_p := \mathbf{C}_p - \mathbf{Q}_p$. (The p-adic analogue of $\mathcal{H}$)

Fix K a real quadratic field, embedded both in $\mathbf{R}$ and $\mathbf{C}_p$.

Motivation for p-adic analysis: $\mathcal{H} \cap K = \emptyset$, but $\mathcal{H}_p \cap K$ need not be empty!

Goal: Define a p-adic "modular parametrisation"

$$\Phi : \mathcal{H}_p^D / \Gamma_0(N) \longrightarrow E(H_D),$$

for *positive* discriminants D.

Hida Theory

Let $U = p$-adic disc in $\mathbf{Q}_p$ with $2 \in U$;

$\mathcal{A}(U) =$ ring of p-adic analytic functions on U.

Theorem. (Hida) There exists a unique formal q-expansion

$$f_\infty = \sum_{n=1}^{\infty} \underline{a}_n q^n, \quad \underline{a}_n \in \mathcal{A}(U),$$

with the property that for all $k \geq 2$, $k \in \mathbf{Z}$, $k \equiv 2 \pmod{p-1}$,

$$f_k := \sum_{n=1}^{\infty} \underline{a}_n(k) q^n$$

is an eigenform of weight k on $\Gamma_0(N)$, and

$$f_2 = f_E.$$

Eichler-Shimura Theory

$\mathcal{P}_k :=$ space of homogenous polynomials of degree $k-2$.

Theorem. (Shimura) If f has weight k, there exists a number Ω_f^+ such that, for all $P \in \mathcal{P}_k$, and for all $r, s \in \mathbf{P}_1(\mathbf{Q})$,

$$(\Omega_f^+)^{-1}\,\mathrm{Re}\left(\int_r^s f(z)P(z,1)dz\right)$$

belongs to $\mathbf{Q}(a_1, \ldots, a_n, \ldots)$.

The modular form f is *completely determined* by these periods integrals.

Eichler-Shimura for Hida families

Theorem (Mazur). For each $r, s \in \mathbf{P}_1(\mathbf{Q})$, there exists a compactly supported p-adic measure $\mu_{r,s}$ on $\mathcal{W} := \mathbf{Q}_p^2 - \{0\}$ such that, for all $P \in \mathcal{P}_k$,

$$\int_{\mathcal{W}} P(x,y) d\mu_{r,s}(x,y)$$

$$= \frac{1}{\Omega_f^+} \mathrm{Re}\left(\int_r^s f_k(z) P(z,1) dz\right).$$

Mazur's measures $\mu_{r,s}$ encode the Shimura periods attached to all the classical f_k's in the Hida family.

Heegner points for real quadratic fields

Definition. Given $\tau \in \mathcal{H}_p/\Gamma_0(M)$, let $\gamma_\tau \in \Gamma_0(M)$ be a generator for $\mathrm{Stab}_{\Gamma_0(M)}(\tau)$.

Let log be the p-adic logarithm, and

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

the p-adic Lie group exponential.

Choose any base point $r \in \mathbf{P}_1(\mathbf{Q})$, and define

$$\boxed{\Phi(\tau) := \exp_E\left(\int_{\mathcal{W}} \log(x - \tau y)\, d\mu_{r,\gamma_\tau r}(x,y)\right)}$$

Conjecture. The maps are compatible with the actions in the following diagram:

$$\begin{array}{ccc} G_D & \xrightarrow{\text{rec}} & \mathrm{Gal}(H_D/K) \\ \circlearrowleft & & \circlearrowleft \\ \mathcal{H}_p^D/\Gamma_0(M) & \xrightarrow{\Phi} & E(H_D). \end{array}$$

An example

Conductor $N = 11$.

$$E : y^2 + y = x^3 - x^2 - 10x - 20$$

The conjecture has been used to efficiently compute points on E defined over ring class fields of real quadratic fields, via 11-adic analysis, thanks to a recently impemented `Magma` package called `shp`.

Another example

The equation

$$\boxed{y^2 - y = x^3 = x}$$

"Which (rational, algebraic) numbers can be expressed as a product of both 2 and 3 *consecutive* numbers?"

$N = 37$, so this problem can be tackled, over class fields of real quadratic fields, via 37-adic analysis!

$D > 0$, $h =$ class number of D.

$$P_1 = (x_1, y_1), \ldots, P_h = (x_h, y_h)$$

$$h_D(x) = \prod_{j=1}^{h} (x - x_j).$$