The Arithmetic of Elliptic Curves

Theory

Conjectures

Computations

Applications

Applications

John Cremona

University of Exeter

Example 1

Zagier, Dudeney, ...

Find $m, n \in \mathbb{N}$ satisfying

$$1^2 + 2^2 + 3^2 + \ldots + n^2 = m^2. \tag{1}$$

Two solutions: $(m, n) = (1, 1), \quad (70, 24)$.

Substituting $X = 12n + 6$, $Y = 72m$ leads to

$$E: \qquad Y^2 = X^3 - 36X \tag{2}$$

which is an **elliptic curve**. There are infinitely many *rational* solutions (X, Y) to (2), but only a finite number of *integral* solutions.

$$E(\mathbb{Q}) = \langle P, T_1, T_2 \rangle \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

where

$$P = (-2, 8), \quad T_1 = (0, 0), \quad T_2 = (6, 0)$$

and

$$Q = -2P - T_1 = (294, 5040) \mapsto (m, n) = (70, 24).$$

Elliptic Curves: definition

An **elliptic curve** (defined over any field K) is a plane cubic curve with equation

$$E: \qquad Y^2 = X^3 + aX + b \qquad a, b \in K$$

where $\Delta = -4a^3 - 27b^2 \neq 0$.

Fields of interest:

$K = \mathbb{C}$: elliptic functions, classical complex analysis.

$K = \mathbb{F}_q$: applications in computational number theory and computer science (factorization, primality testing and proving, cryptography, coding theory).

$K = \mathbb{Q}$ (or a number field): Diophantine equations, Arithmetical Algebraic Geometry.

Also: $K = \mathbb{R}$, $K = \mathbb{Q}_p$, etc.

Two types of question to ask:

GENERAL: classify all elliptic curves over K (up to isomorphism, or isogeny, say)

- easy over $\mathbb{C}$ (via j-invariant)
- well understood over $\mathbb{F}_q$
- much harder over $\mathbb{Q}$: the Weil-Taniyama conjecture states that all elliptic curves E defined over $\mathbb{Q}$ are *modular*, i.e. attached to modular forms.

SPECIFIC: study individual curves over K

In particular, describe the group of "rational points":

$$E(K) = \{(x, y) \in K^2 \mid y^2 = x^3 + ax + b\} \cup \{\infty\}.$$

The group law is

$$P + Q + R = 0 \iff P, Q, R \text{ are collinear.}$$

(The "tangent-chord" process). This turns $E(K)$ into an **Abelian group** (with $\infty = 0$).

Group structure

$$E(\mathbb{C}) \cong \mathbb{C}/\Lambda \cong (\mathbb{R}/\mathbb{Z})^2 \quad \text{where} \quad \Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2.$$

$E(\mathbb{F}_q)$ is finite: $|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$ ("Riemann Hypothesis" for elliptic curves over $\mathbb{F}_q$).

$E(\mathbb{F}_q)$ is *either* cyclic *or* is a product of two cyclic factors (since $nP = 0$ has $\leq n^2$ solutions $\forall n \geq 1$).

If K is a number field, $E(K)$ is called the *Mordell-Weil group*.
Mordell-Weil Theorem: $E(K)$ is *finitely generated*: so

$$E(K) \cong T \times \mathbb{Z}^r$$

where T is the (finite) **torsion subgroup** and r is the **rank**.

Questions:

- Which groups T arise?
- How to find T for a given curve?
- Which ranks r occur?
- How to find r for a given curve?
- How to find a basis of r independent points?

TWO APPLICATIONS

I. Fermat's Last Theorem

Frey, Ribet: Counterexample to FLT
$\Rightarrow \exists$ non-modular (semi-stable) elliptic curve over $\mathbb{Q}$
$\Rightarrow$ Weil-Taniyama **fails**.

Wiles, Taylor: Weil–Taniyama **holds** for semi-stable curves over $\mathbb{Q}$.
Corollary: FLT holds!

N.B. Proof theoretical, **not** computational, but now **all** semi-stable elliptic curves over $\mathbb{Q}$ may be explicitly constructed (in principle) from modular forms.

II. Gauss's Class Number Problem

Goldfeld (1975) proved a good bound on those $d > 0$ for which the field $\mathbb{Q}(\sqrt{-d})$ has class number h.
Proof *needs* an L-function with certain analytic properties, *supplied* (Gross, Zagier 1985) by $L(E, s)$, where

$$E: \qquad Y^2 + Y = X^3 - 7X + 6$$

which **is** modular and has rank 3. These two facts **were** established by computational means (the former originally by Mestre).

Rational newforms for $\Gamma_0(N)$

$N \leq 5077$

Range of N	Total	$r = 0$	$r = 1$	$r = 2$	$r = 3$
1–1000	2463	1321	1124	18	0
1001–2000	3391	1575	1737	79	0
2001–3000	3661	1663	1852	146	0
3001–4000	3837	1665	2006	166	0
4001–5000	3962	1690	2092	180	0
5001–5077	284	121	148	14	1
1–5077	17598	8035	8959	603	1

These are also the numbers of (isogeny classes of) modular elliptic curves of conductor N. The ranks r here are *analytic* ranks (order of vanishing of L-series at $s = 1$), but also agree with the *algebraic* ranks of the Mordell–Weil groups of the corresponding curves in all cases (by a combination of Theorems and explicit computation).

$N = 5077$ is the first case with $r = 3$.

MORDELL-WEIL GROUPS

$$E(K) \cong T \times \mathbb{Z}^r$$

I. Torsion

Over $\mathbb{Q}$, possible torsion groups classified by Mazur c.1970:

$$T \cong \begin{cases} C_n, & (1 \le n \le 10,\ n = 12); \\ C_2 \times C_n, & (1 \le n \le 4). \end{cases}$$

Also, $(x, y) \in T \Rightarrow x, y \in \mathbb{Z}$ and **either** $y = 0$ **or** $y^2 \mid \Delta$ (assuming $a, b \in \mathbb{Z}$), so T is easy to find for a given curve.

Over a number field K of degree d: similar classification exists for $d = 2$ (Kamienny, Kenku, Momose).
The **Uniform Boundedness Conjecture** states that $\forall d \exists B\colon |T| \le B$ for **all** curves E over **all** fields K of degree d.
In particular, the set S_d of primes p such that there exists a curve E defined over a field K of degree d with a point of order p should be **finite** for each d.
This was **proved** in 1993 by L. Merel: he showed $p < d^{3d^2}$. (This bound is likely to be improved.) More work is then needed to determine exactly which groups T can occur for each d.
Examples: $S_1 = \{2, 3, 5, 7\}$, $S_2 = \{2, 3, 5, 7, 11, 13\}$.

MORDELL-WEIL GROUPS (contd.)

II. Rank

No bound on the rank r is known, or believed to exist, for any given number field K.
Over $\mathbb{Q}$, curves of rank up to 21 are known; including infinite families of rank up to 11. (Mestre, Nagao)
Computing r: via **descent**. Same method as used to prove the rank is finite, made very explicit.

Descent

Take $K = \mathbb{Q}$ for simplicity.
Basic idea: cover E with a finite number of auxiliary curves C_1, C_2, ..., C_k (all of genus 1 and isomorphic to E over $\mathbb{C}$).

- If $C_i(\mathbb{Q}) \neq \phi$, then its image is a complete **coset** of $mE(\mathbb{Q})$ in $E(\mathbb{Q})$ for some $m \geq 2$ (usually $m = 2$).
- Hence once hopes to find $[E(\mathbb{Q}) : mE(\mathbb{Q})]$, and hence the rank r, by deciding which C_i have rational points.
- **Problem:** no algorithm exists for deciding this!

One can fairly easily eliminate those C_i for which either $C_i(\mathbb{R}) = \phi$, or $C_i(\mathbb{Q}_p) = \phi$ for some prime p.
BUT some C_i may have points "everywhere locally but not globally".
The extent to which this can happen is measured by the **Tate-Shafarevich group** Ш ("Sha").

Higher descents

We can carry out "further descents", covering each C_i by a finite set of curves C_{ij}, so that $C_i(\mathbb{Q}) \neq \phi \iff C_{ij}(\mathbb{Q}) \neq \phi$ for some j. If we knew that Ш was finite, this process would stop after a finite number of steps. If not, we have a problem: but this procedure might still be practical.

Ш **Conjecture:** For all elliptic curves E defined over $\mathbb{Q}$,

$$|Ш(E/\mathbb{Q})| < \infty.$$

In practice: we can always bound r by descent (using the local solubility conditions) and can often determine it exactly. There now exist general efficient programs for doing this over $\mathbb{Q}$ which are currently being extended to certain quadratic fields. But making these ideas explicit enough to implement as programs is very difficult.

Current status of the Ш conjecture: **Proved** for modular elliptic curves of rank 0 or 1 by Rubin and Kolyvagin, as part of their work on the famous **Birch Swinnerton-Dyer Conjecture**.

The Birch Swinnerton-Dyer Conjecture

This relates the rank r of $E(\mathbb{Q})$ to the behaviour of a certain analytic function $L(E,s)$, called the L-function of E over $\mathbb{Q}$, at $s=1$:

(1) $\mathrm{ord}_{s=1}L(E,s) = r = \mathrm{rank}(E(\mathbb{Q}))$;

It also gives a formula for $|Ш|$, analogous to the analytic class-number formula for number fields:

(2)

$$|Ш| = \frac{L^{(r)}(E,1)\cdot|T|^2}{r!\cdot\Omega\cdot R\cdot\prod_p c_p}$$

where :

Ω is the real period of E;

R is an $r\times r$ determinant of the "height pairing" for generating points;

c_p is a positive integer ($=1$ except for the finite set of "bad" primes).

The BSD conjecture has only been **proved** for certain modular elliptic curves of rank 0 or 1. Until this, the Ш Conjecture was not known to be true for **any** elliptic curve over $\mathbb{Q}$!

INTEGRAL POINTS

$$E: \quad Y^2 = X^3 + aX + b \qquad (a, b \in \mathbb{Z})$$

The set of **integral** points $E(\mathbb{Z}) = E(\mathbb{Q}) \cap \mathbb{Z}^2$ is always finite, even when the group of rational points $E(\mathbb{Q})$ is infinite.
There are bounds on the x-coordinate of integral points in terms of a and b (due to Siegel, Baker) using transcendence theory, but they are too large to be practical.

Recent advances use bounds on linear forms in **elliptic logarithms** to make the determination of all integral points on a given curve a practical proposition, *provided* that a basis for the Mordell group $E(\mathbb{Q})$ is known. If this basis is $P_1, \ldots, P_r$, then the method can provide small bounds for the coefficients k_i of an integral point $P = \sum k_i P_i$. These methods have been developed by DeWeger, Stroeker, Tzanakis, Smart (and others) implemented by these and Zimmer and Gebel.
All these implementations rely on first having a basis for $E(\mathbb{Q})$, so the demand for programs (such as mine, with improvements due to S. Siksek) which can find such a basis (in many cases) is growing.

Example 2

(J. P. Robinson, with help from JC and Smart)

Find all $m, n \in \mathbb{N}$ satisfying

$$1 + 2 + 3 + \ldots + m = 1^2 + 2^2 + 3^2 + \ldots + n^2.$$

Setting $X = 6n + 3$ and $Y = 18m + 9$, this becomes an elliptic curve:

$$E: \quad Y^2 = X^3 - 9X + 81.$$

$E(\mathbb{Q})$ has no torsion and rank 2. E is **not** proved to be modular (it is not semistable, conductor $N = 8604 = 2^2 3^2 239$).
$E(\mathbb{Q})$ is generated by $P = (-3, 9)$ and $Q = (0, 9)$. A search for integral points with $X \leq 6 \times 10^7$ finds the following:

$$X = -5, -3, 0, 3, 7, 9, 24, 33, 39, 513, 1099, 5112.$$

Using the generators P and Q, Smart showed that all integral points are $iP + jQ$ with $|i|$, $|j| \leq 13$. Computing all these points we find just the ones above.
To fit the original problem we require $X = 6n + 3$: only $X = 9, 33, 39, 513$ fit, giving **four** solution to the original problem:

$$(m, n) = (1, 1), (10, 5), (13, 6), (645, 85).$$