Elliptic curves

Main ref.: J. Silverman, "The arithmetic of elliptic curves", G.T.M 106.

Elliptic curves as algebraic curves

A plane affine cubic curve over $\mathbf{C}$ is the set of complex solutions (x, y) of an equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

where the a_i are complex numbers. If the a_i are rational, the curve is said to be defined over $\mathbf{Q}$, and one can consider the basic diophantine question: find all solutions (x, y) in $\mathbf{Q}$.

It is more convenient to look at the equation in homogeneous form and solutions in the *projective plane*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

where $(X : Y : Z) = (\alpha X : \alpha Y : \alpha Z)$ if $\alpha \neq 0$.

If $Z \neq 0$, $x = X/Z$, $y = Y/Z$ gives back the first equation. If $Z = 0$ one adds one point at infinity $\infty = (0 : 1 : 0)$ (always rational).

To "be" an elliptic curve, a plane cubic must be *smooth*, which means that the partial derivatives

$$2y + a_1x + a_3 \text{ and } a_1y - 3x^2 - 2a_2x - a_4$$

do not have a common zero on the cubic. If $a_1 = a_3 = 0$, this means the cubic polynomial $x^3 + a_2x^2 + a_4x + a_6$ has simple roots, equivalently that $\Delta_E = -16(4a_4^3+27a_6^2) \neq 0$.

Examples

• $y^2 = x^3$ is not smooth (it has a cusp).

• $y^2 = x^3 + x^2$ is not smooth (it has a node).

• $y^2 = x^3 - x$ is an elliptic curve (the "congruent number" curve), of CM type.

• $y^2 + y = x^3 - x^2$ is an elliptic curve (the modular curve $X_1(11)$).

• If $\ell > 2$ is a prime, (a, b, c) are non-zero and satisfy $a^\ell + b^\ell = c^\ell$ then $y^2 = x(x - a^\ell)(x + b^\ell)$ is a remarkable elliptic curve. It can not exist if (a, b, c) are rationals.

An elliptic curve as a complex torus

Let ω_1, ω_2 be non-zero complex numbers, with $\omega_1/\omega_2 \notin \mathbf{R}$. Let $\Lambda = \omega_1\mathbf{Z} \oplus \omega_2\mathbf{Z}$ (a lattice in $\mathbf{C}$).

Consider the quotient $\mathbf{C}/\Lambda$: this is a compact Riemann surface and it "is" an elliptic curve; topologically this is a torus.

In terms of functions, consider meromorphic functions

$$f : \mathbf{C} \to \mathbf{C}$$

which are ω_1 and ω_2-periodic:

$$f(z + \omega_1) = f(z) \text{ and } f(z + \omega_2) = f(z).$$

Those f are called elliptic functions because the arc-length on an ellipse can be expressed in terms of (inverses of) such functions.

Correspondance between the two viewpoints

For a given Λ, there is an elliptic function $\wp$ which has a pole of order 2 at points of Λ and satisfies the algebraic differential equation

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3$$

for some g_2, $g_3 \in \mathbf{C}$. In fact

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right),$$

$$g_2 = 60 \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \frac{1}{\omega^4}, \quad g_3 = 140 \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \frac{1}{\omega^6}.$$

Sending $z \mapsto (2\wp(z), \sqrt{2}\wp'(z))$ gives (bijectively) the points on the plane cubic

$$y^2 = x^3 - g_2x - 2g_3$$

with $0 \mapsto \infty$ since $\wp$ has a pole at $z = 0$. One shows this is smooth. All elliptic curves with $a_1 = a_3 = a_2 = 0$ arise in this manner.

The group law

The quotient $\mathbf{C}/\Lambda$ has a natural abelian group structure. So there must be group structure on elliptic curves. Geometrically, if P, Q, R are distinct points on the elliptic curve (as plane cubic curve), we have $P+Q+R=0$ for this group law if and only if P, Q and R are colinear.

[Sketch of "if": The equation $F(x,y,z)=0$ of the line joining P, Q and R gives an elliptic function f such that the divisor of f is $(p)+(q)+(r)-3(0)$. By integrating zf'/f along the boundary of a fundamental parallelogram, one gets $p+q+r\in\Lambda$].

This group law is algebraic: for instance one finds for $y^2=x^3+a_4x+a_6$ that $-(x,y)=(x,-y)$, and $(x_1,y_1)+(x_2,y_2)=(x_3,y_3)$ with

$$x_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-x_1-x_2,$$
$$y_3=\frac{y_2-y_1}{x_2-x_1}(x_3-x_1)-y_1$$

if $x_1\neq x_2$.

Maps between elliptic curves

Some polynomial or rational change of coordinates transform an elliptic curve into another. If they are "well-defined" everywhere, these are morphisms of elliptic curves.

Examples. • For fixed $x_0 \in E(\mathbf{C})$, $f(x) = x + x_0$ (with the group law above) is a morphism $E \to E$.

• For any integer $n \in \mathbf{Z}$, $[n] : x \mapsto nx$ (for the group law) is a morphism $E \to E$ (defined over $\mathbf{Q}$ if E is).

• If $a^2 \neq 4b$,

$$\{y^2 = x^3 + ax^2 + bx\} \to \{w^2 = v^3 - 2av^2 + (a^2 - 4b)v\}$$
$$(x, y) \mapsto (\tfrac{y^2}{x^2}, \tfrac{y(b-x)^2}{x^2})$$

is a morphism with $(0, 0) \mapsto \infty$.

• Let $E : y^2 = x^3 - x$. Then $[i] : (x, y) \mapsto (-x, iy)$ is a morphism defined over $\mathbf{Q}(i)$.

Any morphism is of the form $f(x) = g(x) + x_0$ where g is a morphism preserving the group law (*isogeny*).

For a complex torus $\mathbf{C}/\Lambda$, translations correspond to translations and isogenies $\mathbf{C}/\Lambda_1 \to \mathbf{C}/\Lambda_2$ correspond to multiplication by $\alpha \in \mathbf{C}$ such that $\Lambda_1 \subset \Lambda_2$.

Isogenies, torsion points

Isogenies $E \to E$ form a ring, $\mathrm{End}(E)$. One may have $\mathrm{End}_{\mathbf{C}}(E) \neq \mathrm{End}_{\mathbf{Q}}(E)$. Usually one has $\mathrm{End}(E) \simeq \mathbf{Z}$. Otherwise, E is a *CM curve*.

A non-zero isogeny $f : E_1 \to E_2$ is surjective. The kernel $\ker f = \{x \in E_1 \mid f(x) = 0\}$ is a finite abelian group.

For $f = [n]$, $n \neq 0$, one has $\ker f = E[n] \simeq (\mathbf{Z}/n\mathbf{Z})^2$ by the complex description $E(\mathbf{C}) = \mathbf{C}/\Lambda$.

If E is defined over $\mathbf{Q}$, the points of $E[n]$ have algebraic coordinates. They are analogues of the classical roots of unity (torsion points in $\mathbf{C}^\times$) and are very important in the arithmetic of E.

Example. If E has equation $y^2 = x^3 + a_4x + a_6$ then

$$E[2] = \{\infty, (e_1, 0), (e_2, 0), (e_3, 0)\}$$

where e_i are the (distinct) roots of $x^3 + a_4x + a_6 = 0$.

Classification of elliptic curves

An isomorphism of elliptic curve is an isogeny which is one-to-one. One can try to classify elliptic curves up to isomorphism.

By simple changes of variable, any Weierstrass equation over $\mathbf{C}$ can be brought to the form $y^2 = x^3 + c_4 x + c_6$ for some c_4, c_6. Such curves are elliptic curves if $\Delta = -16(4c_4^3 + 27c_4^2) \neq 0$. They are classified up to $\mathbf{C}$-isomorphism by the j-invariant $j = 1728(4c_4)^3/\Delta$.

Elliptic curves defined over $\mathbf{Q}$ might be isomorphic but only over a bigger field (*twists*).

For complex tori, one checks that there is a unique $\tau \in SL(2,\mathbf{Z})\backslash\mathbf{H}$ such that $\mathbf{C}/\Lambda \simeq \mathbf{C}/(\mathbf{Z} \oplus \tau\mathbf{Z})$. The j-invariant is then a holomorphic map $\mathbf{H} \to \mathbf{C}$ which is $SL(2,\mathbf{Z})$-invariant.

Enter arithmetic (Mordell's theorem)

If the coefficients a_i defining the elliptic curve are rational, one checks immediately that the set of rational solutions is a subgroup of $E(\mathbf{C})$. The main structure theorem is due to Mordell in this case.

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

Thus one can write

$$E(\mathbf{Q}) \simeq \mathbf{Z}^r \oplus F$$

where $r \geq 0$ is the *rank* of E (over $\mathbf{Q}$) and $F = E(\mathbf{Q})_{tors}$ is the finite torsion subgroup of E.

The proof of the theorem is ineffective; more precisely, it yields an upper bound on r, but no effective way of testing whether a finite family x_1, ..., $x_k \in E(\mathbf{Q})$ generates the whole of $E(\mathbf{Q})$ up to torsion.

However the proof shows it suffices to compute $E(\mathbf{Q})/mE(\mathbf{Q})$ for *some* $m \geq 1$ to compute effectively $E(\mathbf{Q})$.

Example: the congruent number problem

Here is a beautiful instance of the intrusion of elliptic curves in a very classical problem: what are the rationals (so-called *congruent numbers*) r such that there is a right-triangle with rational lengths a, b, c and area r.

Proposition. A squarefree integer $n \geq 1$ is a congruent number if and only if the elliptic curve $E_n : y^2 = x^3 - n^2x$ has rank $r_n \geq 1$.

This has led to an algorithm to check whether a given squarefree integer n is a congruent number.

Theorem (Tunnell). If the Birch and Swinnerton-Dyer Conjecture holds, then (for odd squarefree n), n is a congruent number if and only if the number of triples of integers (x, y, z) such that $2x^2 + y^2 + 8z^2 = n$ is twice the number of triples such that $2x^2 + y^2 + 32z^2 = n$.

Example: $n = 41$ is congruent;

$$41 = \overbrace{2(\pm 4)^2 + (\pm 3)^2}^{4} = \overbrace{2(\pm 4)^2 + (\pm 1)^2 + 8(\pm 1)^2}^{8}$$
$$= \overbrace{2(\pm 2)^2 + (\pm 5)^2 + 8(\pm 1)^2}^{8} = \overbrace{(\pm 3)^2 + 8(\pm 2)^2}^{4}$$
$$= \overbrace{2(\pm 2)^2 + (\pm 1)^2 + 8(\pm 2)^2}^{8}$$
$$41 = \overbrace{2(\pm 4)^2 + (\pm 3)^2}^{4} = \overbrace{2(\pm 2)^2 + (\pm 1)^2 + 32(\pm 1)^2}^{8}$$
$$= \overbrace{(\pm 3)^2 + 32(\pm 1)^2}^{4}.$$

[ref.: N. Koblitz, "Introduction to elliptic curves and modular forms", G.T.M 97.]

Digression on torsion

The finite torsion group $E(\mathbf{Q})_{tors}$ is easily computable (the prime-to-p part of it injects in the finite group of points modulo a prime p of good reduction). There is a finite list of possible $E(\mathbf{Q})_{tors}$ for $E/\mathbf{Q}$ (a theorem of Mazur).

$E_1 : y^2 = x^3 - 2$, torsion $= \{0\}$.

$E_2 : y^2 = x^3 + 8$, torsion $\simeq \mathbf{Z}/2\mathbf{Z}$.

$E_3 : y^2 = x^3 + 4$, torsion $\simeq \mathbf{Z}/3\mathbf{Z}$.

$E_4 : y^2 = x^3 + 4x$, torsion $\simeq \mathbf{Z}/4\mathbf{Z}$.

$E_5 : y^2 - y = x^3 - x$, torsion $\simeq \mathbf{Z}/5\mathbf{Z}$.

$E_6 : y^2 = x^3 + 1$, torsion $\simeq \mathbf{Z}/6\mathbf{Z}$.

$E_7 : y^2 - xy - 4y = x^3 - x^2$, torsion $\simeq \mathbf{Z}/7\mathbf{Z}$.

$E_8 : y^2 + 7xy = x^3 + 16x$, torsion $\simeq \mathbf{Z}/8\mathbf{Z}$.

$E_9 : y^2 + xy + y = x^3 - x^2 - 14x + 29$, torsion $\simeq \mathbf{Z}/9\mathbf{Z}$.

$E_{10} : y^2 + xy = x^3 - 45x + 81$, torsion $\simeq \mathbf{Z}/10\mathbf{Z}$.

$E_{11} : y^2 + 43xy - 210y = x^3 - 210x^2$, torsion $\simeq \mathbf{Z}/12\mathbf{Z}$.

$E_{12} : y^2 = x^3 - 4x$, torsion $\simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

$E_{13} : y^2 + xy - 5y = x^3 - 5x^2$, torsion $\simeq \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

$E_{14} : y^2 + 5xy - 6y = x^3 - 3x^2$, torsion $\simeq \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

$E_{15} : y^2 + 17xy - 120y = x^3 - 60x^2$, torsion $\simeq \mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.

Reduction modulo a prime

Let $E/\mathbf{Q}$ be an elliptic curve. By change of variable one can assume the equation (1) has integral coefficient. For any prime p, one can reduce modulo p and look at solutions (x, y) in the finite field $\mathbf{Z}/p\mathbf{Z}$ of

$$y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6 \pmod{p}.$$

If $p \nmid \Delta_E$ this is an elliptic curve over $\mathbf{Z}/p\mathbf{Z}$.

Theorem (Hasse). The number of projective solutions is $N_p = p + 1 - a_p$ with $|a_p| \leq 2\sqrt{p}$.

Remark. If $a_1 = a_3 = 0$ then

$$a_p = -\sum_{x \,(\mathrm{mod}\, p)} \Big(\frac{x^3 + a_2x^2 + a_4x + a_6}{p}\Big)$$

with $\left(\frac{y}{p}\right)$ the Legendre symbol. So size $\sqrt{p}$ is reasonable on probabilistic grounds.

Example. $y^2 = x^3 - x$, $\Delta_E = 64$. If $p \equiv 3 \,(\mathrm{mod}\, 4)$, $a_p = 0$; if $p \equiv 1 \,(\mathrm{mod}\, 4)$, write (Fermat) $p = a^2 + b^2$ with a odd, b even, $a + b \equiv 1 \,(\mathrm{mod}\, 4)$; then $a_p = 2a$.

The (partial) Hasse-Weil L-function

To go from local (modulo primes) to global, define first

$$\ell(E,s) = \prod_{p \nmid \Delta_E} (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

This product converges absolutely for Re$(s) >$ 3/2 by Hasse's Theorem.

Hasse conjectured that $\ell(E,s)$ has analytic continuation to $\mathbf{C}$. This is an imprecise form of the *modularity* of elliptic curves over $\mathbf{Q}$, proved by Wiles, Taylor-Wiles, Breuil-Conrad-Diamond-Taylor.

The conductor

To obtain the "right" L-function, one needs correct factors at the primes $p \mid \Delta_E$. One can have $p \mid \Delta_E$ for some equation but not for another (Δ is not an isomorphism-invariant).

One defines the *conductor* $N_E \geq 1$ such that $p \nmid N_E$ if and only if E has a smooth reduction modulo p, possibly after change of variable. For $p \mid N_E$, the exponent f_p of p in N_E is dictated by the geometry of the singular reduction.

Examples • If the reduction of E modulo p has a node, then $f_p = 1$ ("multiplicative reduction").

• If $p > 3$ and the reduction of E modulo p has a cusp, then $f_p = 2$ ("additive reduction").

• For $y^2 + y = x^3 - x$, $N_E = 11$. This is the smallest possible conductor for $E/\mathbf{Q}$.

The cases $p = 2$, 3 with a cusp are much more intricate.

The complete Hasse-Weil L-function

If $p \mid N_E$, define

$$a_p = \begin{cases} 0 & \text{if } f_p \geq 2, \\ -1 & \text{if } f_p = 1, \text{ slopes in } \mathbf{Z}/p\mathbf{Z}, \\ 1 & \text{otherwise.} \end{cases}$$

Then

$$L(E,s) = \prod_{p|N_E} (1 - a_p p^{-s})^{-1} \prod_{p \nmid N_E} (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

Modularity of E implies that $L(E,s)$ has holomorphic continuation to an entire function, and that it satisfies

$$\Lambda(E,s) = w_E N_E^{1-s} \Lambda(E, 2-s)$$

where $w_E = \pm 1$ (sign of the functional equation) and $\Lambda(E,s) = (2\pi)^{-s}\Gamma(s)L(E,s)$.

Remark. The sign w_E factorizes as a product over $p \mid N_E$ of local signs. It is effectively computable.

Modularity explained

In fact the continuation of $L(E,s)$ is proved indirectly.

Write $L(E,s) = \sum_{n\geq 1} a_n n^{-s}$ and put

$$f(z) = \sum_{n\geq 1} a_n e^{2\pi i n z} \text{ for } \mathrm{Im}(z) > 0.$$

Modularity means exactly that f is holomorphic, satisfies

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z)$$

for $a,b,c,d \in \mathbf{Z}$, $ad-bc = 1$, $N_E \mid c$, and $\mathrm{Im}(z)|f(z)|$ is bounded ("cusp form of weight 2 for $\Gamma_0(N_E)$").

Then the formula (Hecke)

$$\Lambda(E,s) = \int_0^\infty f(iy) y^{s-1} dy$$

easily gives analytic continuation/functional equation.

The Birch and Swinnerton-Dyer Conjecture

Let E be an elliptic curve defined over $\mathbf{Q}$. So $L(E,s)$ is holomorphic, in particular defined at $s=1$. The simplest form of the Birch and Swinnerton-Dyer Conjecture is

Conjecture. We have

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

Remark. If $w_E = -1$ (a *local* condition), then $L(E,1) = 0$ so the conjecture implies that $\operatorname{rank} E \geq 1$ in this case. Find a non-torsion point!

There is a more refined form:

Conjecture. We have

$$L(E,s) \sim \alpha (s-1)^r \text{ as } s \to 1,$$

where

$$\alpha = \frac{\Omega |Ш(E)| R(E) c}{|E(\mathbf{Q})_{tors}|^2} > 0.$$

We will now explain the various factors in the constant α.

Explanation I: the "easy" terms

• $|E(\mathbf{Q})_{tors}|$ is the cardinality of the set of rational torsion points on E. This is easy to compute theoretically and algorithmically.

• c is given by the product over primes of $c_p = |E(\mathbf{Q}_p)/E_0(\mathbf{Q}_p)|$, $E_0(\mathbf{Q}_p)$ being the set of points which have non-singular reduction modulo p. If E has good reduction at p, $c_p = 1$. Otherwise there is an efficient algorithm to compute c_p.

Explanation II: the regulator

$R(E)$ is the elliptic regulator. Let x_1,. . . , x_r be a basis for the free part of $E(\mathbf{Q})$. Then

$$R(E) = \det(\langle x_i, x_j \rangle)$$

where $\langle \cdot, \cdot \rangle$ is the canonical height on $E(\mathbf{Q}) \otimes \mathbf{R}$, the bilinear form coming from the quadratic form

$$\|p\| = \lim_{n \to +\infty} 4^{-n} h([2^n]p)$$

where

$$h(x, y) = \frac{1}{2} \log H(x),$$
$$H(p/q) = \max(|p|, |q|) \text{ if } (p, q) = 1.$$

There are explicit and efficiently computable formulas for the height.

Explanation III: the Tate-Shafarevich group

The group $Ш(E)$ is the most mysterious term in the Birch and Swinnerton-Dyer conjecture. In contrast with the others, it is not known to be effectively computable, in fact it is not known to be finite.

One can sketch how $Ш(E)$ arises as follows. Let $E/\mathbf{Q}$ have equation $y^2 = (x-e_1)(x-e_2)(x-e_3)$ with $e_i \in \mathbf{Q}$ (so $E[2] \subset E(\mathbf{Q})$. If $(x,y) \in E(\mathbf{Q})$, note that for $p \nmid \Delta_E$ the smoothness modulo p implies $x-e_i$ are pairwise coprime so p occurs with even power in the factorization of $x-e_i$. So there is a computable finite set T of triples $b = (b_1, b_2, b_3)$ of non-zero rationals and rationals z_1, z_2, z_3 such that for some $b \in T$

$$\begin{cases} y^2 = (x-e_1)(x-e_2)(x-e_3) \\ x - e_1 = b_1 z_1^2 \\ x - e_2 = b_2 z_2^2 \\ x - e_3 = b_3 z_3^2. \end{cases}$$

For any fixed b, this defines a curve C_b (in affine 5-space). Eliminating some unknowns it is isomorphic to the space curve

$$\begin{cases} b_1 z_1^2 - b_2 z_2^2 = (e_2 - e_1) \\ b_1 z_1^2 - b_1 b_2 z_3^2 = (e_3 - e_1). \end{cases}$$

Finding all C_b which have a rational point allows to compute easily $E(\mathbf{Q})/2E(\mathbf{Q})$ and then $E(\mathbf{Q})$.

Problem: There is no algorithm to check whether $C_b(\mathbf{Q}) \neq \emptyset$.

However one can compute easily the subset $S \subset T$ of those b for which C_b has "locally" a point at all p, and a real-valued point.

Those elements of S which still do not have a rational point (they fail the "Hasse principle") "are" the elements of order 2 in $Ш(E)$. (It is a finite set here, in fact a group).

General definition as a set: a curve C is a principal homogeneous space for E if one can define $p + P$ for $p \in C$, $P \in E$ with $p + (P + Q) = (p + P) + Q$ and $p + P = q$ has a unique solution $q - p$ for all (p, q). The curves C_b above are examples. Then $Ш(E)$ is the set of all such C for which $C(\mathbf{R})$ and $C(\mathbf{Q}_p)$, for all p, are non-empty, modulo isomorphism (as homogeneous spaces). There is a group structure with E as identity element. A $C \in Ш(E)$ is trivial if and only if $C(\mathbf{Q}) \neq \emptyset$ ($p \mapsto p - p_0$ gives $C \simeq E$).

Cohomology definition:

$$Ш(E) = \ker\left\{H^1(G_{\mathbf{Q}}, E) \to \prod_v H^1(G_{\mathbf{Q}_v}, E)\right\}$$

Conjecture. For all $E/\mathbf{Q}$, the Tate-Shafarevich group $Ш(E)$ is a finite group.

The refined form of the Birch and Swinnerton-Dyer conjecture does not make sense without this conjecture.

This is known for only very few cases where $\mathrm{ord}_{s=1} L(E, s) \leq 1$ (Rubin, Kolyvagin...)

Example: a Tate-Shafarevich group

Let E be the elliptic curve $y^2 = x^3 - 24300$, $j = 0$. The rank is 0, the regulator is 1, the torsion group is trivial, the Tamagawa number is 1,

$$L(E, 1) = 4.061375813927\ldots$$
$$\Omega = 0.451263979325\ldots$$

and so $|Ш(E)| = 9$, $Ш(E) \simeq (\mathbf{Z}/3\mathbf{Z})^2$. In fact, the following are equations for all locally trivial homogeneous spaces under E:

$$\begin{array}{rl} C \simeq E & x^3 + y^3 + 60x^3 = 0 \\ C_1 & 3x^3 + 4y^3 + 5z^3 = 0 \\ C_2 & 12x^3 + y^3 + 5z^3 = 0 \\ C_3 & 15x^3 + 4y^3 + z^3 = 0 \\ C_4 & 3x^3 + 20y^3 + z^3 = 0 \end{array}$$

(each of the four equations C_i above corresponds to two opposite elements of $Ш(E)$, equivalently to a line in $(\mathbf{Z}/3\mathbf{Z})^2$).

[ref.: B. Mazur, "On the passage from local to global in number theory", Bull. A.M.S 29 (1993), 14–50].

Enter random matrices...

If the Birch and Swinnerton-Dyer Conjecture holds, the L-function gives an analytic handle on the very mysterious rank of elliptic curves. One may hope to be able in this way to understand (or solve?) some of the outstanding problems, such as:

• Are there elliptic curves over $\mathbf{Q}$ of arbitrarily large rank?

• If yes, "how many" are there when one looks at "families" of elliptic curves?

For some of these questions, the link with zeros of L-functions allows the use of models coming from Random Matrix Theory to try and understand those issues. Comparison with insights from algebraic geometry is then very desirable.

Quadratic twists

The family of curves $y^2 = x^3 - n^2 x$, indexed by n, are special cases of *quadratic twists*. More generally if E has equation

$$E : y^2 = x^3 + a_4 x + a_6$$

consider the curves E_d

$$E_d : dy^2 = x^3 + a_4 x + a_6.$$

Note that $E \simeq E_d$ over $\mathbf{C}$ $((x, y) \mapsto (x, d^{1/2} y))$.

Question. How does the rank of E_d vary as function of d? How do the other invariants?

Function field analogues and low-lying zeros results suggest that the family (E_d), as d varies, has orthogonal symmetry.

The root number is equidistributed in $\{\pm 1\}$. One then expects (Goldfeld)

$$|\{d \leq X \mid \operatorname{rank} E_d = 0\}| \sim \frac{1}{2} \sum_{d \leq X} 1$$

$$|\{d \leq X \mid \operatorname{rank} E_d = 1\}| \sim \frac{1}{2} \sum_{d \leq X} 1.$$

The numerics are ambiguous (suggest "excess rank", especially for even ranks).

Number of twists with higher rank: Random Matrix Theory has been used to predict, e.g,

$$|\{d \leq X \mid w_{E_d} = 1, \operatorname{rank} E_d \geq 2\}| \sim c_E X^{3/4} (\log X)^{b_E}$$

for some $c_E > 0$, $b_E \geq 0$ (Conrey, Keating, Rubinstein, Snaith).

Higher order/rank??