Ranks of elliptic curves

Karl Rubin

June 19, 2002

Fields Institute 10th Anniversary Celebration

Press the Escape key to leave full screen mode

Elliptic curves

An elliptic curve is a curve defined by an equation of the form

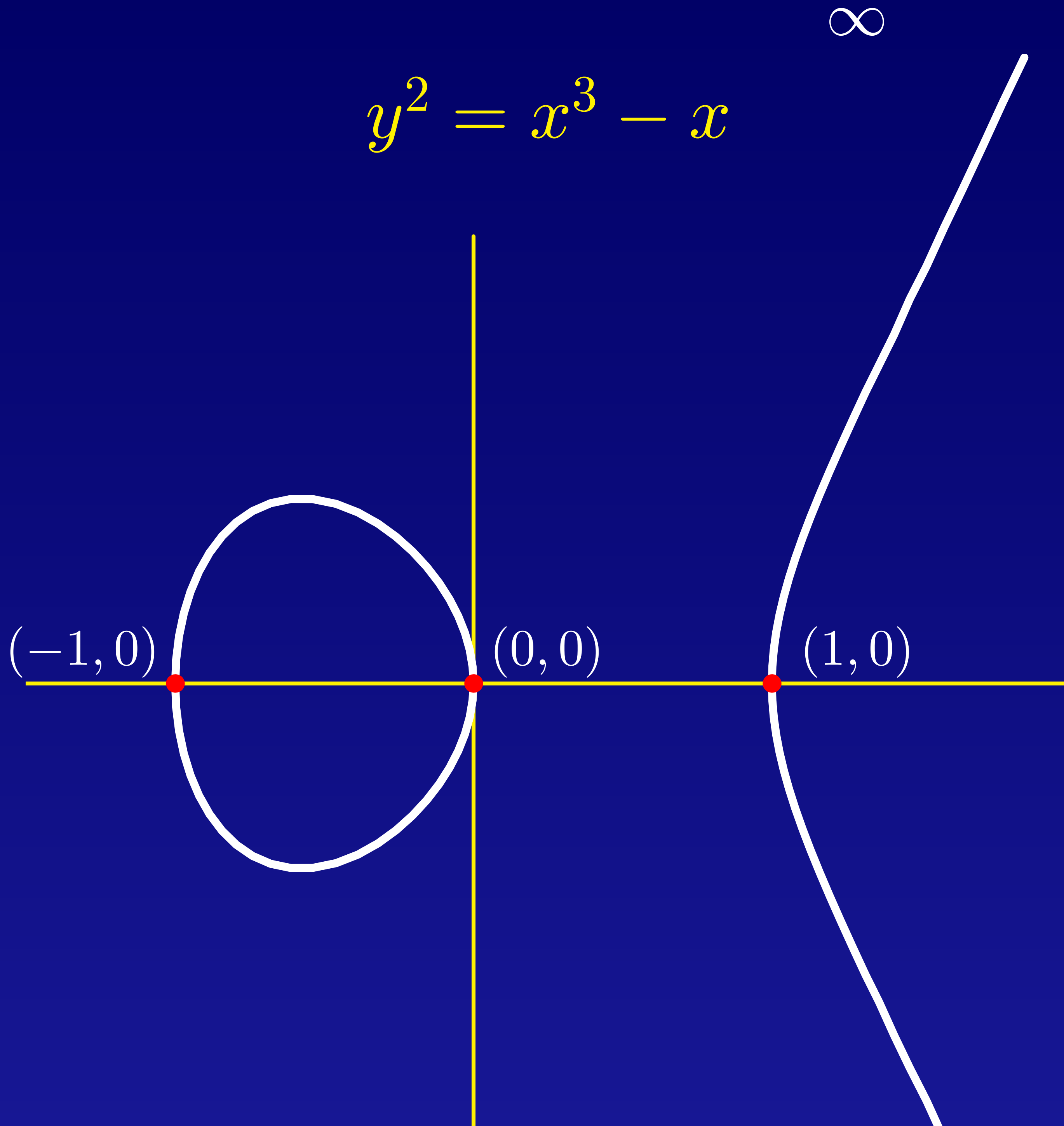
$$y^2 = x^3 + ax + b$$

with integer constants a, b such that

$$\Delta = -16(4a^3 + 27b^2) \neq 0.$$

(The discriminant Δ is nonzero if and only if $x^3 + ax + b$ has distinct roots in $\mathbf{C}$.)

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



Basic problem

Given an elliptic curve E, find all rational solutions:

$$E(\mathbf{Q}) = \{\text{rational points on } E\} \cup \{\infty\}.$$

Theorem (Fermat). *If E is $y^2 = x^3 - x$, then*

$$E(\mathbf{Q}) = \{(-1,0),(0,0),(1,0),\infty\}.$$

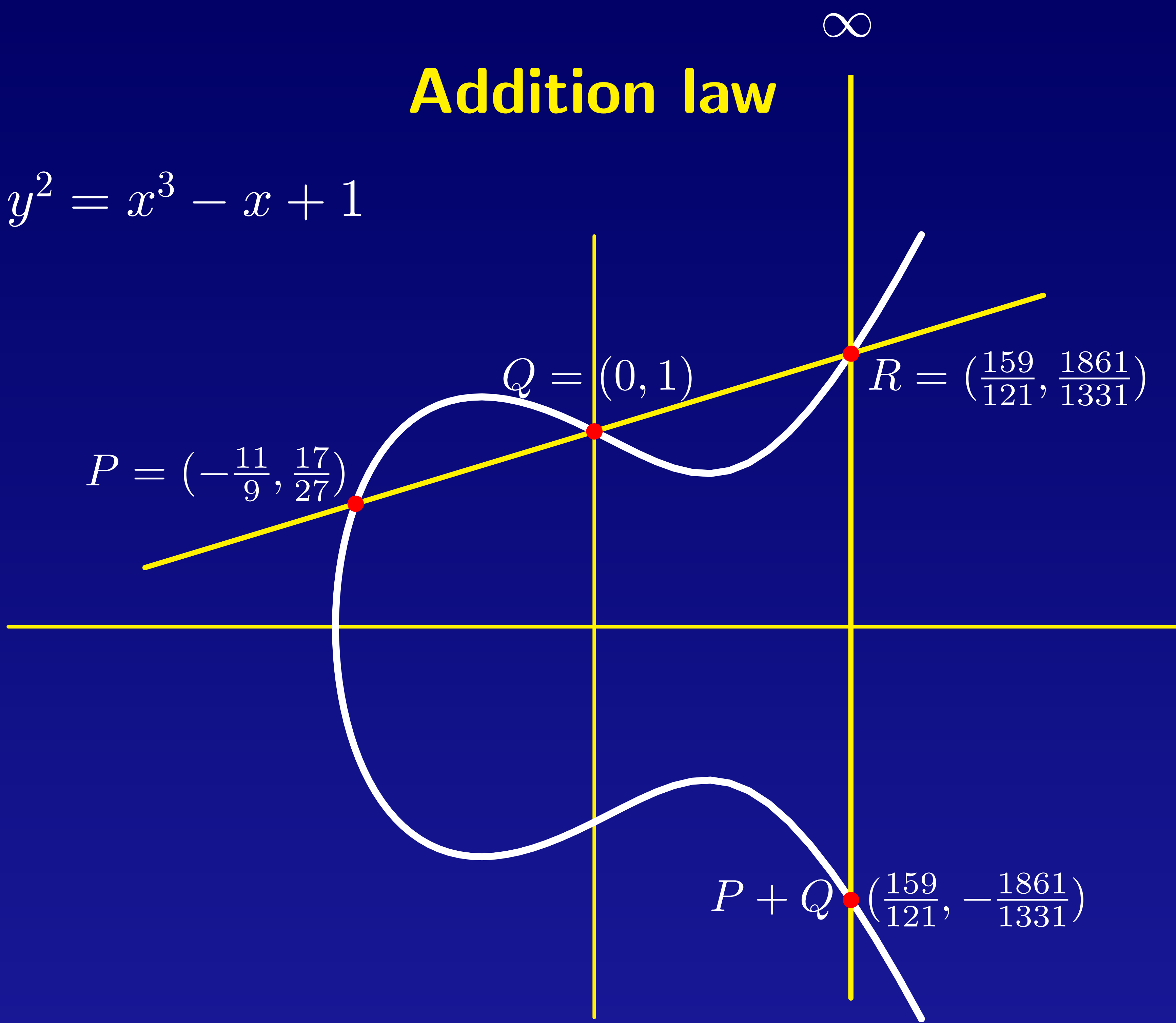
Addition law

$E(\mathbf{Q})$ has a natural, geometrically defined addition law

3 collinear points sum to zero

which makes $E(\mathbf{Q})$ into a commutative group, with ∞ as the identity element.

Addition law



Addition law

If E is the elliptic curve $y^2 = x^3 + ax + b$, and

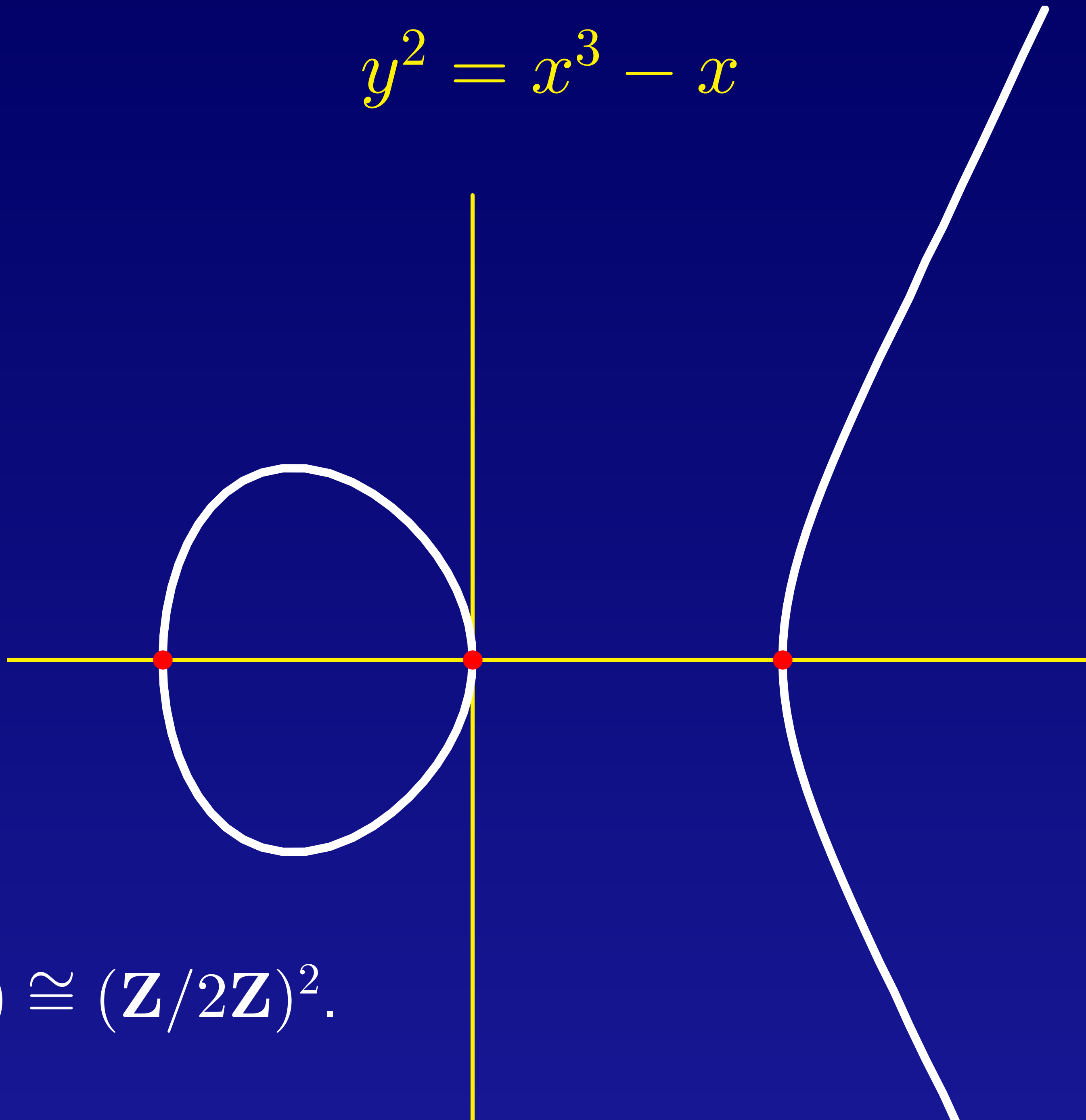
$$P = (x_1, y_1), \;\; Q = (x_2, y_2) \in E(\mathbf{Q})$$

with $x_1 \neq x_2$, then $P + Q = (x_3, y_3)$ with

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

$$y_3 = \left(\tfrac{y_2 - y_1}{x_2 - x_1}\right) x_3 - \left(\tfrac{y_1 x_2 - y_2 x_1}{x_2 - x_1}\right).$$

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



$$E(\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z})^2.$$

Mordell's Theorem

Theorem (Mordell 1922) $E(\mathbf{Q})$ *is a finitely generated commutative group.*

In other words,

$$E(\mathbf{Q}) \cong \mathbf{Z}^r \oplus \text{(finite group)}.$$

- The finite group is written $E(\mathbf{Q})_{\text{tors}}$, the subgroup of elements of finite order in $E(\mathbf{Q})$.
- The integer r is called the *rank* of E, and written $\text{rank}(E)$.

Torsion subgroups

Theorem (Nagell 1935, Lutz 1937). *If* $(x, y) \in E(\mathbf{Q})_{\text{tors}}$ *and* $(x, y) \neq \infty$, *then*

- $x, y \in \mathbf{Z}$,
- *either* $y = 0$ *or* y^2 *divides* Δ.

Theorem (Mazur 1977). $E(\mathbf{Q})_{\text{tors}}$ *is one of the following 15 groups:*

$$\mathbf{Z}/n\mathbf{Z}, \text{ with } 1 \leq n \leq 10 \text{ or } n = 12,$$

$$(\mathbf{Z}/2m\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z}), \text{ with } 1 \leq m \leq 4,$$

and each of these groups occurs infinitely often.

Ranks

Question. Given E, how can one compute rank(E)?

Question. Which ranks can occur?

- Can the rank be arbitrarily large?
- Is every positive integer the rank of some elliptic curve? Of infinitely many elliptic curves?
- What is the distribution of ranks?

The answers to these questions are not known.

Rank records

Rank $\geq$	**Year**	
4	1945	Wiman
6	1974	Penney & Pomerance
7	1975	Penney & Pomerance
8	1977	Grunewald & Zimmert
9	1977	Brumer & Kramer
12	1982	Mestre
14	1986	Mestre
15	1991	Mestre
17	1992	Nagao
19	1992	Fermigier
20	1993	Nagao
21	1994	Nagao & Kouya
22	1996	Fermigier
23	1998	Martin & McMillen
24	2000	Martin & McMillen

Rank records

$$y^2+xy+y = x^3-120039822036992245303534619191166796374x$$
$$+504224992484910670010801799168082726759443756222911415116$$

has rank at least 24. Some independent points:

$$(2005024558054813068, -16480371588343085108234888252),$$
$$(-4690836759490453344, -31049883525785801514744524804),$$
$$(4700156326649806635, -6622116250158424945781859743),$$
$$(6785546256295273860, -1456180928830978521107520473),$$
$$(7788809602110240789, -6462981622972389783453855713).$$

Rank records

Mestre has constructed an elliptic curve

$$y^2 = x^3 + f(t)x + g(t)$$

with polynomials $f(t)$, $g(t)$, which has rank 14 over the rational function field $\mathbf{Q}(t)$. Specializing to rational values of t gives infinitely many curves E_t defined over $\mathbf{Q}$ with rank at least 14.

Rank records

Rank of $E_d : y^2 = x^3 - d^2x$.

d	rank	
1	0	Fermat ($\sim$1640)
5	1	$(-4, 6)$
34	2	$(-2, 48), (-16, 120)$
1254	3	$(-98, 12376), (109554, 36258840), (1650, 43560)$
29274	4	Wiman (1945)
205015206	5	Rogers (2000)
61471349610	6	Rogers (2000)

Theorem. $\mathrm{rank}(E_d) < \log(d)$.

Idea of Birch and Swinnerton-Dyer

If p is a prime not dividing Δ, then we can reduce the equation for E modulo p, to think of E as an elliptic curve over the finite field $\mathbf{Z}/p\mathbf{Z}$.

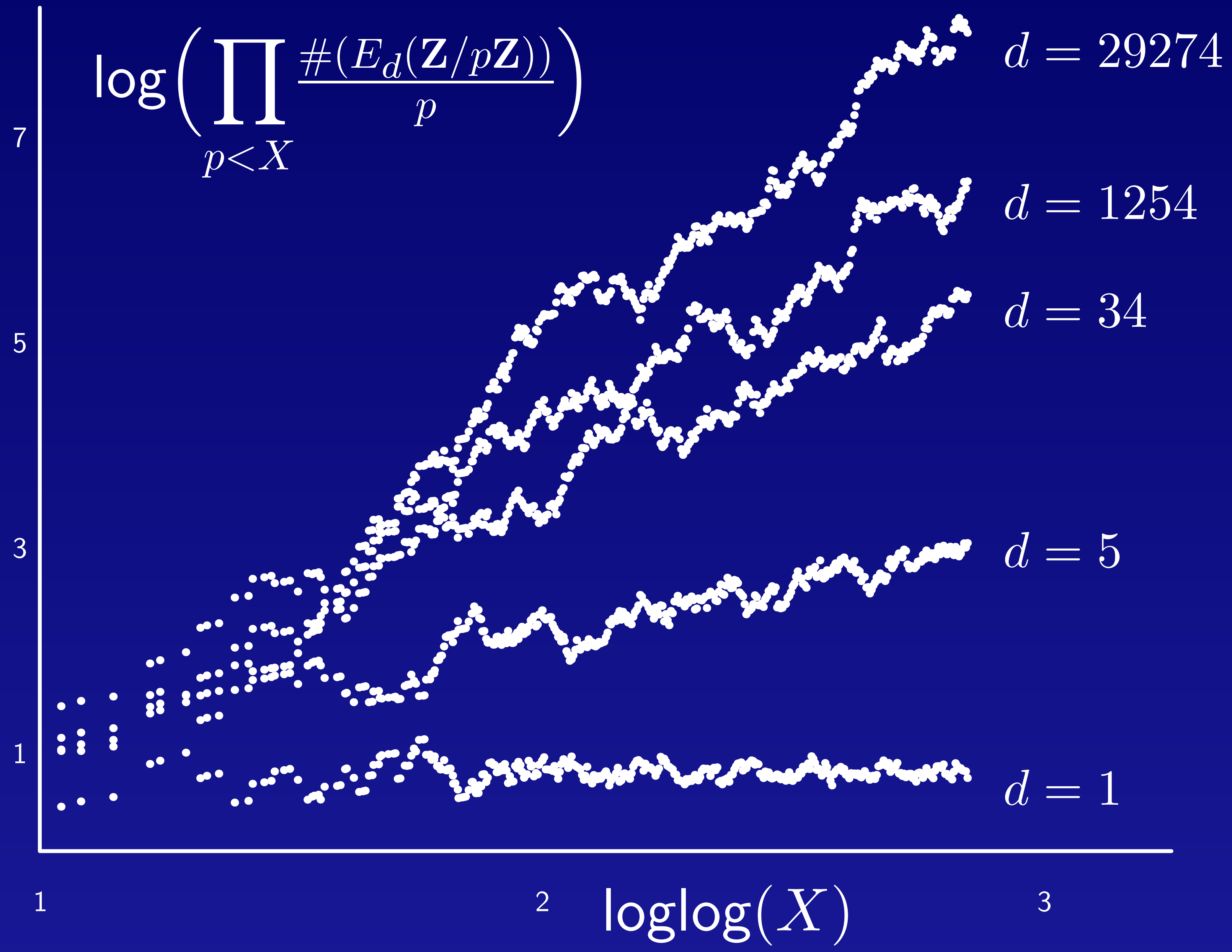
Birch and Swinnerton-Dyer suggested that the larger $E(\mathbf{Q})$ is, the larger the $E(\mathbf{Z}/p\mathbf{Z})$ should be "on average".

To check this, they computed

$$\prod_{p<X} \frac{\#(E(\mathbf{Z}/p\mathbf{Z}))}{p}$$

as X grows.

Idea of Birch and Swinnerton-Dyer



The L-function

Given E, define a Dirichlet series

$$L(E,s) = \prod_{p \nmid \Delta} \left(1 - \frac{1+p-\#E(\mathbf{Z}/p\mathbf{Z})}{p^s} + \frac{p}{p^{2s}}\right)^{-1} \prod_{p \mid \Delta} \left(1 + \frac{a_p}{p^s}\right)^{-1}$$

where $a_p = 0$ or ± 1 is given by an explicit recipe.

This converges if $\mathrm{Re}(s) > \frac{3}{2}$.

The L-function

Theorem (Wiles et al.). *$L(E, s)$ has an analytic continuation to $\mathbf{C}$ and a functional equation*

$$\Lambda(s) = w_E \Lambda(2 - s)$$

where $w_E = \pm 1$ and

$$\Lambda(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E, s)$$

with a positive integer N (the "conductor" of E).

The L-function

The Euler product

$$L(E,s) = \prod_{p \nmid \Delta} \left(1 - \frac{1+p-\#E(\mathbf{Z}/p\mathbf{Z})}{p^s} + \frac{p}{p^{2s}}\right)^{-1} \prod_{p \mid \Delta} \left(1 + \frac{a_p}{p^s}\right)^{-1}$$

need not converge at $s = 1$. But *purely formally*

$$L(E,1) \text{ ``}\sim\text{''} \prod_{p \nmid \Delta} \frac{p}{\#E(\mathbf{Z}/p\mathbf{Z})}.$$

So heuristically, the larger $E(\mathbf{Q})$ is, the larger the $\#E(\mathbf{Z}/p\mathbf{Z})$ will be, and the faster $L(E,s)$ should approach zero as $s \to 1$.

Birch and Swinnerton-Dyer Conjecture

Conjecture (Birch & Swinnerton-Dyer, $\sim$1960).
$\text{rank}(E) = \text{ord}_{s=1} L(E, s)$.

Theorem (Kolyvagin, Gross & Zagier, ... 1988).

(i) $\text{ord}_{s=1} L(E, s) = 0 \quad \Rightarrow \quad \text{rank}(E) = 0$.

(ii) $\text{ord}_{s=1} L(E, s) = 1 \quad \Rightarrow \quad \text{rank}(E) = 1$.

(iii) $\text{ord}_{s=1} L(E, s) \geq 2 \quad \Rightarrow \quad ???$

Example: $y^2 = x^3 - x$

For this E we have $\Delta = 64$ and

$$L(E,s) = \prod_{p \neq 2} (1 - \frac{a_p}{p^s} + \frac{p}{p^{2s}})^{-1}$$

where $a_p = \begin{cases} 0 & \text{if } p \equiv 3 \pmod 4, \\ 2n & \text{if } p \equiv 1 \pmod 4,\ p = n^2 + m^2 \\ & \quad \text{with } n \text{ odd},\ n \equiv m+1 \pmod 4. \end{cases}$

$L(E,1) = .65551538857302995\ldots$

Thus (as Fermat proved) this curve has rank zero.

Parity

Recall the functional equation $\Lambda(s) = w_E \Lambda(2-s)$ with $w_E = \pm 1$. It follows that

$$\mathrm{ord}_{s=1} L(E,s) = \mathrm{ord}_{s=1} \Lambda(E,s) \text{ is } \begin{cases} \text{even} & \text{if } w_E = +1 \\ \text{odd} & \text{if } w_E = -1. \end{cases}$$

Parity Conjecture (weak consequence of BSD).

$$\mathrm{rank}(E) \text{ is } \begin{cases} \text{even} & \text{if } w_E = +1 \\ \text{odd} & \text{if } w_E = -1. \end{cases}$$

Parity

Example. Let E_d be the elliptic curve $y^2 = x^3 - d^2x$, where d is a squarefree integer.

$$w_E = \begin{cases} +1 & \text{if } |d| \equiv 1, 2, \text{ or } 3 \pmod 8, \\ -1 & \text{if } |d| \equiv 5, 6, \text{ or } 7 \pmod 8. \end{cases}$$

So the Parity Conjecture implies that $\mathrm{rank}(E_d)$ is odd (and therefore nonzero!) for half of the squarefree integers d.

Theorem. If $p \equiv 5$ or $7 \pmod 8$ is prime, then $\mathrm{rank}(E_p) = 1$.

Parity

Theorem. If $p \equiv 5$ or $7 \pmod 8$ is prime, then rank$(E_p) = 1$.

Example: $p = 157$. The simplest rational point of infinite order on $y^2 = x^3 - (157)^2 x$ is

$$\Big(-\frac{43565582610691407250551997}{609760250665615167250729},$$
$$\frac{562653616877773225244609387368307126580}{47614438250616355400538204422249067}\Big).$$

Quadratic twists

More generally, if E is $y^2 = x^3 + ax + b$, the *quadratic twist* of E by a nonzero integer d is

$$E_d : y^2 = x^3 + ad^2x + bd^3.$$

After a change of variables we can rewrite this as

$$dy^2 = x^3 + ax + b.$$

- We may assume that d is squarefree.
- E and E_d are isomorphic over $\mathbf{C}$, but not over $\mathbf{Q}$, so $E(\mathbf{Q})$ and $E_d(\mathbf{Q})$ can be very different.

Ranks in a family of quadratic twists

Fix E. We want to study the distribution of rank(E_d) as d varies.

Let $S(X) = \{\text{squarefree } d : |d| < X\}$. Define

- the *average rank* $\mathrm{Avg}(E) = \lim\limits_{X\to\infty} \frac{\sum_{d\in S(X)} \mathrm{rank}(E_d)}{\#S(X)}$,
- $N_*(E,X) = \#\{d \in S(X) : \mathrm{rank}(E_d) \text{ is } *\}$, where the symbol $*$ can be "2", "odd", "≥ 3", etc.,
- the density $\mathrm{Dens}_*(E) = \lim\limits_{X\to\infty} \frac{N_*(E,X)}{\#S(X)}$,

if these limits exist.

Ranks in a family of quadratic twists

The Parity Conjecture implies

- $\mathrm{Dens}_{\mathrm{even}}(E) = 1/2$ and $\mathrm{Dens}_{\mathrm{odd}}(E) = 1/2$,
- $\mathrm{Avg}(E) \geq 1/2$.

Conjecture (Goldfeld 1979). $\mathrm{Avg}(E) = 1/2$.

Goldfeld's Conjecture says that the average rank is as small as the Parity Conjecture allows, which implies that

$$\mathrm{Dens}_0(E) = \mathrm{Dens}_1(E) = 1/2, \quad \mathrm{Dens}_{\geq 2}(E) = 0.$$

Ranks in the family $E_d : dy^2 = x^3 - x$

For the rest of the talk we fix E to be $y^2 = x^3 - x$.

Let $\mathrm{Avg}^o(E)$ and $\mathrm{Dens}^o_*(E)$ denote the average and density restricted to odd d.

Theorem (Heath-Brown 1994).

(i) $\mathrm{Avg}^o(E) \le 1.2645$

(ii) $\mathrm{Dens}_r(E) \le 1.7313 \cdot 2^{-(r^2-r)/2}$

(iii) $\mathrm{Dens}_0(E) > 0$.

Ranks in the family $E_d : dy^2 = x^3 - x$

Theorem (Gouvêa & Mazur, Stewart & Top, Rubin & Silverberg).

unconditionally	*assuming Parity Conjecture*
$N_{\geq 1}(E, X) \gg X^{1/2}$	$N_{\geq 1}(E, X) \gg X$
$N_{\geq 2}(E, X) \gg X^{1/3}$	$N_{\geq 2}(E, X) \gg X^{1/2}$
$N_{\geq 3}(E, X) \gg X^{1/6}$	$N_{\geq 3}(E, X) \gg X^{1/3}$
	$N_{\geq 4}(E, X) \gg X^{1/6}$

One expects $X^{3/4-\epsilon} \ll N_2(E, X) \ll X^{3/4+\epsilon}$,

$$X^{3/4-\epsilon} \ll N_3(E, X) \ll X^{3/4+\epsilon},$$

but nobody has a good guess for $N_4(E, X)$.

Ranks in the family $E_d : dy^2 = x^3 - x$

Idea of proof: Let $f(t) = 6(t^{12} - 33t^8 - 33t^4 + 1)$. Then

$$E_{f(t)} : f(t)y^2 = x^3 - x$$

is an elliptic curve over $\mathbf{Q}(t)$ with 3 independent points

$$\Big(-\tfrac{t^4-6t^2+1}{3(t^2+1)^2}, \tfrac{2}{9(t^2+1)^3}\Big), \Big(-\tfrac{t^4+6t^2+1}{3(t^2-1)^2}, \tfrac{2}{9(t^2-1)^3}\Big), \Big(\tfrac{t^4+1}{6t^2}, \tfrac{1}{36t^3}\Big)$$

Specializing to $t \in \mathbf{Q}$ gives many curves of rank at least 3. Counting them gives a lower bound for $N_{\geq 3}(E, X)$. Counting the ones with $w_{E_d} = +1$ gives a (conjectural) lower bound for $N_{\geq 4}(E, X)$.

More generally

Problem: *Given an elliptic curve*

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

and $r \in \mathbf{Z}^+$, find a polynomial $g(t) \in \mathbf{Q}[t]$ such that

$$E_{g(t)} : g(t)y^2 = x^3 + ax + b$$

has rank r over $\mathbf{Q}(t)$.

This would give an unconditional lower bound for $N_{\geq r}(E, X)$ and a conditional lower bound for $N_{\geq r+1}(E, X)$.

More generally

How to find such a $g(t)$, with r "large"? Suppose

- $E_{g(t)}$ has rank r over $\mathbf{Q}(t)$
- $E_{g(t)h(t)}$ has rank r' over $\mathbf{Q}(t)$.

Then $E_{g(t)}$ has rank $r + r'$ over $\mathbf{Q}(t, \sqrt{h(t)})$.

If $h(t)$ is *linear*, and $r' \geq 1$, then (with $u = \sqrt{h(t)}$)

- $\mathbf{Q}(t, \sqrt{h(t)}) = \mathbf{Q}(u)$
- $E_{g(t(u))}$ has rank at least $r + 1$ over $\mathbf{Q}(u)$.

More generally

- If E is $y^2 = x^3+ax+b$, start with $g(t) = t^3+at+b$. Then $r = 1$, from the point $(t, 1)$ on

$$E_{g(t)} : g(t)y^2 = x^3 + ax + b.$$

- Find (for some E) $h(t)$ so $E_{g(t)h(t)}$ has rank 1 over $\mathbf{Q}(t)$. This gives $E_{g(t(u))}$ with rank 2 over $\mathbf{Q}(u)$.

- Repeat with the new, rank-2 $g(t)$. Find (for some E) $h(t)$ so $E_{g(t)h(t)}$ has rank at least 1 over $\mathbf{Q}(t)$. This gives $E_{g(t(u))}$ with rank at least 3 over $\mathbf{Q}(u)$.

More generally

This is how the examples in the previous theorem were found.

There is no example known of a curve E and a $g(t) \in \mathbf{Q}(t)$ such that $E_{g(t)}$ has rank at least 4 over $\mathbf{Q}(t)$.

Ranks in the family $E_d : dy^2 = x^3 - x$

Given d, it may be hard to find $(x, y) \in E_d(\mathbf{Q})$.

But given x, it is *easy* to find y and d such that $(x, y) \in E_d(\mathbf{Q})$: we can write $x^3 - x$ uniquely as the square of a rational number y times a squarefree integer d.

If $t \in \mathbf{Q}^\times$, let $\mathrm{sf}(t)$ denote the *squarefree part* of t, the unique squarefree integer such that $t/\mathrm{sf}(t)$ is a square.

If $x \in \mathbf{Q}$, $x \neq 0, \pm 1$ then x is the x-coordinate of a point of infinite order in $E_{\mathrm{sf}(x^3-x)}(\mathbf{Q})$.

Ranks in the family $E_d : dy^2 = x^3 - x$

If $x = u/v$ with relatively prime integers u and v, and $B > 0$, define

$$h(x) = \mathsf{max}\{1, \mathsf{log}(u), \mathsf{log}(v)\},$$
$$M(d, B) = \{x \in \mathbf{Q} : h(x) < B, \mathsf{sf}(x^3 - x) = d\}.$$

Lemma. *For every d there is a $C_d \in \mathbf{R}^+$ such that for large B*

$$M(d, B) \sim C_d B^{\mathsf{rank}(E_d)/2}.$$

Thus $\mathsf{rank}(E_d) > \mathsf{rank}(E_{d'}) \Rightarrow M(d, B) > M(d', B)$ for sufficiently large B.

Searching for large ranks

- Let x run through all rational numbers x with $h(x) < B$ and make a list of the values $M(d, B)$.
- Pick out those d for which $M(d, B)$ is large, and compute $\mathrm{rank}(E_d)$.

N. Rogers implemented this method and found

$$\mathrm{rank}(E_{205015206}) = 5,$$
$$\mathrm{rank}(E_{61471349610}) = 6.$$

Searching for large ranks

If $a, b, c, d \in \mathbf{Z}^+$, let $\omega_{a,b,c,d} \in \mathbf{Z}^2$ be a shortest nonzero vector in the lattice

$$\{(u,v) \in \mathbf{Z}^2 : a^2 \mid u, b^2 \mid v, c^2 \mid u+v, d^2 \mid u-v\}$$

and define

$$Q(j,k) \;=\; \sideset{}{'}\sum_{a,b,c,d=1}^{\infty} \frac{(abcd)^{2k}}{\|\omega_{a,b,c,d}\|^{4k} h(\omega_{a,b,c,d})^j}$$

summing over a, b, c, d such that, if $\omega_{a,b,c,d} = (u,v)$, then u and v are relatively prime and $uv(u+v)(u-v) \neq 0$.

Searching for large ranks

Define $S(j,k) = \sum_{x \in \mathbf{Q} - \{0,1,-1\}} |\mathsf{sf}(x^3 - x)|^{-k} h(x)^{-j}$.

Theorem (Rubin & Silverberg). *If $j \in \mathbf{R}^+$, then the following are equivalent.*

(i) $\mathrm{rank}(E_d) < 2j$ for every $d \in \mathbf{Z}^+$,

(ii) $S(j,k)$ converges for some $k \geq 1$,

(iii) $S(j,k)$ converges for every $k \geq 1$,

(iv) $Q(j,k)$ converges for some $k \geq 1$,

(v) $Q(j,k)$ converges for every $k \geq 1$.