Ranks of elliptic curves

Karl Rubin

January 20, 2000

http://math.stanford.edu/~rubin

Elliptic curves

An elliptic curve over the field $\mathbb{Q}$ of rational numbers is a curve E defined by a cubic equation

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

where $a, b \in \mathbb{Z}$ and

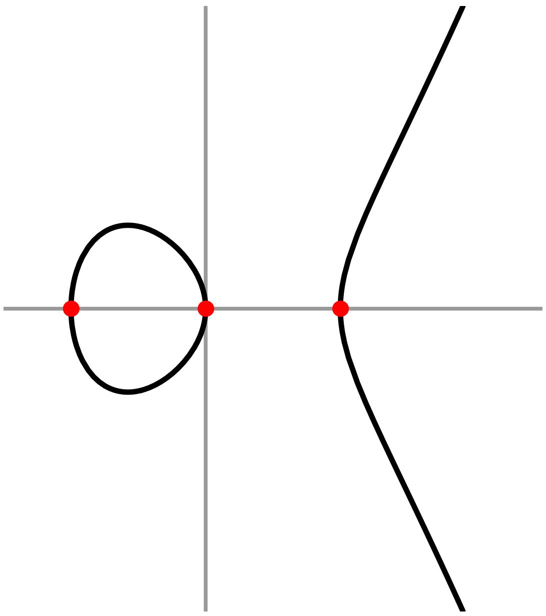
$$\Delta = -16(4a^3 + 27b^2) \neq 0.$$

(More generally we may suppose that E is non-singular and given by an equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in \mathbb{Q}$.)

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



Basic problem:

Given an elliptic curve E, find all rational solutions.

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

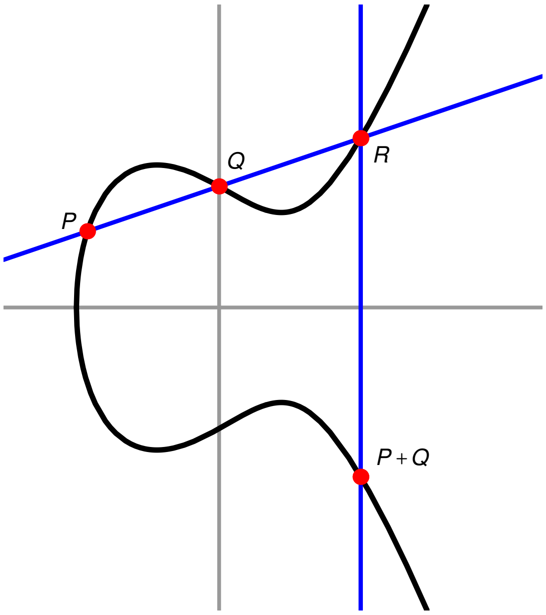
(If we view E as a curve in projective space, it has one point at "infinity"; this point lies on all vertical lines.)

Example (Fermat).

$$E : y^2 = x^3 - x,$$

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

$$y^2 = x^3 - x + 1$$



$P = (-\frac{11}{9}, \frac{17}{27})$, $Q = (0, 1)$, $P + Q = (\frac{159}{121}, -\frac{1861}{1331})$

Addition law

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

3 collinear points sum to zero

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

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

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

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

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

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

Mordell's Theorem

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

In other words, there is always a *finite* set of points $P_1, \ldots, P_k$ which generate all points in $E(\mathbb{Q})$ using the geometric chord-and-tangent process.

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

The finite group is written $E(\mathbb{Q})_{\text{tors}}$, the subgroup of elements of finite order in $E(\mathbb{Q})$.

The integer r is called the *rank* of E, and written $\text{rank}(E)$.

In Fermat's example ($E : y^2 = x^3 - x$), recall that $E(\mathbb{Q})$ has 4 points.

The three points different from ∞ all satisfy $P + P = \infty$. Therefore

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

Thus

$$E(\mathbb{Q})_{\text{tors}} = E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2,$$

$$\text{rank}(E) = 0.$$

What can we say about $E(\mathbb{Q})_{\text{tors}}$ and $\text{rank}(E)$ for general E?

Torsion subgroup

Theorem (Nagell 1935, Lutz 1937). *Suppose E is the elliptic curve $y^2 = x^3 + ax + b$. If $(x, y) \in E(\mathbb{Q})_{\text{tors}}$, $(x, y) \neq \infty$, then*

(i) $x, y \in \mathbb{Z}$,

(ii) *either $y = 0$ or y^2 divides $4a^3 + 27b^2$.*

Theorem (Mazur 1977). *If E is an elliptic curve then $E(\mathbb{Q})_{\text{tors}}$ is one of the following 15 groups:*

$\mathbb{Z}/n\mathbb{Z}$, *with* $1 \le n \le 10$ *or* $n = 12$,

$(\mathbb{Z}/2m\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, *with* $1 \le m \le 4$.

Each of these groups occurs infinitely often.

Examples of torsion subgroups

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

By the Nagell-Lutz theorem, we only need to check $y = 0, \pm 1, \pm 2$ and integers x. The only such solutions are $y = 0$ and $x = 0, 1, -1$.

Example. Suppose $t \in \mathbb{Q}$, and $t \neq 0, -1$. Define E by

$$y^2 + (1 - t - t^2)xy + (t^2 + t^3)y = x^3 + (t^2 + t^3)x^2.$$

Then $(0, 0) \in E(\mathbb{Q})$, and one can check that

$$7 \cdot (0, 0) = \infty.$$

By Mazur's theorem, the group generated by $(0, 0)$ must be all of $E(\mathbb{Q})_{\text{tors}}$, so

$$E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/7\mathbb{Z}.$$

Conversely, one can show that every elliptic curve with torsion subgroup of order 7 is isomorphic to a curve defined by the equation above, for some $t \in \mathbb{Q}$.

Ranks

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

Question. *Which ranks can occur?*

- *Is every positive integer the rank of some elliptic curve?*
- *Is every positive integer the rank of infinitely many elliptic curves?*

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

Notes: In 1954 Néron showed there exists E with rank ≥ 11, but his proof did not give an example.

Kihara (1997) found an infinite family of curves all with rank at least 14.

See horizontal slide #1

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

d	rank(E_d)	
1	0	Fermat ∼1640
5	1	$(-4, 6)$
34	2	$(-98, 1176)$, $(350, 5880)$
1254	3	
29274	4	Wiman 1945
205015206	5	Rogers 1999
61471349610	6	Rogers 1999

Fact. *There is a right triangle with rational sides and area d if and only if* rank(E_d) > 0.

For every prime number p let

$$N_p = \#\Big\{0 \le x, y \le p-1 : y^2 \equiv x^3 + ax + b \pmod{p}\Big\} + 1 = \#(E(\mathbb{Z}/p\mathbb{Z})).$$

Idea of Birch and Swinnerton-Dyer: *The more rational solutions there are of the equation*

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

the larger the N_p will be "on average".

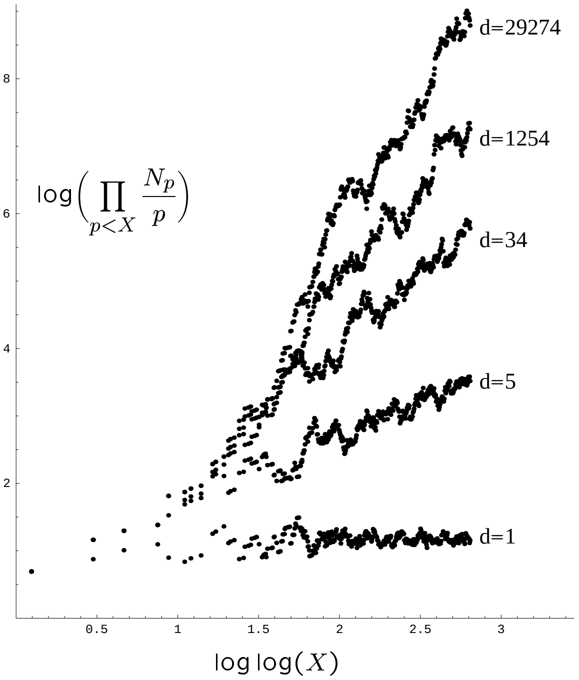
How can this be measured?

Birch and Swinnerton-Dyer computed

$$\prod_{p \le X} \frac{N_p}{p}$$

as X grows.

$E_d : y^2 = x^3 - d^2x$



The L-function

Given E, define a function of a complex variable s

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

where $a_p = 0$, 1, or -1.

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

So we can't evaluate it at $s = 1$. But if we could, we would get

$$L(E,1) \text{ “=” } \prod_{p \nmid \Delta} \left(\frac{N_p}{p}\right)^{-1} \prod_{p \mid \Delta} \left(1 + \frac{a_p}{p}\right)^{-1}$$

Theorem. *$L(E,s)$ has an analytic continuation to all of $\mathbb{C}$, and satisfies a functional equation*

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

where $w_E = \pm 1$ and

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

for an appropriate positive integer N.

Thus we can expand $L(E,s)$ in a power series at $s = 1$

$$L(E,s) = \sum_{i=n}^{\infty} c_i (s-1)^i$$

with $n \geq 0$, $c_n \neq 0$. Define $\mathrm{ord}_{s=1} L(E,s) = n$.

Conjecture (Birch and Swinnerton-Dyer, ~1960). *For every elliptic curve E,*

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

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

$$\mathrm{ord}_{s=1} L(E,s) = 0 \Rightarrow \mathrm{rank}(E) = 0$$
$$\mathrm{ord}_{s=1} L(E,s) = 1 \Rightarrow \mathrm{rank}(E) = 1$$

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

Example. If E is Fermat's curve $y^2 = x^3 - x$, then

$$L(E,1) = 0.65551438857302995... \neq 0.$$

Thus $\mathrm{ord}_{s=1} L(E,s) = 0$, so (as Fermat said) $\mathrm{rank}(E) = 0$.

The sign in the functional equation determines the parity of $\mathrm{ord}_{s=1} L(E,s)$:

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

Thus the Birch and Swinnerton-Dyer conjecture predicts the following.

Parity Conjecture.

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

Example. Let E_d be $y^2 = x^3 - d^2 x$. Then

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

Thus conjecturally, $\mathrm{rank}(E_d)$ is odd (and therefore nonzero!) for half of the positive squarefree integers d.

From now on we will consider only the family of curves $E_d : y^2 = x^3 - d^2x$.

Theorem (Tunnell 1983).

$$L(E_d, 1) = \frac{(n-2m)^2 a\Omega}{16\sqrt{d}}$$

where

$a = 1$ *if* d *is odd,* $a = 2$ *if* d *is even,*

$n = \#\{(x,y,z) \in \mathbb{Z}^3 : x^2 + 2ay^2 + 8z^2 = \frac{d}{a}\}$,

$m = \#\{(x,y,z) \in \mathbb{Z}^3 : x^2 + 2ay^2 + 32z^2 = \frac{d}{a}\}$,

$\Omega = \int_1^\infty \frac{dx}{\sqrt{x^3 - x}} \approx 2.6220575542921198\ldots$

In particular

$$L(E_d, 1) = 0 \iff n = 2m.$$

Example. If $d = 1$, then $m = n = 2$ and

$$L(E_1, 1) = \frac{\Omega}{4}.$$

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

Fact. $\text{rank}(E_d) \le \log(d)$.

Let $S(X) = \{\text{squarefree } d \in \mathbb{Z}^+ : d \le X\}$.

Define the average rank to be

$$\lim_{X\to\infty} \frac{\sum_{d \in S(X)} \text{rank}(E_d)}{\#(S(X))},$$

and define the density of the set of curves with rank r to be

$$\lim_{X\to\infty} \frac{\#\{d \in S(X) : \text{rank}(E_d) = r\}}{\#(S(X))},$$

if these limits exist. Similarly we can define the density of the set of curves with rank at least r, with odd rank, etc.

The Parity conjecture implies:

- The set of curves with even rank has density 1/2, and the set of curves with odd rank has density 1/2.
- The average rank is at least 1/2.

Conjecture (Goldfeld 1979). *The average rank is* 1/2.

I.e., the average rank is as small as the Parity conjecture allows.

Goldfeld's conjecture + Parity conjecture imply:

- The set of curves with rank zero has density 1/2,
- The set of curves with rank one has density 1/2,
- The set of curves with rank at least two has density zero.

Let $S_{\text{odd}}(X) = \{\text{odd squarefree } d : d \le X\}$.

Theorem (Heath-Brown 1994).

1) $$\limsup_{X\to\infty} \frac{\sum_{d \in S_{\text{odd}}(X)} \text{rank}(E_d)}{\#(S_{\text{odd}}(X))} \le 1.2645.$$

2) $$\limsup_{X\to\infty} \frac{\#\{d \in S_{\text{odd}}(X) : \text{rank}(E_d) \ge R\}}{\#(S_{\text{odd}}(X))} \le 1.7313 \cdot 2^{-\left(\frac{R^2-R}{2}\right)}.$$

3) $$\liminf_{X\to\infty} \frac{\#\{d \in S_{\text{odd}}(X) : \text{rank}(E_d) = 0\}}{\#(S_{\text{odd}}(X))} > 0.$$

4) *If the Parity conjecture is true, then*

$$\liminf_{X\to\infty} \frac{\#\{d \in S_{\text{odd}}(X) : \text{rank}(E_d) = 1\}}{\#(S_{\text{odd}}(X))} > 0.$$

Lower bounds for ranks

By change of variables we can replace E_d by

$$E^{(d)}: dy^2 = x^3 - x.$$

Given d, it is not easy to find points in $E^{(d)}(\mathbb{Q})$. But:

Idea of Gouvêa and Mazur: Given $x \in \mathbb{Q}$, we can find d and y such that $(x,y) \in E^{(d)}(\mathbb{Q})$.

For every nonzero $r \in \mathbb{Q}$, there is a unique squarefree integer $s(r)$ such that $r = s(r)y^2$ with $y \in \mathbb{Q}$. Call $s(r)$ the squarefree part of r.

Suppose $x \in \mathbb{Q}$, $x \neq 0, 1, -1$. If we let

$$d = s(x^3 - x), \quad y = \sqrt{(x^3 - x)/d},$$

then

$$(x,y) \in E^{(d)}(\mathbb{Q}).$$

Further, $(x,y) \notin E^{(d)}(\mathbb{Q})_{\text{tors}}$.

If $d = s(x^3 - x)$ for some rational number x, then $\text{rank}(E_d) \geq 1$.

If $d = s(x^3 - x)$ for some rational number x, and $d \equiv 1, 2$ or $3 \pmod 8$, and the Parity conjecture holds, then $\text{rank}(E_d) \geq 2$.

By estimating how many d occur in this way:

Theorem (Gouvêa and Mazur 1991). *Suppose that the Parity conjecture holds. If ϵ is a positive real number, then for all sufficiently large X*

$$\#\{d \in S(X) : \text{rank}(E_d) \geq 2\} > X^{1/2-\epsilon}.$$

The methods of Gouvêa and Mazur were extended by Stewart and Top.

For the rest of the lecture everything is joint work with A. Silverberg.

Theorem. *There is a constant $C > 0$ such that for all sufficiently large X,*

(i) $\#\{d \in S(X) : \text{rank}(E_d) \geq 2\} > CX^{1/3}$,

(ii) $\#\{d \in S(X) : \text{rank}(E_d) \geq 3\} > CX^{1/6}$,

and if the Parity conjecture holds,

(iii) $\#\{d \in S(X) : \text{rank}(E_d) \geq 4\} > CX^{1/6}$.

Sketch of proof. Consider (ii). Let

$$f(t) = 6(t^2 - 4t + 2)(t^4 - 4t^3 + 6t^2 - 4t + 2) \cdot (t^2 - 2)(t^4 - 4t^3 + 12t^2 - 16t + 8).$$

For all but finitely many rational numbers t, $\text{rank}(E_{s(f(t))}) \geq 3$. Following Gouvêa & Mazur and Stewart & Top one can bound below the number of $d < X$ which occur as $s(f(t))$ for some rational t.

See horizontal slide #2

Looking for large rank(E_d)

Instead of just counting how many d's occur as $s(x^3 - x)$, count *how often* each d occurs.

If $x \in \mathbb{Q}$, $x \neq 0$, define

$$h(x) = \max\{1, \log|u|, \log|v|\}$$

where $x = u/v$ with relatively prime integers u, v.

For $B > 0$ let

$$N(d, B) = \#\{x \in \mathbb{Q} : h(x) < B,\ s(x^3 - x) = d\}.$$

Fact. *For every d there is a $C_d > 0$ such that for large B,*

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

So if rank(E_d) > rank($E_{d'}$), then for sufficiently large B we will always have $N(d, B) > N(d', B)$.

Computational method

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

N. Rogers implemented this method and found

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

Rubin and Silverberg implemented this method with rational functions $u(t)/v(t)$ instead of rational numbers x, and found

$$\mathrm{rank}(E_{f(t)}) = 3$$

for the polynomial $f(t)$ of degree 12 given earlier.

Theoretical method

1. Define

$$S(j, k) = \sum_{x \in \mathbb{Q} - \{0,1,-1\}} |s(x^3 - x)|^{-k} h(x)^{-j}$$

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

$$\left\{(u, v) \in \mathbb{Z}^2 : \begin{array}{cc} a^2 \mid u, & b^2 \mid v, \\ c^2 \mid u + v, & d^2 \mid u - v \end{array}\right\}$$

and define

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

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

Theorem. *If j is a positive real number, then the following are equivalent:*

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

(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* $k \geq 1$.