Ranks

Question. *How can one compute the rank of an elliptic curve?*

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?
- How are ranks distributed?

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

Martin-McMillen [2000]

The elliptic curve

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

has rank at least 24. Some independent points:

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

Rank records

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

d	rank	
1	0	Fermat (∼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 (1999)
61471349610	6	Rogers (1999)
157	1	

$\mathrm{rank}(E_{157}) = 1.$

The simplest point of infinite order in $E_{157}(\mathbb{Q})$ is

$$\Big(-\frac{43565582610691407250551997}{609760250665615167250729},$$

$$\frac{562653616877773225244609387368307126580}{476144382506163554005382044222449067}\Big).$$

Idea of Birch & Swinnerton-Dyer

For prime numbers p not dividing the discriminant of E, let

$$N_p = \#(E(\mathbb{F}_p)).$$

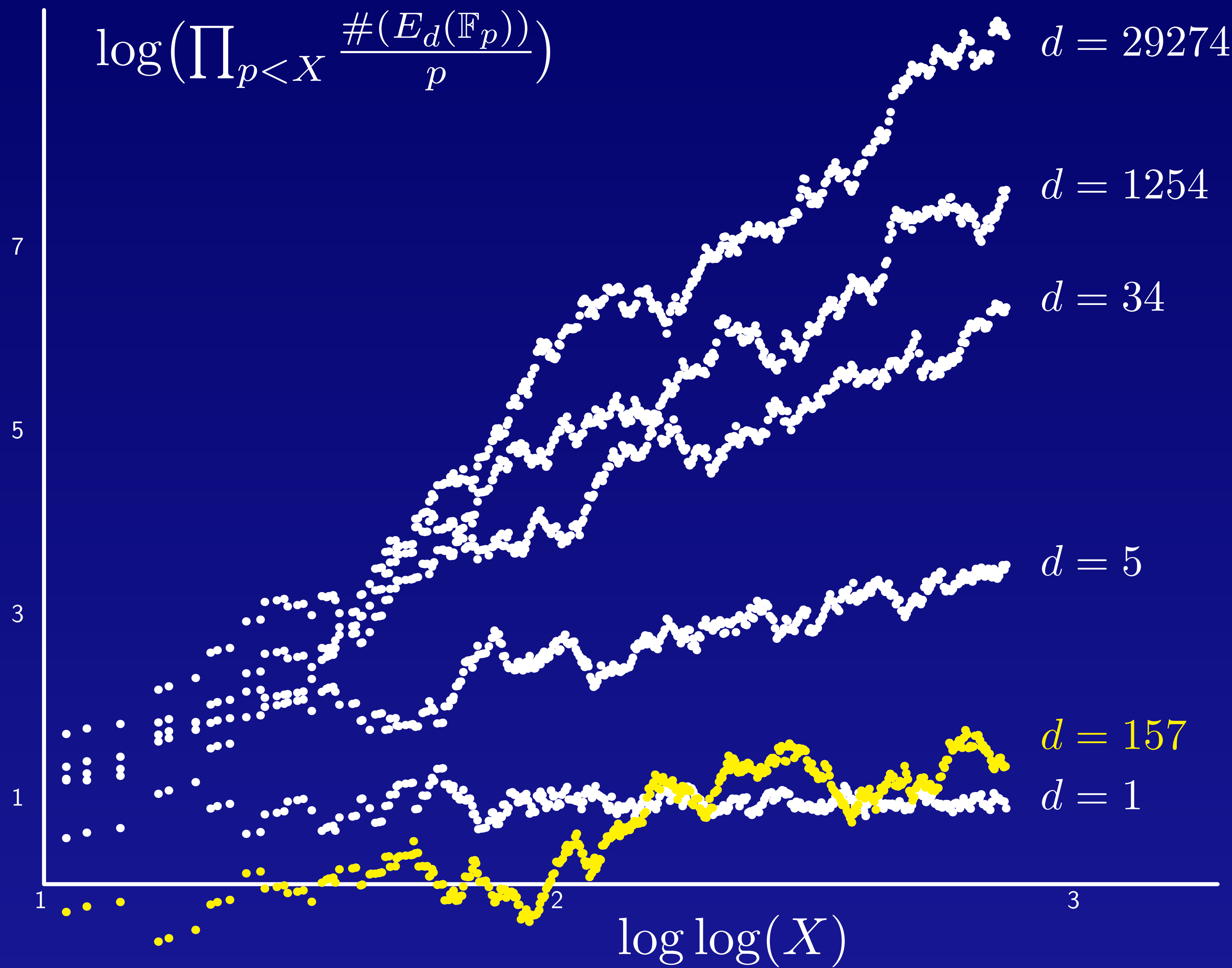
Idea: Recall the reduction map

$$E(\mathbb{Q}) \longrightarrow E(\mathbb{F}_p).$$

The more rational points $E(\mathbb{Q})$ has, the larger the N_p will be "on average". How can this be measured?

Birch and Swinnerton-Dyer computed $\displaystyle\prod_{p \le X} \frac{N_p}{p}$ as X grows.

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



Karl Rubin, Ross program July 2003

The L-function

Given E, define a function of a complex variable s

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

where $a_p = 0$, 1, or -1. This converges if $\mathrm{Re}(s) > 3/2$, because $|1+p-N_p| < 2\sqrt{p}$. So we can't evaluate it at $s=1$. But if we could, we would get

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

Theorem (Wiles et al. 1999). *$L(E,s)$ 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.

Conjecture (Birch & Swinnerton-Dyer, $\sim$1960).

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

Theorem (Kolyvagin, Gross & Zagier. . . 1989).

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

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

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

Example. If E is $y^2 = x^3 - x$, then

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

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

Parity

Recall the functional equation $\Lambda(s) = w_E \Lambda(2-s)$, where $\Lambda(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$. The sign w_E 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.

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

Parity

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

Theorem (Heegner, Birch, Monsky, . . .). *If p is an odd prime then*

$$\mathrm{rank}(E_p) = \begin{cases} 0 & \textit{if } p \equiv 1 \textit{ or } 3 \pmod 8, \\ 1 & \textit{if } p \equiv 5 \textit{ or } 7 \pmod 8. \end{cases}$$

Right triangles

From now on we fix $E_d : y^2 = x^3 - d^2x$.

Recall that there is a right triangle with rational sides and area d if and only if E_d has a rational point (x, y) with $y \neq 0$.

We also know that

$$E_d(\mathbb{Q})_{\mathrm{tors}} = \{(x, y) \in E_d(\mathbb{Q}) : y = 0\} \cong \mathbb{Z}/2\mathbb{Z}.$$

Theorem. *There is a right triangle with rational sides and area d if and only if $\mathrm{rank}(E_d) > 0$.*

Conjecture. *If $d \equiv 5, 6,$ or $7 \pmod 8$ then there is a right triangle with rational sides and area d.*

Theorem (Tunnell 1983). *If $d > 0$ is squarefree, then*

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

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

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

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

$$\Omega = \int_1^\infty \frac{dx}{\sqrt{x^3 - x}} \approx 2.622057554292119\ldots$$

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

d	1	2	3	5	6	7	10	11	34	$8k+5$	$8k+6$	$8k+7$
n	2	2	4	0	0	0	4	12	8	0	0	0
m	2	2	4	0	0	0	4	2	4	0	0	0

Triangles:

d	a	b	c
5	$3/2$	$20/3$	$41/6$
6	3	4	5
7	$35/12$	$24/5$	$337/60$
34	$17/6$	24	$145/6$
157	$\dots$	$\dots$	$\dots$

Distribution of ranks

What is known about the distribution of ranks?

Philosophy:

- ranks can be arbitrarily large, but large ranks are sparse,
- on average, ranks tend to be as small as "possible".

Distribution of ranks

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

Define the *average rank* to be

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

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

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

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

Distribution of ranks

The Parity conjecture implies:

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

Conjecture (Goldfeld). *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 $= 0$ has density $1/2$,
- The set of curves with rank $= 1$ has density $1/2$,
- The set of curves with rank ≥ 2 has density zero.

Distribution of ranks

Let $S_{\mathrm{odd}}(X) = \{\text{odd squarefree } d : 0 < d \le X\}$.

Theorem (Heath-Brown 1994).

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

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

(iii) $$\liminf_{X\to\infty} \frac{\#\{d\in S(X) \;:\; \mathrm{rank}(E_d)=0\}}{\#(S(X))} > 0.$$

Distribution of ranks

Theorem (Gouvêa & Mazur, Stewart & Top, Rubin & Silverberg). *There is a constant* $C > 0$ *such that for all sufficiently large* X*,*

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

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

and if the Parity conjecture holds,

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

Distribution of ranks

Sketch of proof. Let

$$g(t) = 6(t^6 - 33t^4 - 33t^2 + 1).$$

Then $\mathrm{rank}(E_{g(t)}(\mathbb{Q}(t)) = 2$ and $\mathrm{rank}(E_{g(t^2)}(\mathbb{Q}(t)) = 3$, where $Q(t)$ is the field of rational functions in the variable t (with coefficients in $\mathbb{Q}$), and $E_{g(t)}$ is the elliptic curve $y^2 = x^3 - g(t)^2 x$ over $\mathbb{Q}(t)$.

For example, the following are independent points on $E_{g(t^2)}$:

$$P_1(t) = \left(-\tfrac{t^4-6t^2+1}{3(t^2+1)^2}, \tfrac{2}{9(t^2+1)^3}\right), \quad P_2(t) = \left(\tfrac{t^4+1}{6t^2}, \tfrac{1}{36t^3}\right),$$
$$P_3(t) = \left(-\tfrac{t^4+6t^2+1}{3(t^2-1)^2}, \tfrac{2}{9(t^2-1)^3}\right).$$

Distribution of ranks

Theorem. *For all but finitely many rational numbers* t_0,

$$\operatorname{rank}(E_{g(t_0)}(\mathbb{Q})) \geq 2, \quad \operatorname{rank}(E_{g(t_0^2)}(\mathbb{Q})) \geq 3.$$

By plugging in lots of values of t, we get lots of curves of rank at least 3. Gouvêa & Mazur and Stewart & Top show how to count the number of curves E_d that appear this way, and we get

$$\#\{d \in S(X) : \operatorname{rank}(E_d) \geq 3\} \; > \; CX^{1/6}.$$

Distribution of ranks

Theorem. *For all but finitely many rational numbers* t_0,

$$\mathrm{rank}(E_{g(t_0)}(\mathbb{Q})) \geq 2, \quad \mathrm{rank}(E_{g(t_0^2)}(\mathbb{Q})) \geq 3.$$

Among the curves produced this way with rank at least 3, a positive proportion "should" have even rank. This (conjecturally) gives us lots of curves of rank at least 4. So assuming the Parity Conjecture we get

$$\#\{d \in S(X) : \mathrm{rank}(E_d) \geq 4\} \ > \ C' X^{1/6}.$$

Looking for curves of large rank

How can we efficiently look for curves of large rank?

Use the Birch and Swinnerton-Dyer idea:

- Given E, compute $|E(\mathbb{F}_p)|$ for lots of p. If "most" of these satisfy $|E(\mathbb{F}_p)| > p+1$, then this curve is a good candidate for high rank.

Use families:

- Mestre constructed an elliptic curve E over $\mathbb{Q}(t)$ of rank 12. Plugging in rational values of t gives an infinite family of elliptic curves over $\mathbb{Q}$ of rank at least 12. Searching among these curves, and using the BSD idea to look for the best candidates, has produced all known curves of large rank.

```
From owner-nmbrthry@LISTSERV.NODAK.EDU  Fri Jul 18 12:03:36 2003
Date:          Fri, 18 Jul 2003 12:02:55 -0400
From: Noam Elkies <elkies@math.harvard.edu>
Subject:       Rank records for x^3+y^3=k, cont'd
To: NMBRTHRY@LISTSERV.NODAK.EDU

We have found the first known cases of an elliptic curve x^3+y^3=k
of rank 9 over Q.  The 3-isogenous curves XY(X+Y)=k are also the
first known example of an elliptic curve of any form over Q
whose Mordell-Weil group is  Z^9 \oplus Z/3Z; according to
<www.math.hr/~duje/tors/z3.html>, the rank record for curves
with a rational 3-torsion point was 8.  One such k is

k = 18686874226924241 = 13 * 23 * 31 * 43 * 61 * 73 * 157 * 199 * 337.

The resulting curve with M-W group  Z^9 \oplus Z/3Z  has minimal form
[0,0,1,0,(k^2-1)/4] = [0,0,1,0,87299817093221362429969788356520]
(i.e. Y^2 + Y = X^3 + (k^2-1)/4 = X^3 + 87299817093221362429969788356520),
with 3-torsion point  (0,(k-1)/2) = (0,9343437113462120)
and 9 independent rational points

[-34739896854, 6735993625205487],   [59816792760, 17358779174601879],
[-44207258970, 9520387929815O4],   [6576595440, 9358646559113879],
[55473407808, 16062629859888488],   [-19255568904, 8953228261141352],
[101583478425/4, 81458264395412407/8],   [-162960849255/4, 35490296320657335/8],
[5040498496762O4337/3161284, 361690636655007439985736621/5620762952],
```