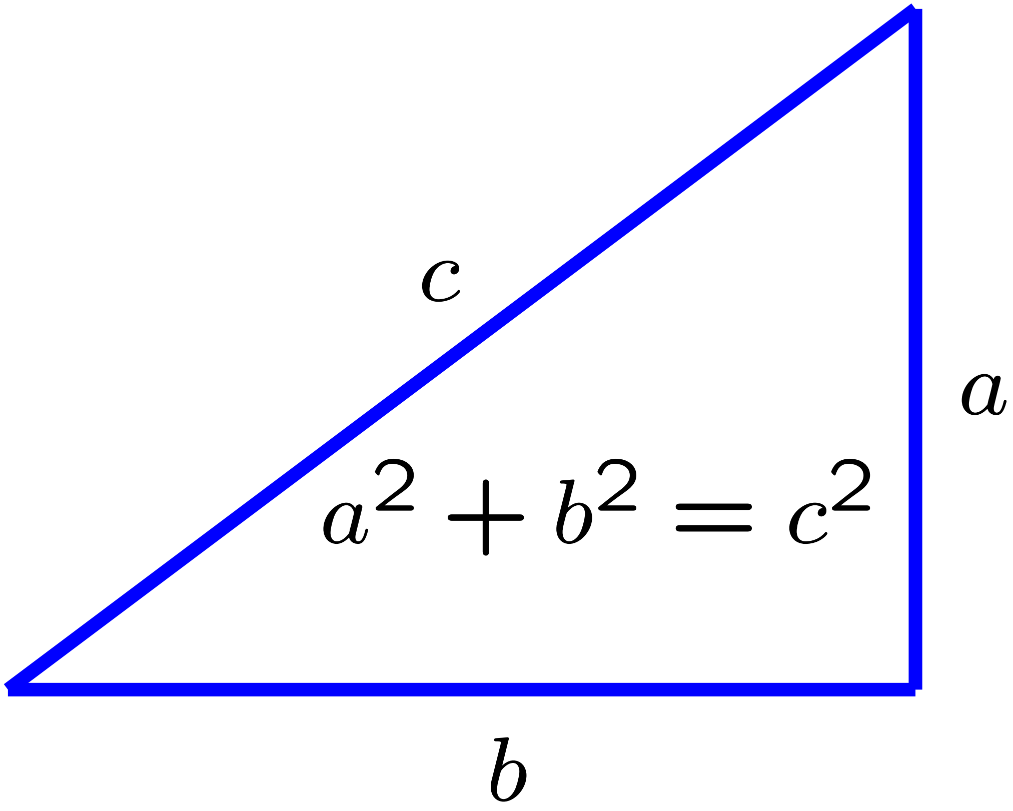
The Birch and Swinnerton-Dyer Conjecture

William Stein

February 11, 2005, Dartmouth

The Pythagorean Theorem

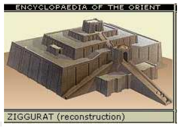


$$a^2 + b^2 = c^2$$

Pythagoras
Approx 569–475BC

Pythagorean Triples

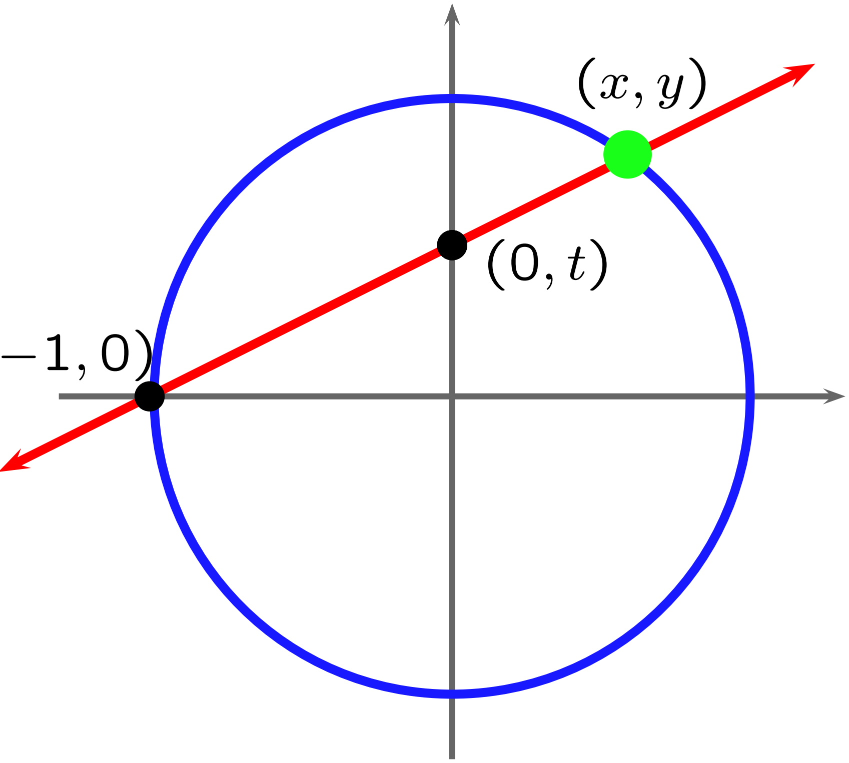
$(3, 4, 5)$
$(5, 12, 13)$
$(7, 24, 25)$
$(9, 40, 41)$
$(11, 60, 61)$
$(13, 84, 85)$
$(15, 8, 17)$
$(21, 20, 29)$
$(33, 56, 65)$
$(35, 12, 37)$
$(39, 80, 89)$
$(45, 28, 53)$
$(55, 48, 73)$
$(63, 16, 65)$
$(65, 72, 97)$
$(77, 36, 85)$
$\vdots$



Triples of integers a, b, c such that

$$a^2 + b^2 = c^2$$

Enumerating Pythagorean Triples



$$\text{Slope} = t = \frac{y}{x+1}$$

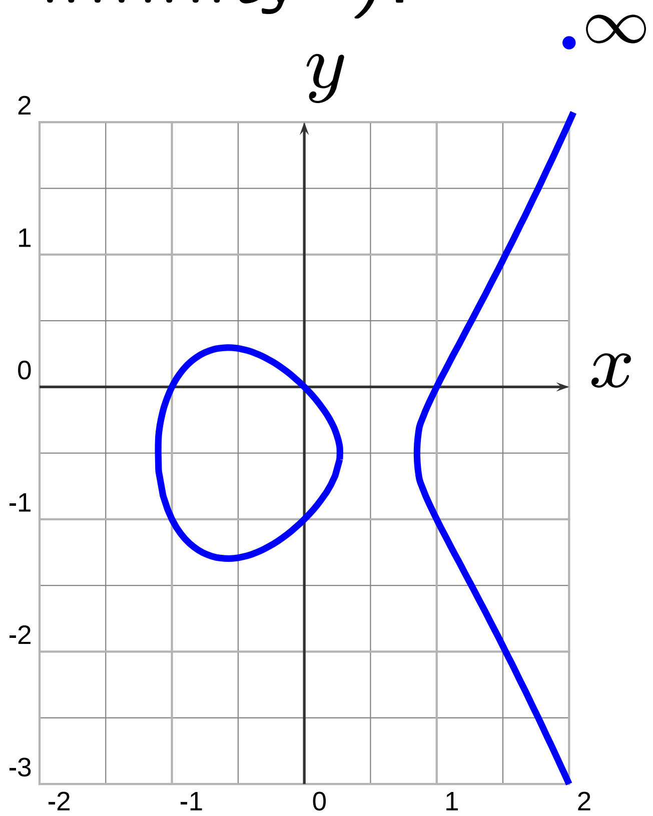
$$x = \frac{1-t^2}{1+t^2}$$

$$y = \frac{2t}{1+t^2}$$

If $t = \frac{r}{s}$, then $a = s^2 - r^2, \quad b = 2rs, \quad c = s^2 + r^2$
is a Pythagorean triple, and all primitive unordered triples arise in this way.

Elliptic Curves over the Rational Numbers $\mathbb{Q}$

An **elliptic curve** is a nonsingular plane cubic curve with a rational point (possibly “at infinity”).



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

EXAMPLES

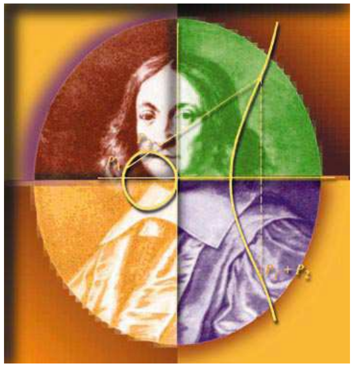
$$y^2 + y = x^3 - x$$

$$x^3 + y^3 = z^3 \text{ (projective)}$$

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

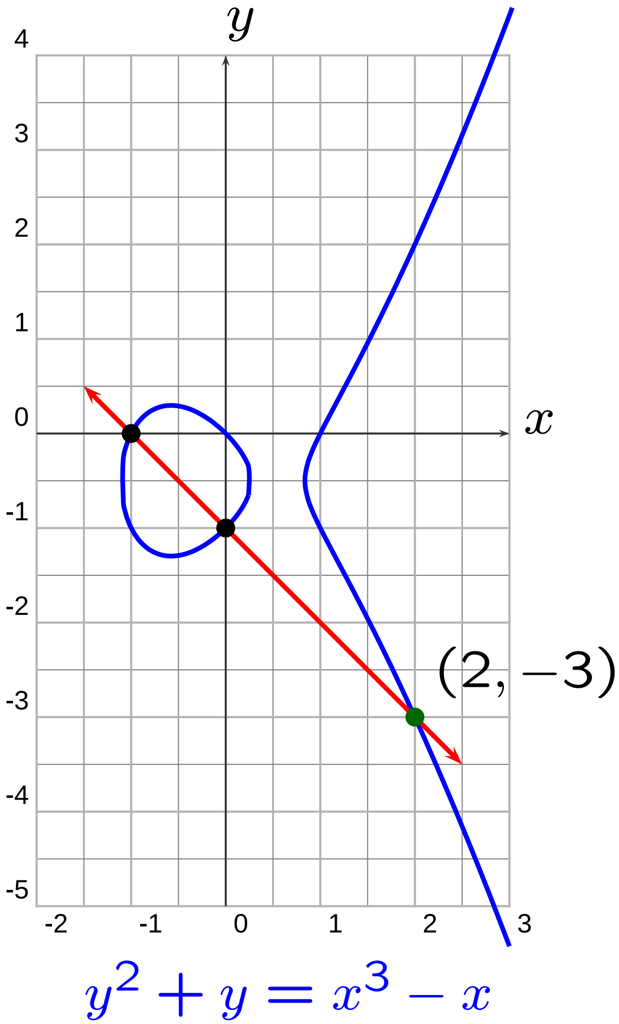
$$\xcancel{3x^3 + 4y^3 + 5z^3 = 0}$$

The Secant Process

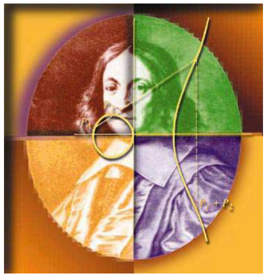


Fermat

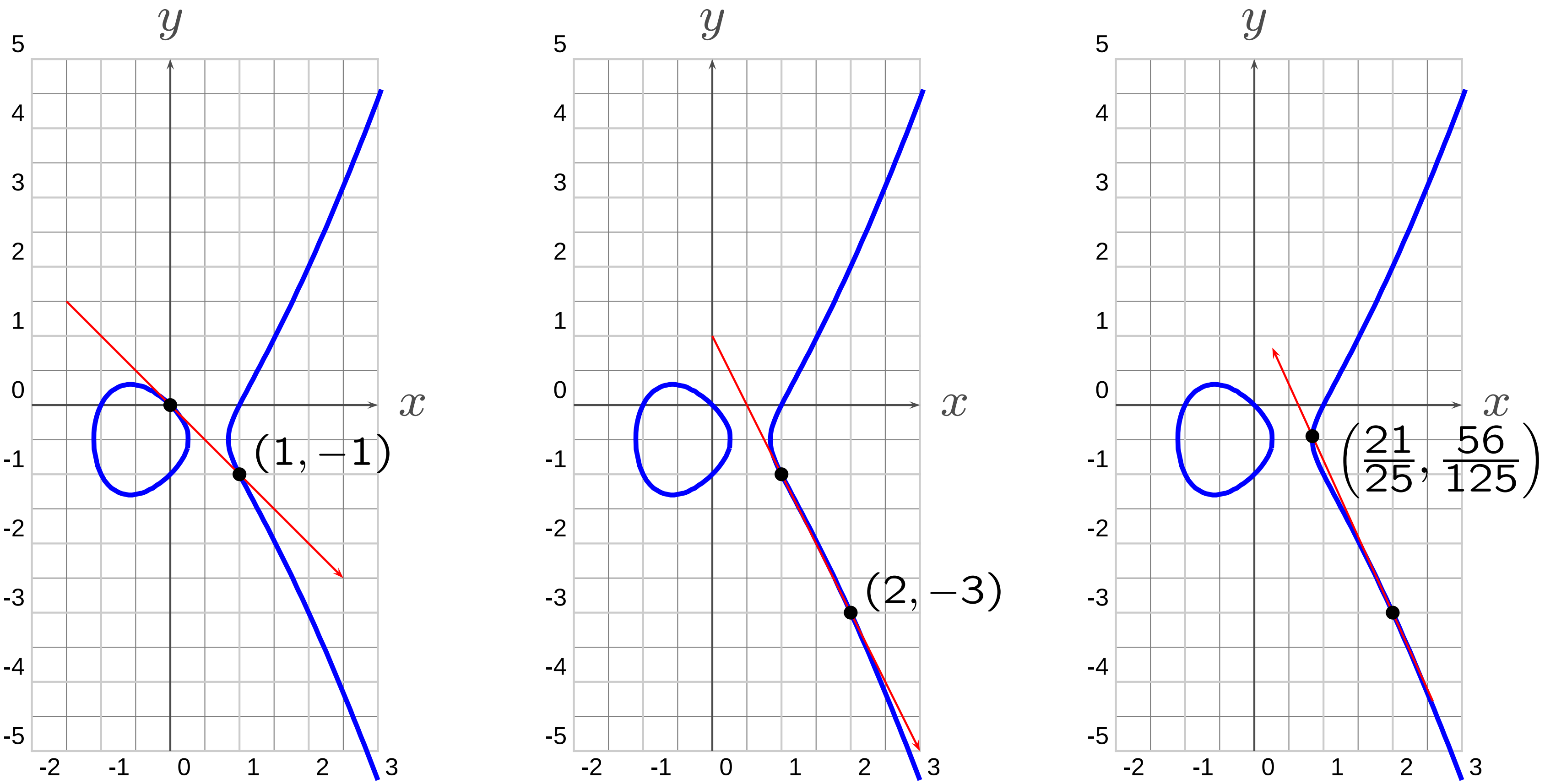
Obtain a third rational point from two rational points.



The Tangent Process



New rational point from a single rational point.



Iterate the Tangent Process

Fermat

$$(0,0)$$

$$(1,-1)$$

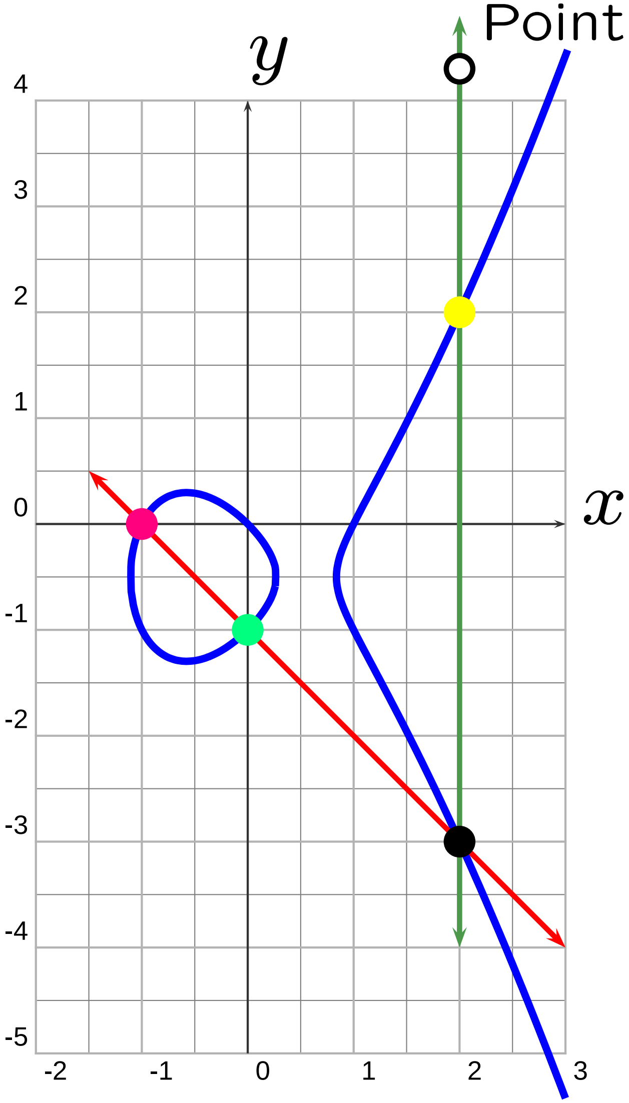
$$(2,-3)$$

$$\left(\frac{21}{25},-\frac{56}{125}\right)$$

$$\left(\frac{480106}{4225},\frac{332513754}{274625}\right)$$

$$\left(\frac{53139223644814624290821}{1870098771536627436025},-\frac{12282540069555885821741113162699381}{80871745605559864852893980186125}\right)$$

The Group Operation



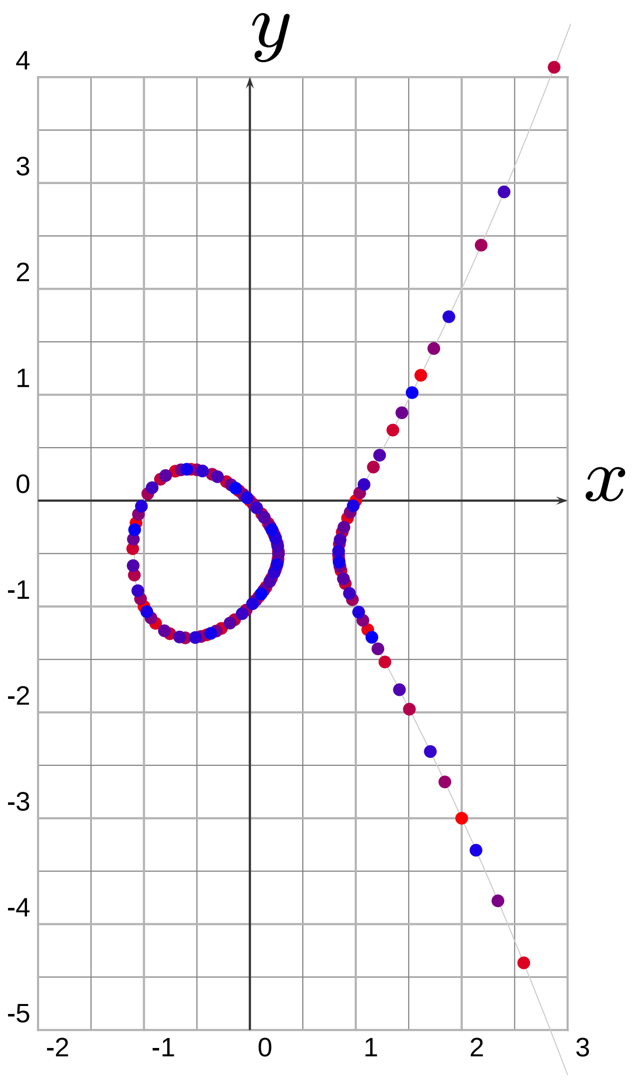
$y^2 + y = x^3 - x$

● ⊕ ● = ●

$(-1, 0) \oplus (0, -1) = (2, 2)$

The set of rational points on E forms an abelian group.

The First 150 Multiples of $(0,0)$



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

(The bluer the point, the bigger the multiple.)

Fact: The group $E(\mathbb{Q})$ is infinite cylic, generated by $(0,0)$.

In contrast, $y^2 + y = x^3 - x^2$ has only 5 rational points!

What is going on here?

Mordell's Theorem

Theorem (Mordell). The group $E(\mathbb{Q})$ of rational points on an elliptic curve is a **finitely generated abelian group**, so

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T,$$

with $T = E(\mathbb{Q})_{\text{tor}}$ finite.

Mazur classified the possibilities for T. It is conjectured that r can be arbitrary, but the biggest r ever found is (probably) 24.

The Simplest Solution Can Be Huge

Simplest solution to $y^2 = x^3 + 7823$:

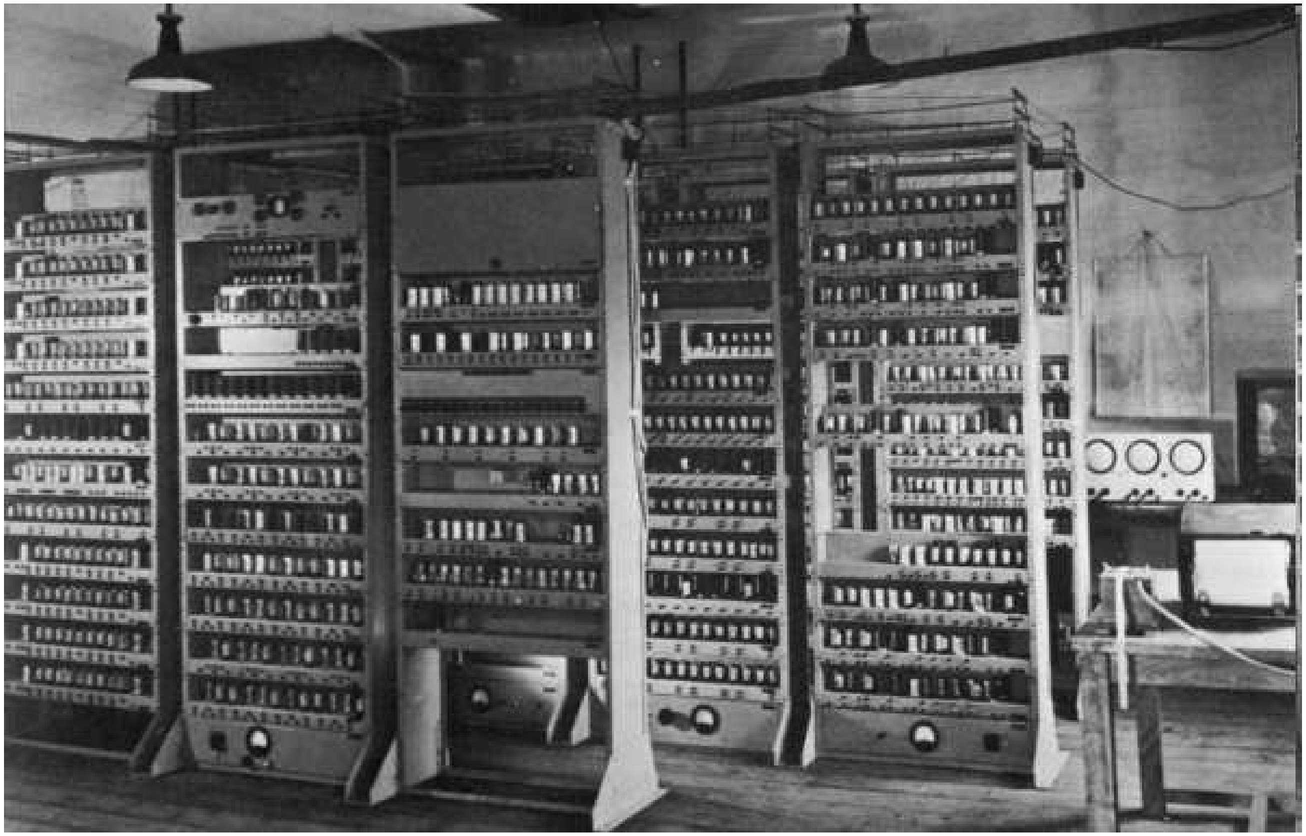
$$x = \frac{2263582143321421502100209233517777}{143560497706190989485475151904721}$$

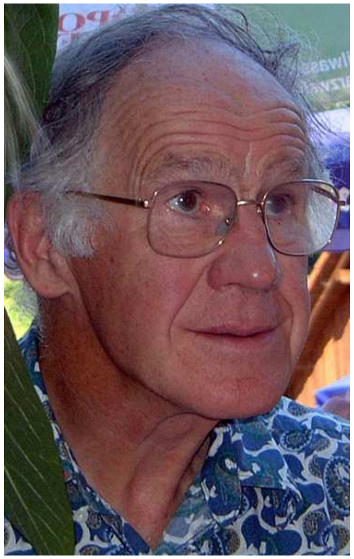
$$y = \frac{186398152584623305624837551485596770028144776655756}{1720094998106353355821008525938727950159777043481}$$

(Found by Michael Stoll in 2002.)

The Central Question

Given an elliptic curve,
what is its rank?





Conjectures Proliferated

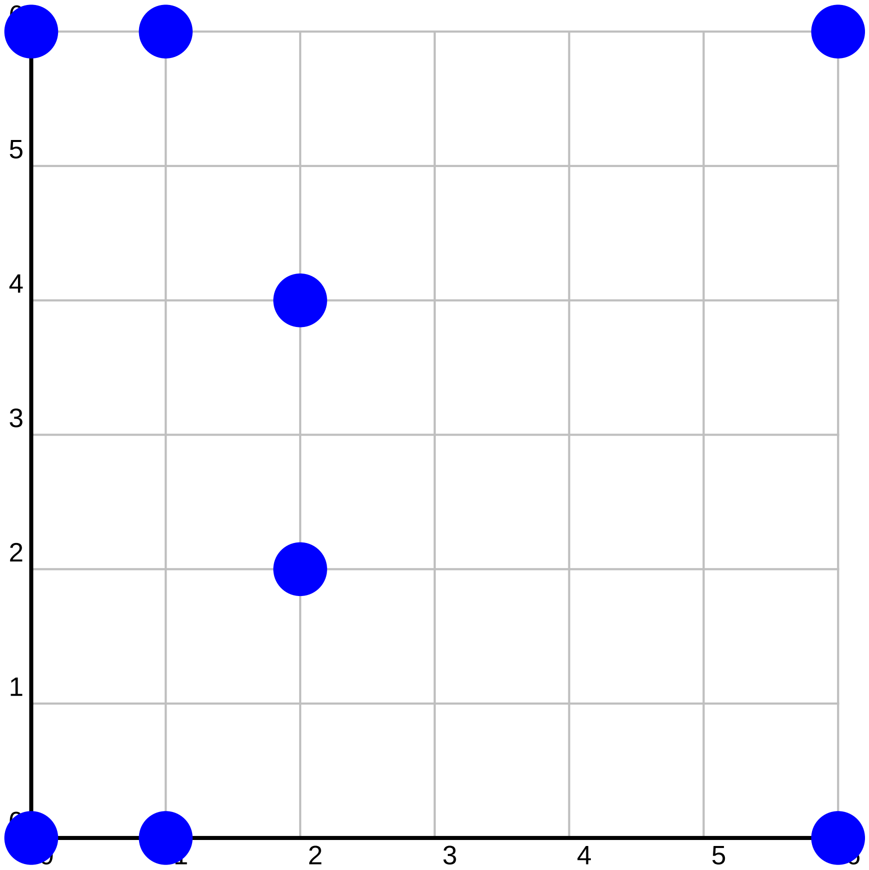
"The subject of this lecture is rather a special one. I want to describe some computations undertaken by myself and Swinnerton-Dyer on EDSAC, by which we have calculated the zeta-functions of certain elliptic curves. As a result of these computations we have found an analogue for an elliptic curve of the Tamagawa number of an algebraic group; and conjectures have proliferated. [...] though the associated theory is both abstract and technically complicated, the objects about which I intend to talk are usually simply defined and often machine computable; **experimentally we have detected certain relations between different invariants**, but we have been unable to approach proofs of these relations, which must lie very deep." – Birch 1965

Counting Solutions Modulo p

$$N(p) = \#\text{ of solutions } \pmod{p}$$

$$y^2 + y = x^3 - x \pmod{7}$$

●∞



$$N(7) = 9$$

t counting gnomes

The Error Term

Let

$$a_p = p + 1 - N(p).$$

Hasse proved that

$$|a_p| \leq 2\sqrt{p}.$$

$a_2 = -2, \quad a_3 = -3, \quad a_5 = -2, \quad a_7 = -1, \quad a_{11} = -5, \quad a_{13} = -2, \quad a_{17} =$

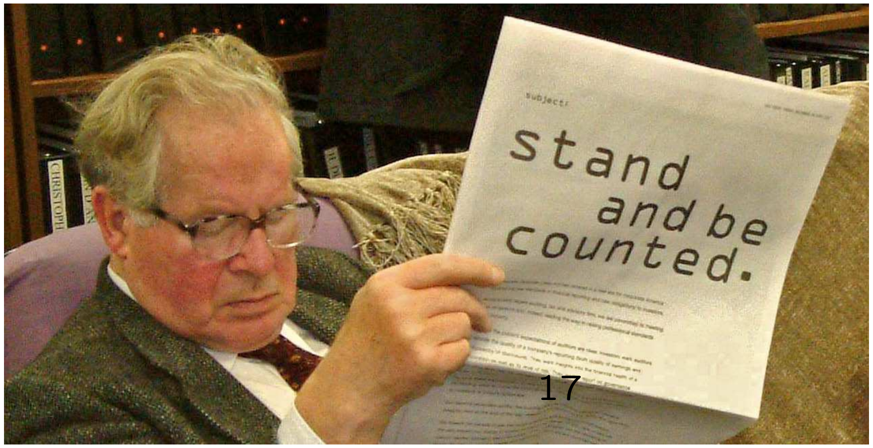
$a_{19} = 0, \quad a_{23} = 2, \quad a_{29} = 6, \quad \ldots$

Guess

If an elliptic curve E has positive rank, then perhaps $N(p)$ is on average larger than p, for many primes p. Thus maybe

$$f_E(x) = \prod_{p \le x} \frac{p}{N(p)} \to 0 \text{ as } x \to \infty$$

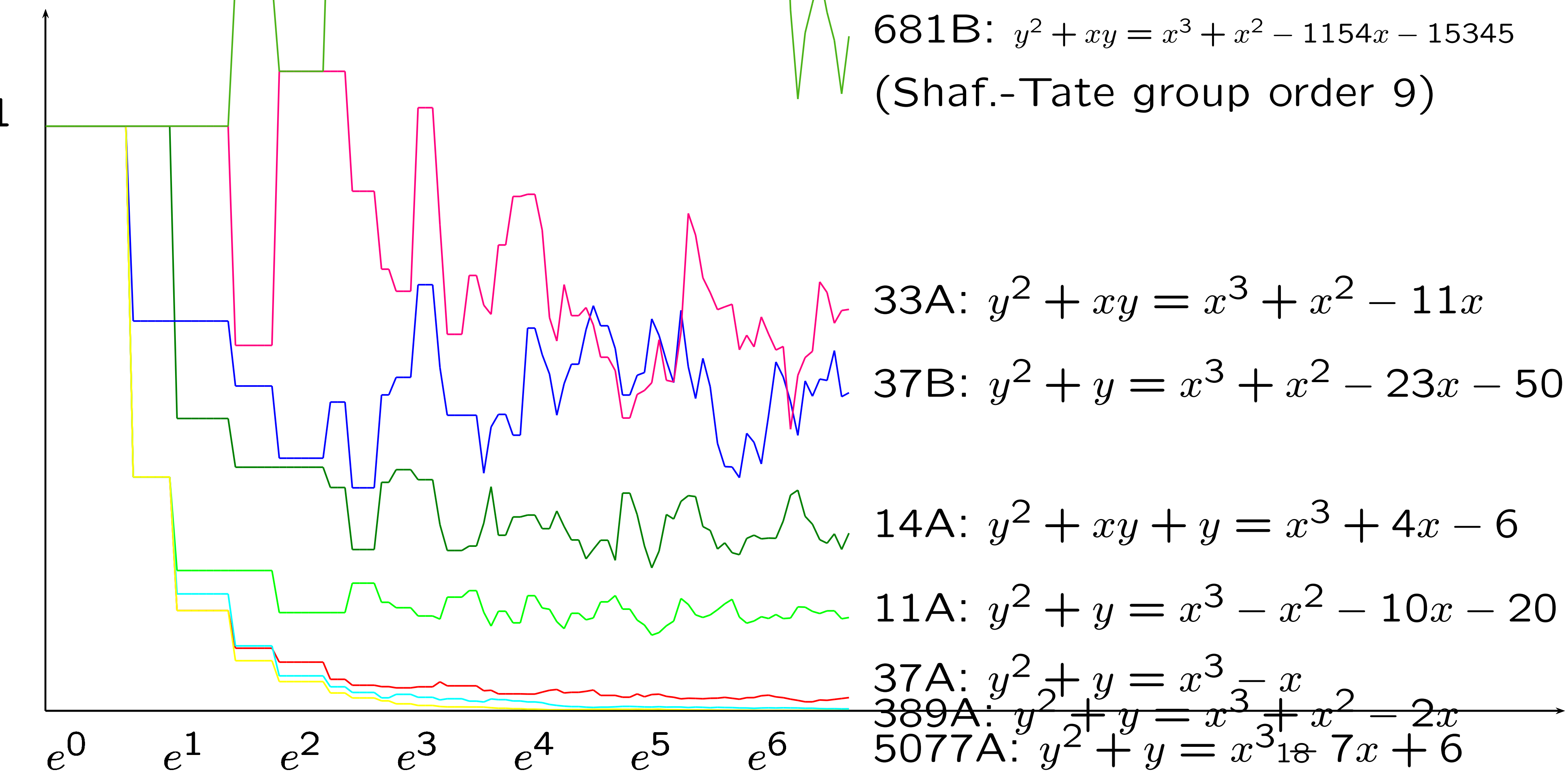
exactly when E has positive rank??



Swinnerton-Dyer

Graphs of $f(x) = \Pi_{p \leq x} \frac{p}{N(p)}$

The following are graphs, on a log scale, of $f_E(x)$:



Something Better: The L-Function

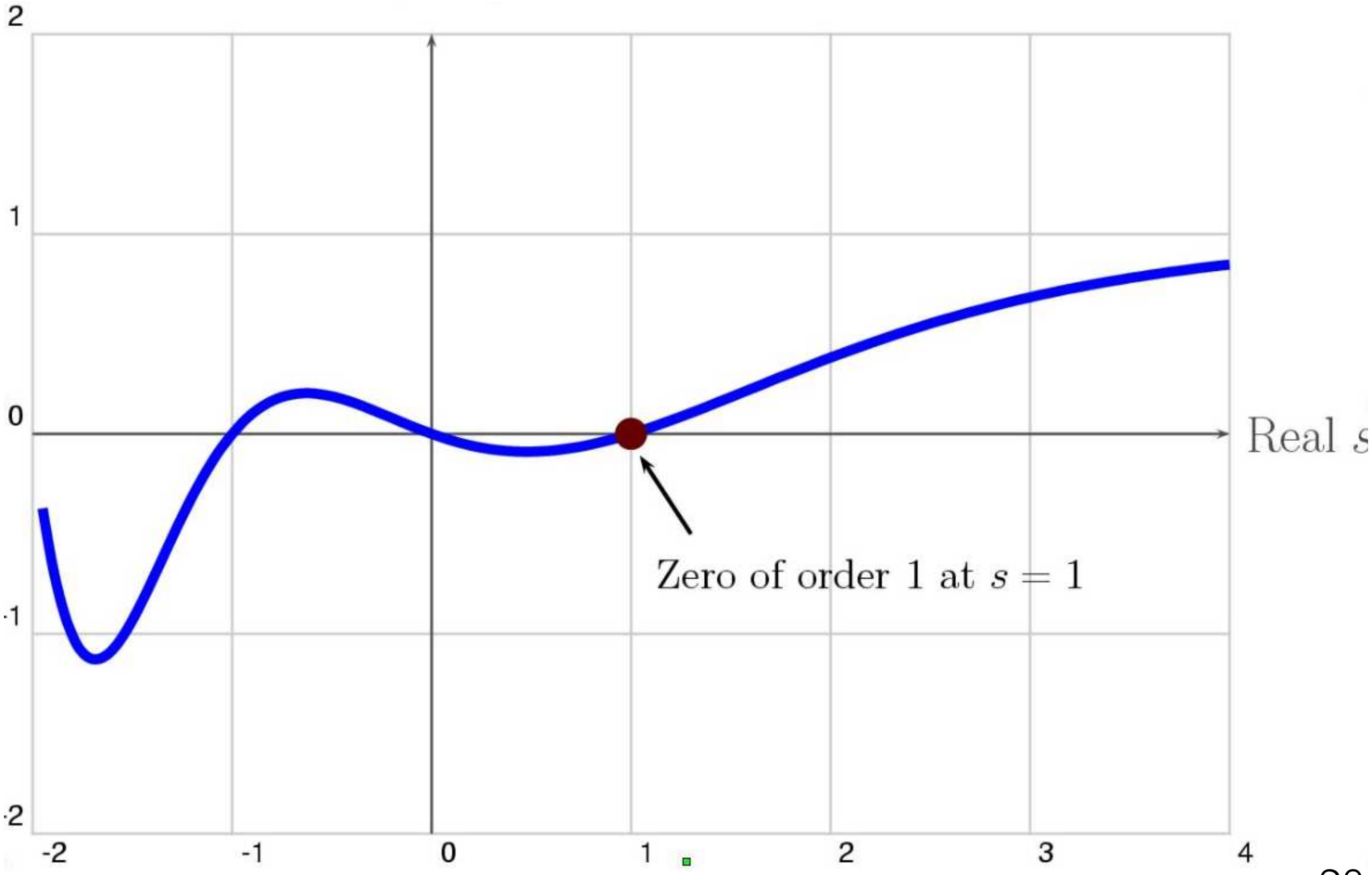
Theorem (Wiles et al., Hecke) The following function extends to a holomorphic function on the whole complex plane:

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

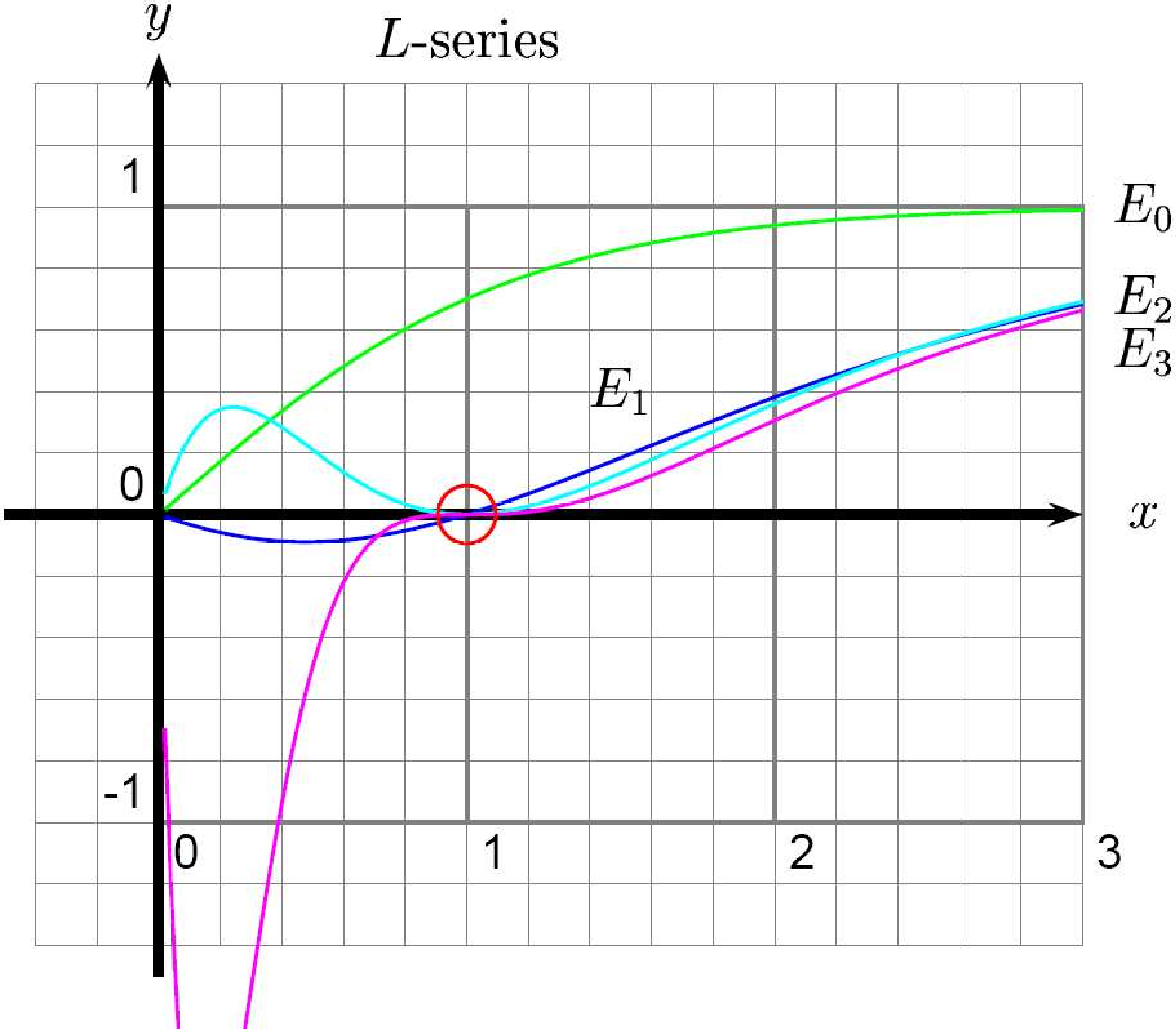
Note that formally,

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

Real Graph of the L-Series of $y^2 + y = x^3 - x$



More Graphs of Elliptic Curve L-functions



The Birch and Swinnerton-Dyer Conjecture

Conjecture: Let E be any elliptic curve over $\mathbb{Q}$. The order of vanishing of $L(E,s)$ as $s=1$ equals the rank of $E(\mathbb{Q})$.

The Kolyvagin and Gross-Zagier Theorem

Theorem: If the ordering of vanishing $\mathrm{ord}_{s=1} L(E, s)$ is ≤ 1, then the conjecture is true for E.

What Proportion of Elliptic Curves are Covered by the Theorem?

The rest of this talk is about the **state of the art in building databases** of elliptic curves, and **new data about average ranks of these curves**. We arrange elliptic curves by either their conductor, minimal discriminant, or naive height. Each is an integer invariant of an elliptic curve, and there are only finitely many elliptic curves with that invariant.

- **Discriminant** of $y^2 = x^3 + ax + b$ is $-16(4a^3 + 27b^2)$.

- **Conductor:** Integer divisible by same primes as (minimal) discriminant (measures the nature of reduction modulo p).

- **Naive Height:** Measure of size of coefficients of equation.

What is the Average Rank of All Elliptic Curves?

In 1990, Brumer and MicGuinness published a paper in the Bulletins of the AMS about ranks of elliptic curves of prime conductor. Brumer-McGuinness begins:

> “The opinion had been expressed that, in general, an elliptic curve might tend to have the smallest possible rank, namely 0 or 1, compatible with the rank parity predictions of Birch and Swinnerton-Dyer. We present evidence that this may not be the case. [...] This proportion of rank 2 curves seemed too large to conform to **the conventional wisdom**.”

Our New Data

Brumer and McGuinness considered 310,716 curves of prime conductor $\leq 10^8$.

Mark Watkins, Baur Bektemirov and I consider 136,832,795 curves of conductor $\leq 10^8$, and 11,378,911 curves of prime conductor $\leq 10^{10}$. The results of our rank computations are similar to those of Brumer and McGuinness, which suggests that if one orders all elliptic curves over $\mathbb{Q}$ by their conductor, then **a surprising number of curves have rank bigger than one**.

Brumer and McGuinness

Brumer and McGuinness found, by thousands of hours of computer search on numerous Mac II's, 311,219 curves of prime conductor $\leq 10^8$. For 310,716 of these curves they computed the probable rank by a combination of point searches and computation of apparent order of vanishing of L-functions. This table summarizes the rank distribution that they found:

Rank	0	1	2	3	4	5
$\Delta > 0$	31748	51871	24706	5267	377	0
$\Delta < 0$	61589	91321	36811	6594	427	5
Totals	93337	143192	61517	11861	804	5
Percents	30.04	46.08	**19.80**	3.82	0.26	

Let $r_\varepsilon(X)$ be the *average rank* of elliptic curves in the Brumer-McGuinness tables with conductor at most X and discriminant sign ε. They observe that in their data, r_+ **climbs to** 1.04 **and** r_- **climbs to** 0.94**.**

Quadratic Twists

Let E be an elliptic curve over $\mathbb{Q}$. Consider quadratic twists $Dy^2 = x^3+ax+b$ of $E : y^2 = x^3+ax+b$ by square-free integers D.

Conjecture 1 (Goldfeld). *The average rank of the curves E^D is $\frac{1}{2}$, in the sense that*

$$\lim_{X\to\infty} \frac{\sum_{|D|<X} \mathrm{rank}(E^D)}{\#\{D : |D| < X\}} = \frac{\mathbf{1}}{\mathbf{2}}.$$

(Here the D are squarefree.)

There are many conditional and unconditional results in the direction of Goldfeld's conjecture (e.g., work of Katz, Sarnak, et al.). For a survey of these results, see Silverberg's PCMI article.

Cubic Twists of $x^3 + y^3 = 1$

Kramarz and Zagier considered elliptic curves $x^3 + y^3 = D$ and found that in their data that **23.3%** of the curves with even rank have rank at least 2, and 2.2% of those with odd rank have rank at least 3. Mark Watkins followed up on these computations, and found that the rank eventually starts *decreasing*:

23.3% up to 70000, **20.5%** up to 10^6, **17.7%** up to 10^7.

Since only $j = 0, 1728$ have non-quadratic twists, taken together the above data and conjectures suggests that the average rank of elliptic curves "ordered by j-invariants" should be $1/2$, since it should be an average of infinitely many numbers all but two of which are equal to $1/2$. We will not concern ourselves further with questions about twists in this

The Stein-Watkins Database

Brumer and McGuinness fixed the a_1, a_2, a_3 invariants (12 total possibilities) and then searched for a_4 and a_6 which made $|\Delta|$ small.

Instead, Watkins and I break the c_4 and c_6 invariants into congruence classes, and then find small solutions to $c_4^3 - c_6^2 = 1728\Delta$.

Generating Our Table

1. For each of the 288 possible pairs ($c_4 \mod 576$, $c_6 \mod 1728$), we loop over c_4 and c_6, "hoping" to find all curves with $|\Delta| \leq 10^{12}$. We do not know a bound on c_4 to guarantee this. We took $c_4 \leq 1.44 \cdot 10^{12}$ in this step. We throw away all curves whose conductor is composite and $\geq 10^8$, or prime and $\geq 10^{10}$.

2. Include all curves that are isogenous to a curve found above.

3. Include all twists with conductor $\leq 10^8$.

The Number of Curves That We Found

The following table lists the number of curves in our database with various properties:

Type	Number
Curves with conductor $\leq 10^8$	**136,832,795**
Optimal curves with conductor $\leq 10^8$	115,821,258
Curves with square-free conductor $\leq 10^8$	21,826,791
Optimal curves with square-free conductor $\leq 10^8$	19,963,592
Curves with prime conductor $\leq 10^{10}$	11,378,911
Curves with prime conductor $\leq 10^8$	312,435

Cremona's Tables

Cremona has enumerated *every* elliptic curve of conductor up to $25,000$. He found $103,174$ isogeny classes of elliptic curves of conductor up to $25,000$. In our computation, we find $88,700$ isogeny classes of curves of conductor up to $25,000$, so we miss $14,474$ isogeny classes. The first conductor where Cremona has a curve and we don't is conductor 174. The curve 174A1 with a-invariants $[1,0,1,-7705,1226492]$ has discriminant -621261297432576, which is substantially larger in absolute value than 10^{12}.

Thus we expect that our table is far from complete for composite conductor.

Cremona's Rank Distribution

Amongst Cremona's 103,174 isogeny classes, the rank distribution is as follows:

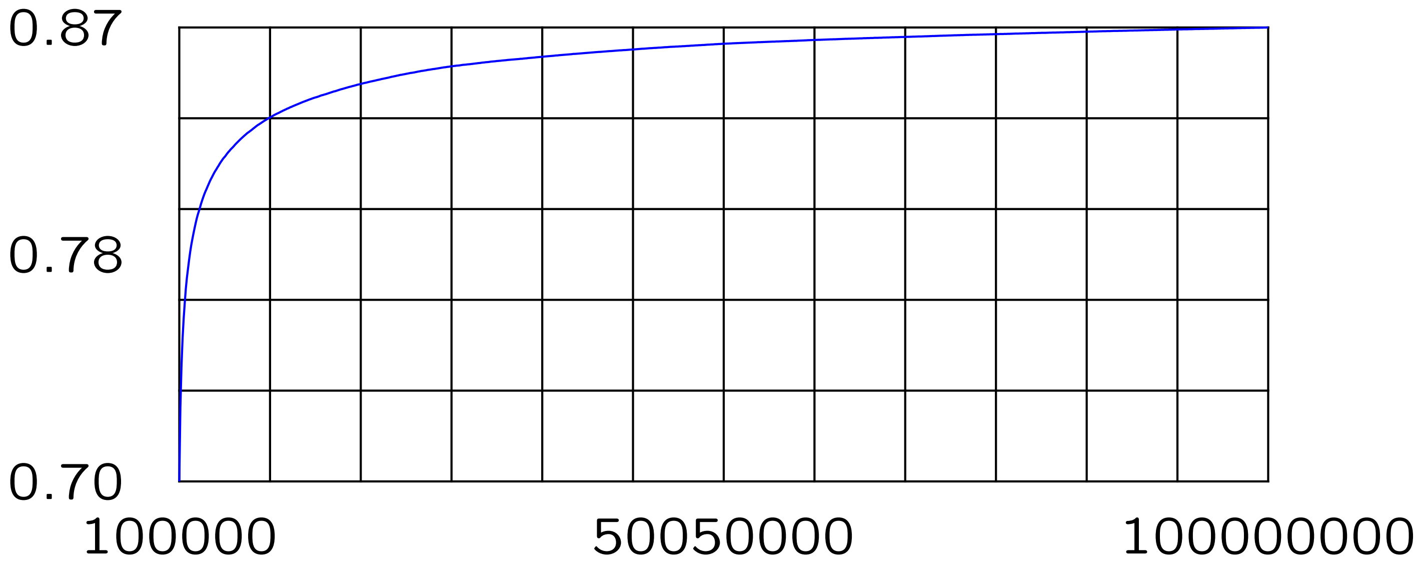
Rank	0	1	2	≥ 3
Number	42165	53483	7509	17
Proportion	41%	52%	**7%**	0%

Graphs of Ranks

For the rest of this talk, we give data about the ranks of elliptic curves in our data. Thus everywhere hence, when we say "elliptic curves with property P", we **always** mean "elliptic curves in the Stein-Watkins database with property P".

All Curves Ordered By Conductor

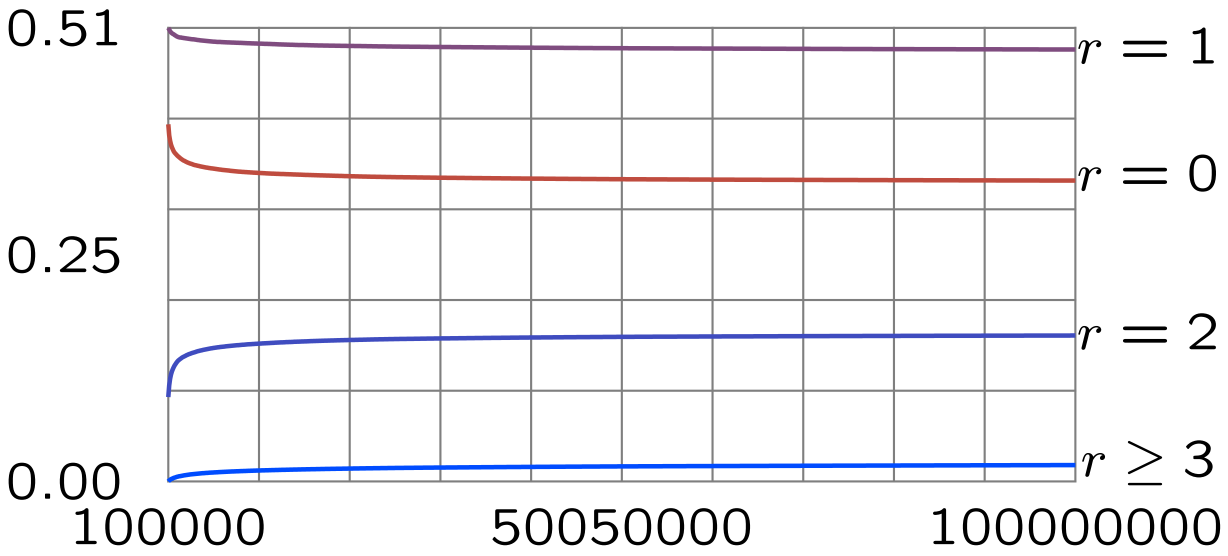
The average rank of all curves of conductor $\leq 10^8$ is $0.8664\ldots$.
A graph of the average rank as a function:



We created this graph by computing the average rank of curves of conductor up to $n \cdot 10^5$ for $1 \leq n \leq 1000$.

Rank Distribution

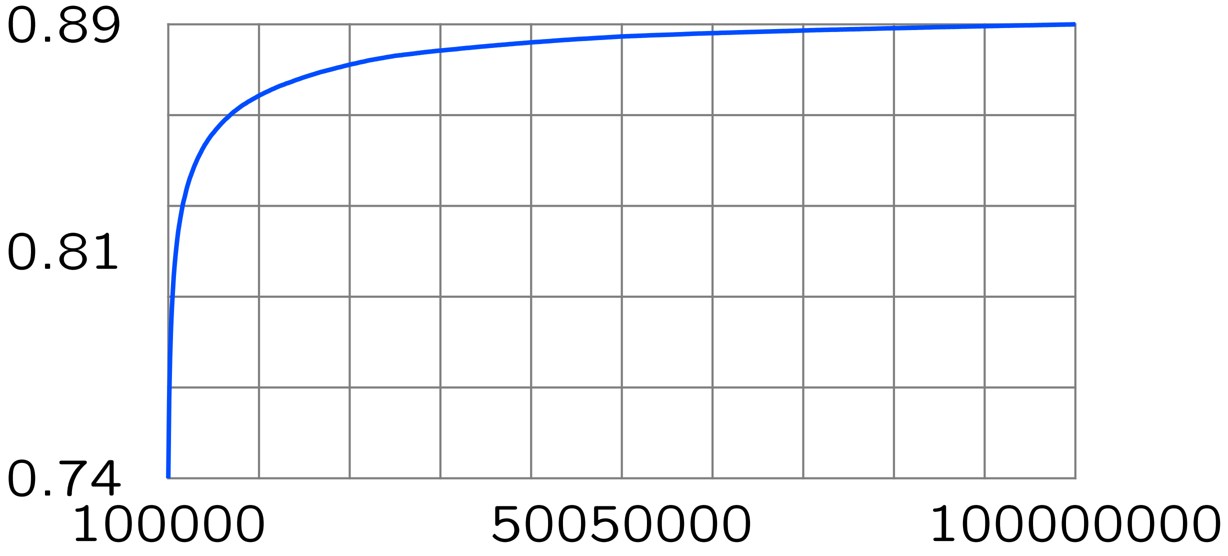
The following graph gives the proportion of curves of rank each rank 0, 1, 2, and ≥ 3, as a function of the conductor, all on a single graph.



Rank	0	1	2	≥ 3
Proportion	33.6%	48.2%	16.3%	1.9%

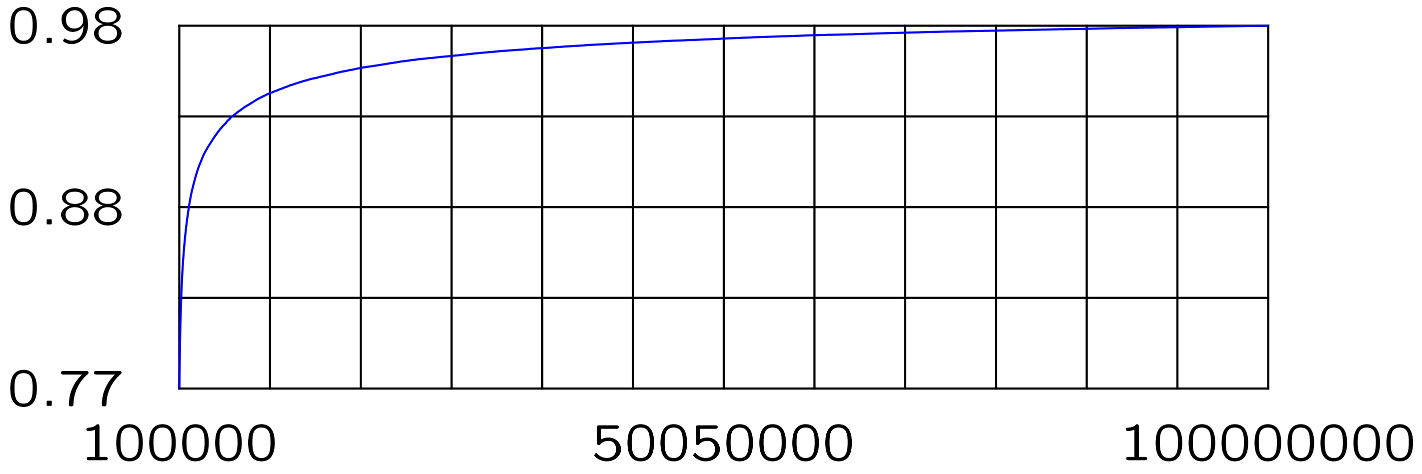
Optimal Curves Ordered By Conductor

The average rank of optimal curves of conductor $\leq 10^8$ is $0.8855\ldots$, and the following is a graph of the average rank as a function of the conductor:



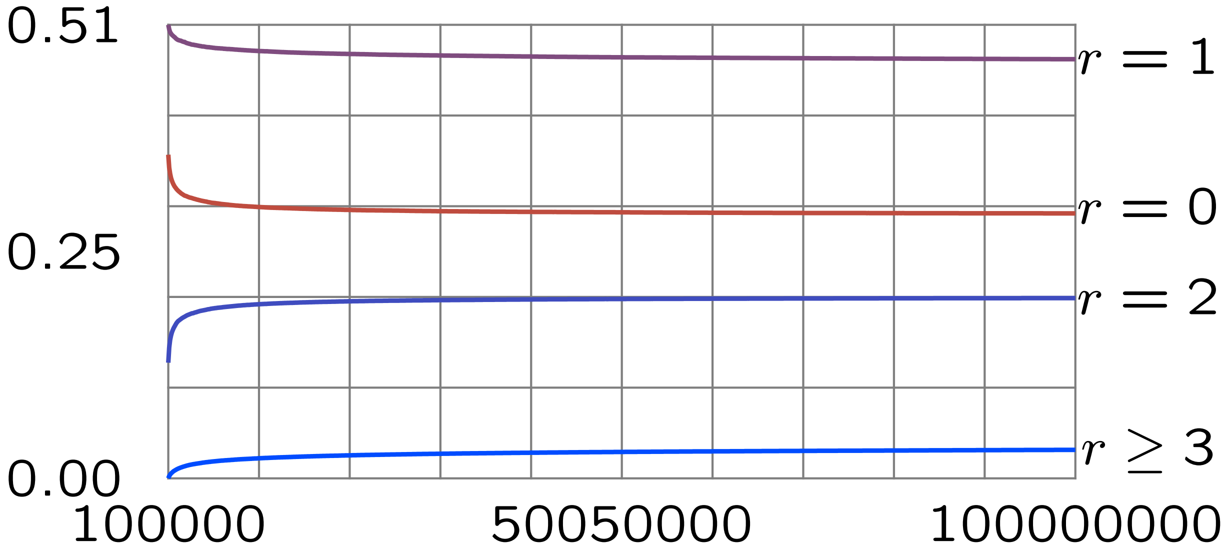
Curves of Squarefree Conductor

The average rank of all curves of squarefree conductor $\leq 10^8$ is $0.9756\ldots$. The following is a graph of the average rank of squarefree curves as a function of the conductor:



The data suggests that the average rank of all elliptic curves of squarefree conductor tends to 1.

Squarefree Conductor Rank Distribution

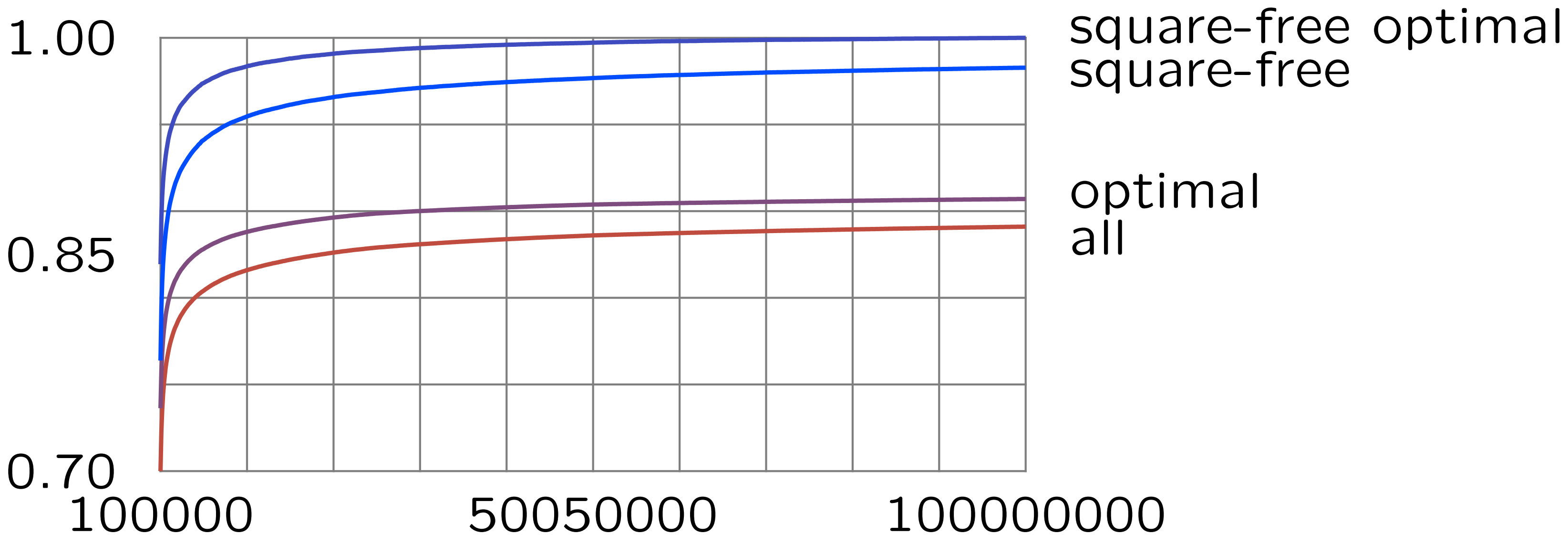


The overall proportion of each rank is as follows:

Rank	0	1	2	≥ 3
Proportion	29.6%	46.7%	20.2%	3.4%

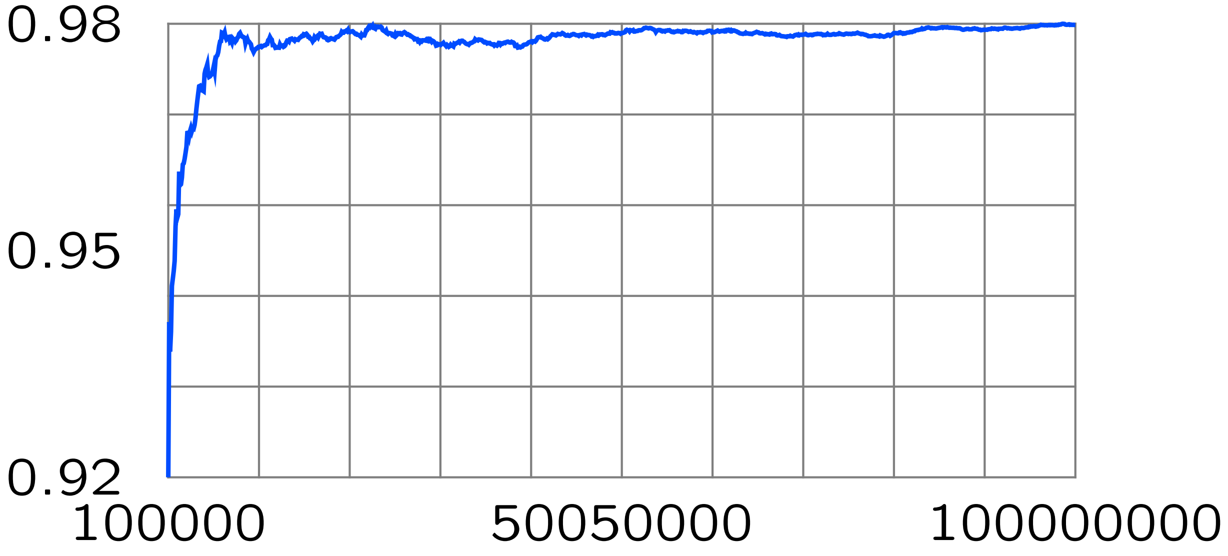
Comparison of Average Rank Graphs

The graph below shows the average rank graphs for four different sets of elliptic curves up to conductor 10^8 considered above.



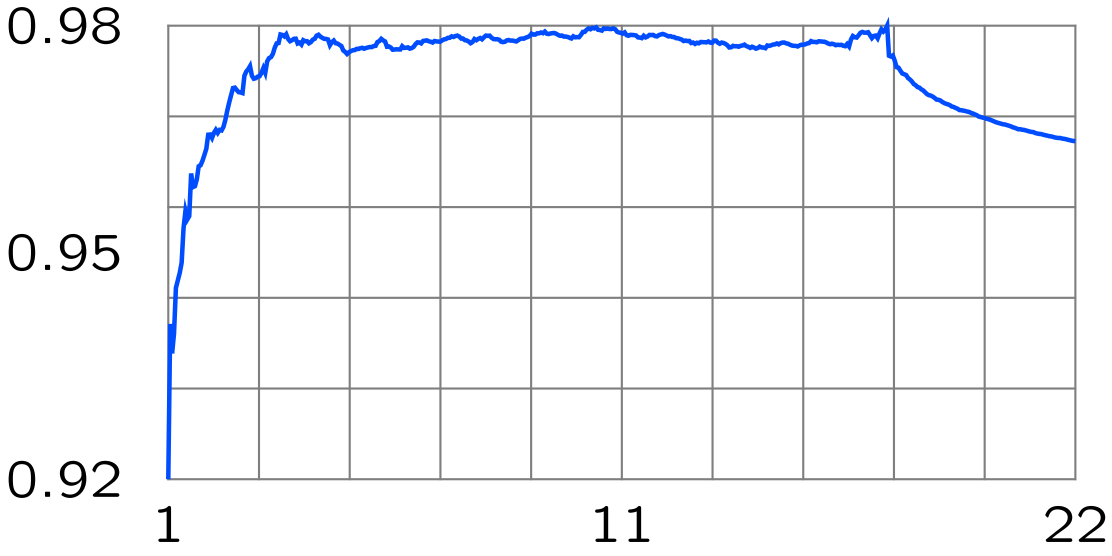
Curves of Prime Conductor Up to 10^8

The average rank of curves of prime conductor $\leq 10^8$ is near 1. We created the following graph by computing the average rank up to conductor $n \cdot 10^5$ for $1 \leq n \leq 1000$.



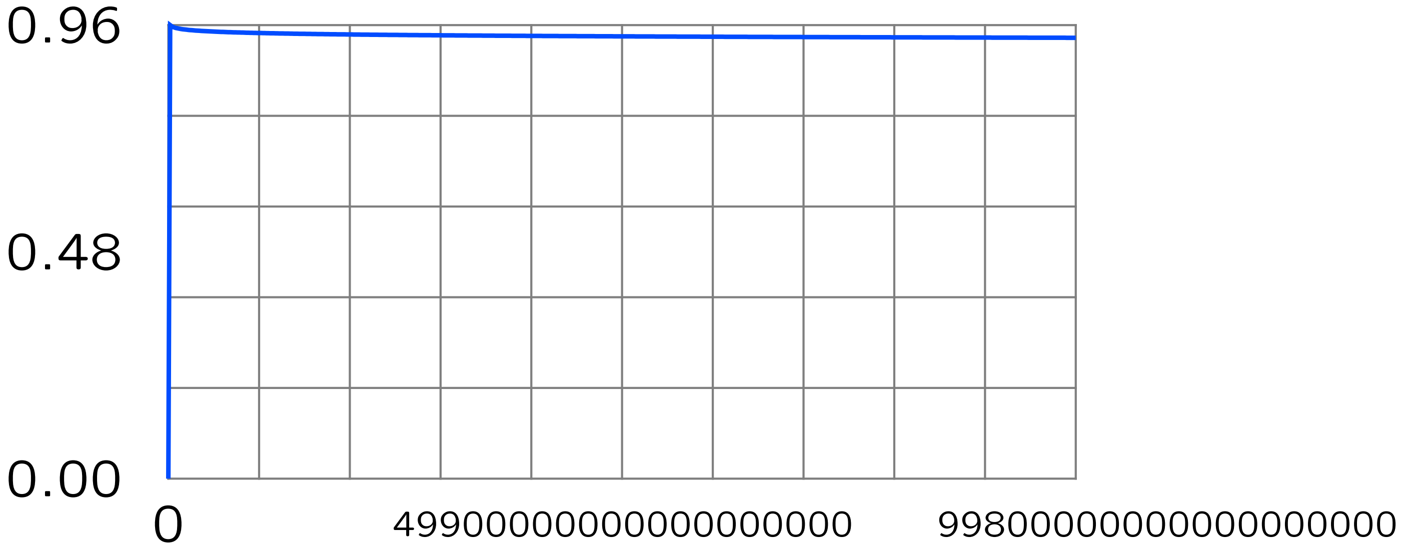
Curves of Prime Conductor Up to 10^{10}

The average rank of curves of prime conductor $\leq 10^{10}$ is $0.964\ldots$. The following graph shows the average rank graphed on a **logarithmic scale** (the horizontal axis contains $\log(N)$):



All Curves Ordered By Naive Height

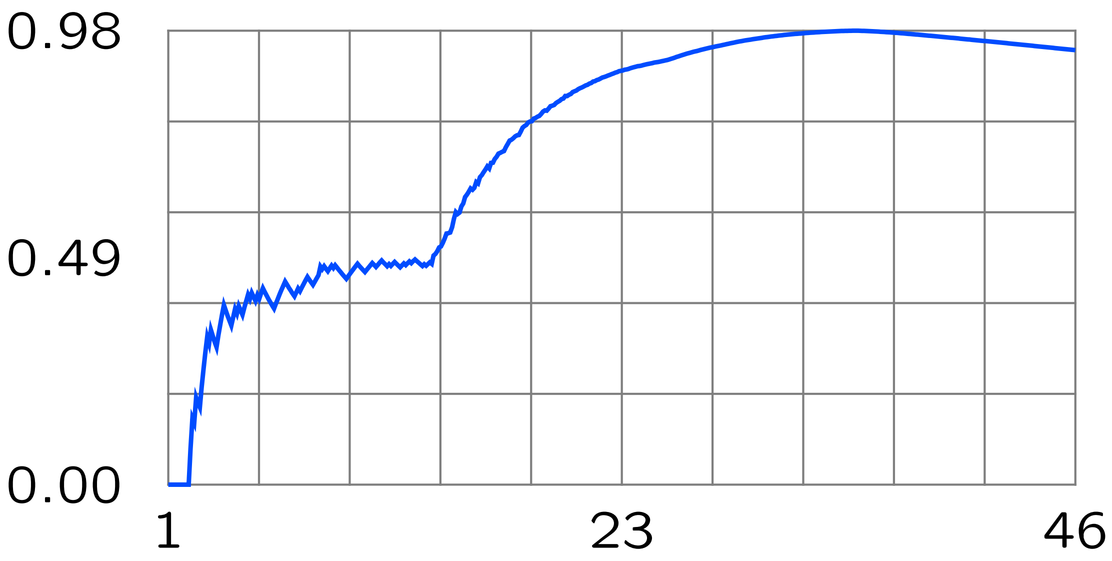
The naive height of E is $\max\{|c_4|^3, |c_6|^2\}$. The following graph gives the average rank of all curves up to a given naive height.



Try again with log scale...

All Curves Ordered By Naive Height

The horizontal axis is plotted on a **logarithmic scale**, and is labeled with the logarithm of the naive height.

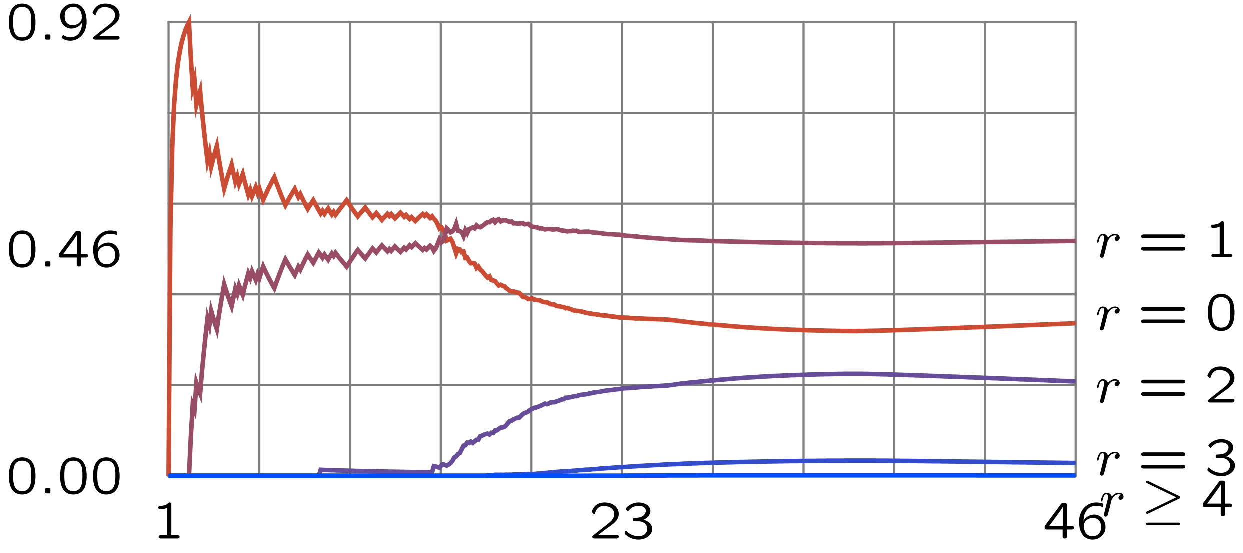


Interesting points at 2.5 million and and $1.7 \cdot 10^{14}$.

Theorem (Brumer). *(BSD, RH, etc.) imply the limit is* ≤ 2.3.

Proportions of Each Rank Ordered By Naive Height

The horizontal axis is plotted on a **logarithmic scale**, and is labeled with the logarithm of the naive height.



Interesting points at 2.5 million and and $1.7 \cdot 10^{14}$.

Open Questions

1. What is the average rank ordered by conductor?

2. What is the average rank ordered by discriminant?

3. What is the average rank ordered by height?

4. What is the proportion of curves of rank 2, rank 3, rank 4, etc.? Are each 0 or is every proportion positive?

5. Why are the so many curves of rank ≥ 2 in our data?

6. Is the rank unbounded? (Standard Conjecture: Yes.)

Despite our data, Mark Watkins and other people have heuristics that predict that the average rank in each case is 0.5 and the proportion of all curves of rank ≥ 2 is 0.

Acknowledgment.

Armand Brumer, Frank Calegari, Keith Conrad, Noam Elkies, Benedict Gross, Barry Mazur, Ariel Shwayder.