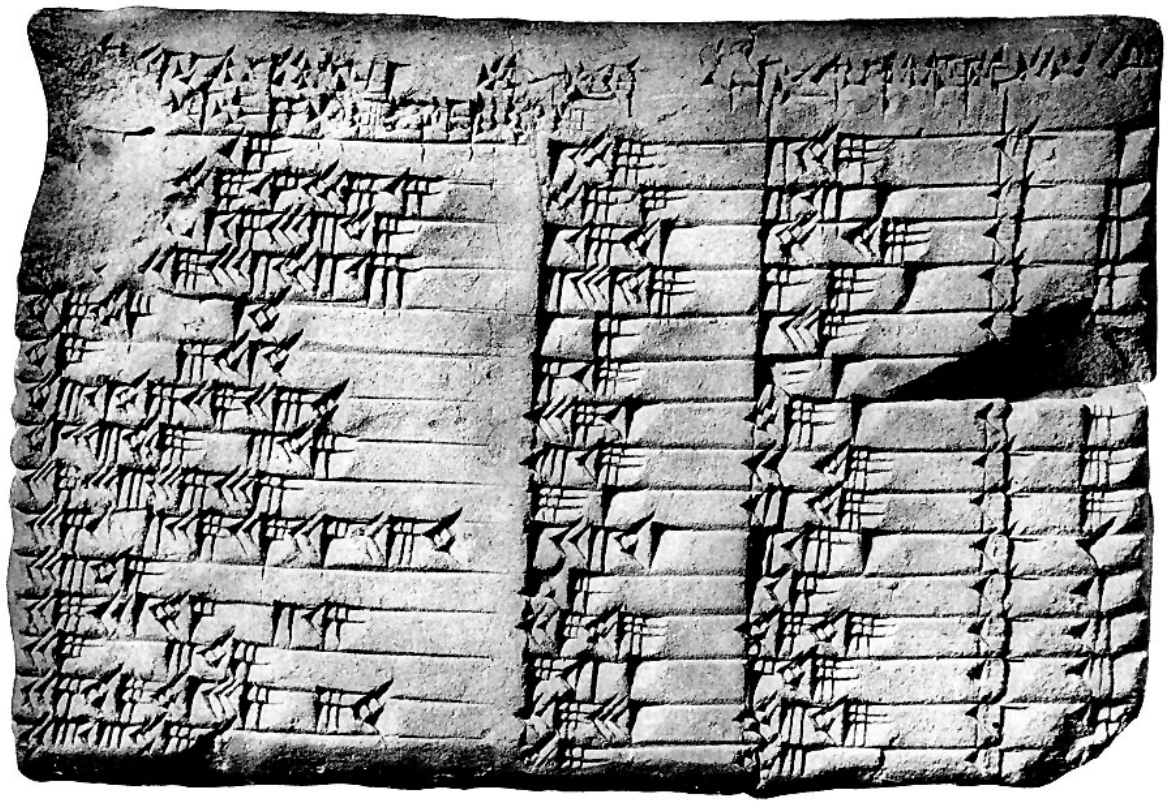
The rank of elliptic curves

Benedict Gross

April, 2015

Integral solutions of the quadratic equation $x^2 + y^2 = z^2$ were found by Babylonian mathematicians in the time of Hammurabi (1750 BCE).



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

After linear and quadratic equations come cubic equations, or elliptic curves.

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

After linear and quadratic equations come cubic equations, or elliptic curves.

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

There may either be a finite or an infinite number of rational solutions.

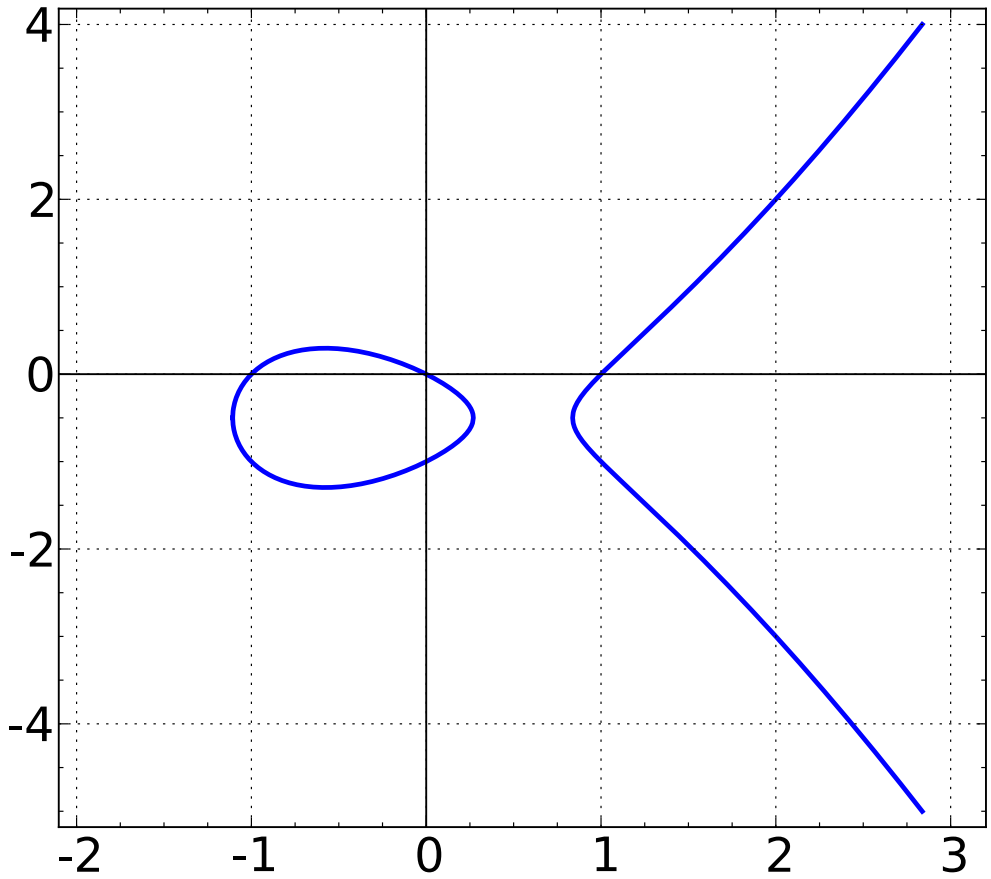
After linear and quadratic equations come cubic equations, or elliptic curves.

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

There may either be a finite or an infinite number of rational solutions.

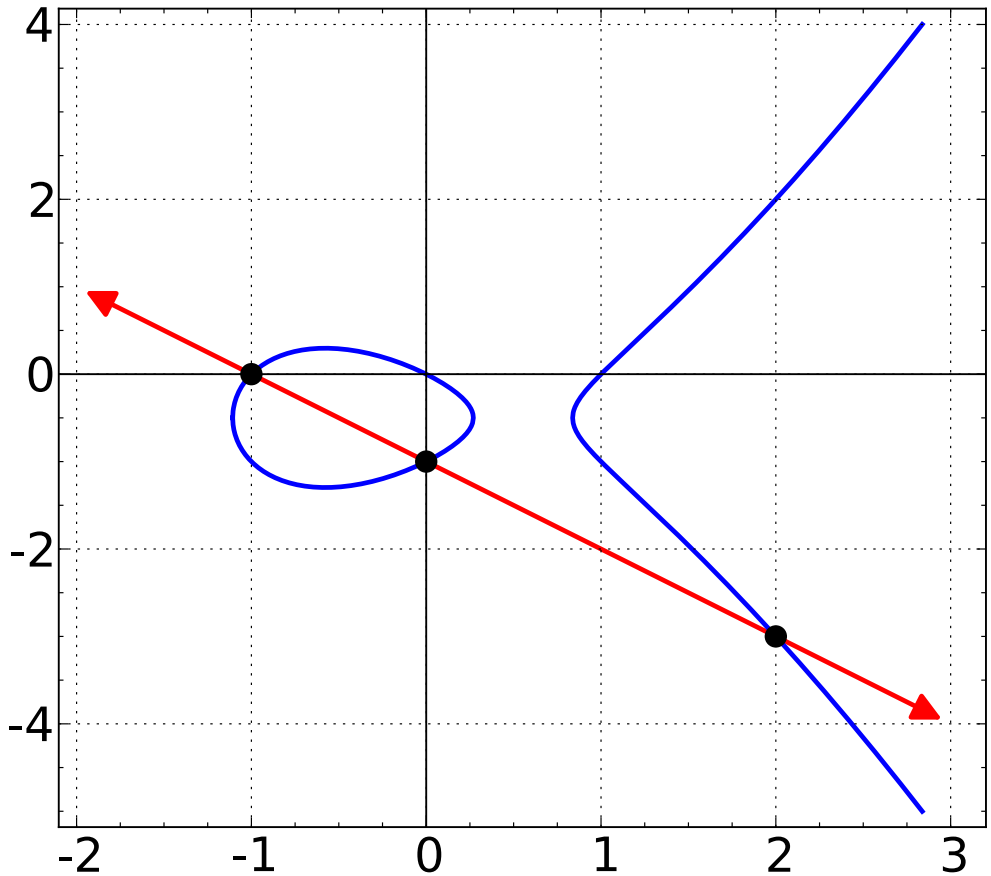
The graph

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



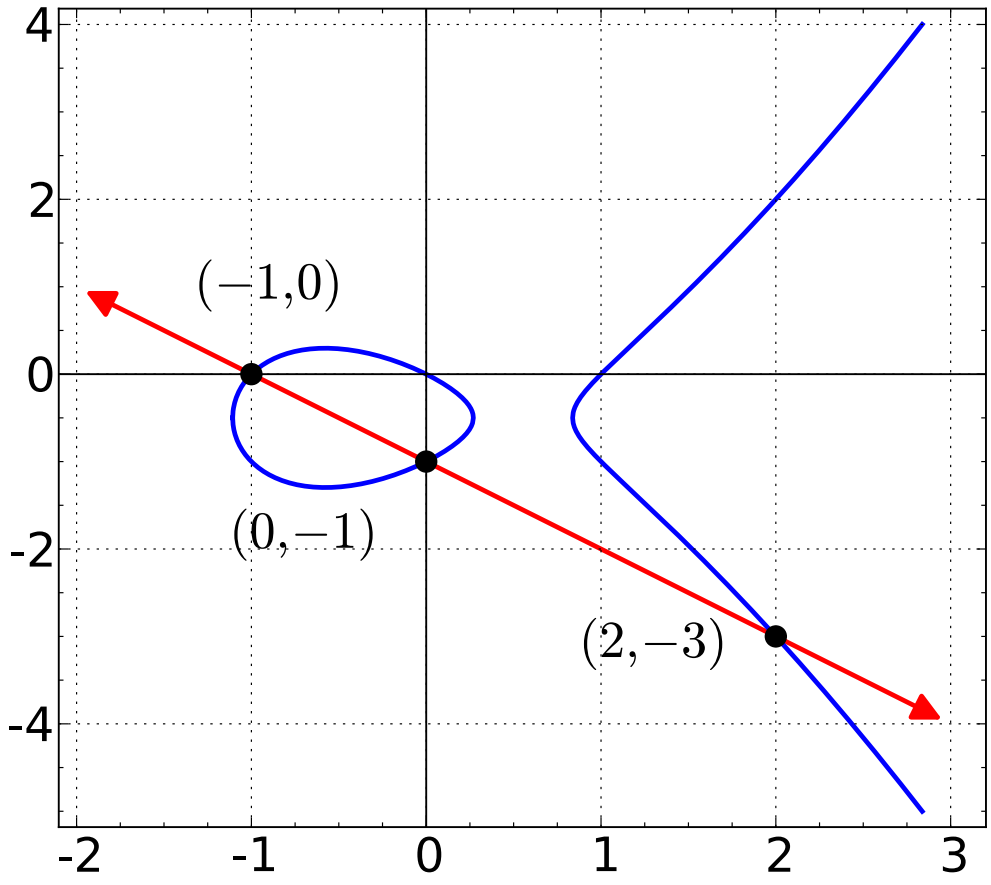
The graph

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



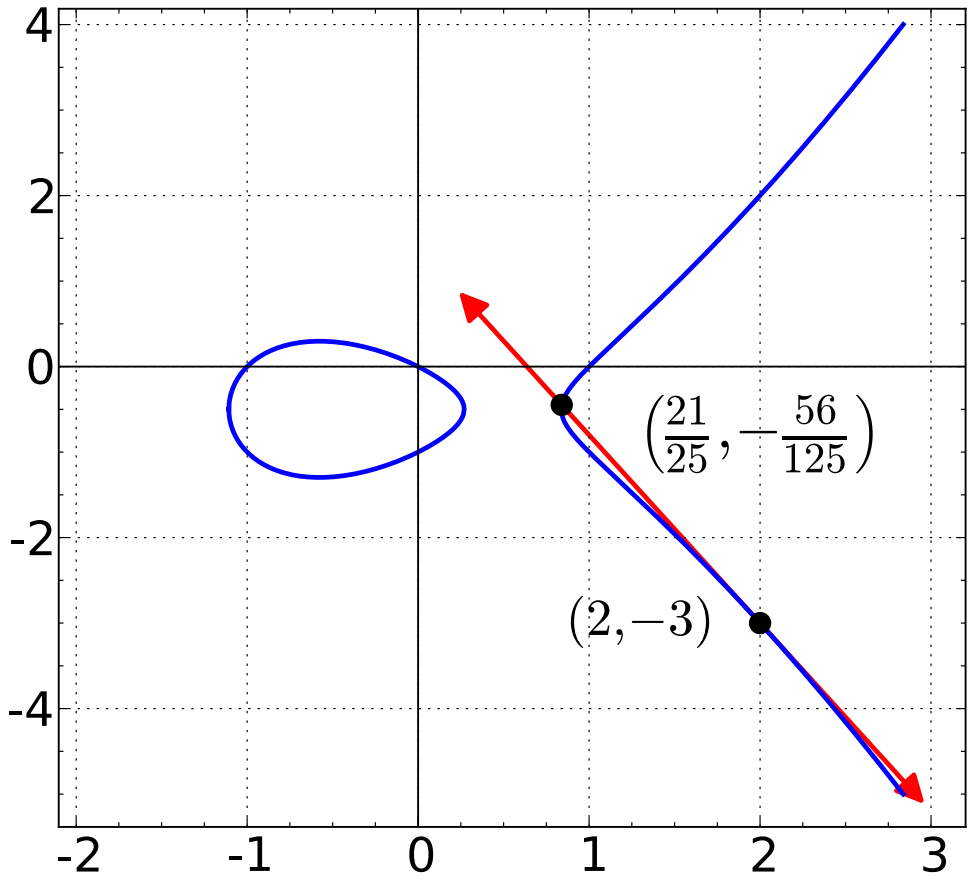
The graph

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



The limit of a secant line is a tangent

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



Large solutions

If the number of solutions is infinite, they quickly become large.

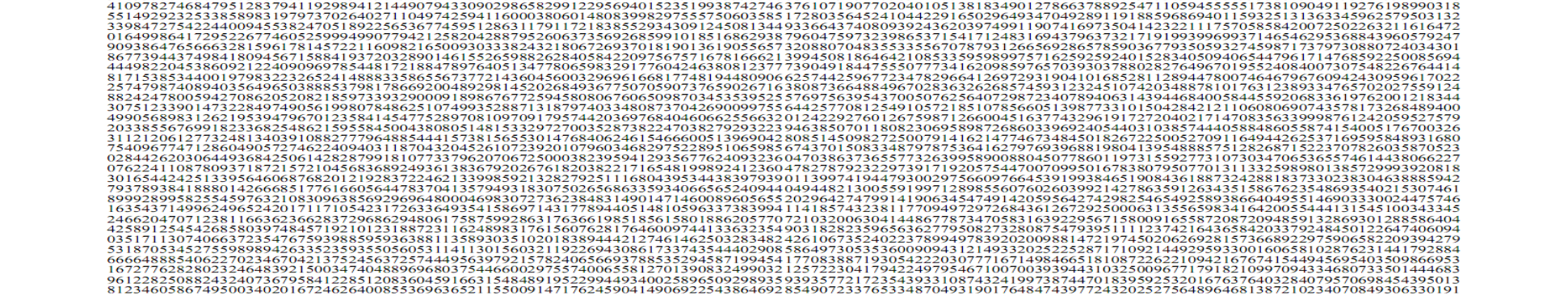
$$y^2 + y = x^3 - x$$

```
(0, 0)
(1, 0)
(-1, -1)
(2, -3)
(1/4, -5/8)
(6, 14)
(-5/9, 8/27)
(21/25, -69/125)
(-20/49, -435/343)
(161/16, -2065/64)
(116/529, -3612/12167)
(1357/841, 28888/24389)
(-3741/3481, -43355/205379)
(18526/16641, -2616119/2146689)
(8385/98596, -28076979/30959144)
(480106/4225, 332513754/274625)
(-239785/2337841, 331948240/3574558889)
(12551561/13608721, -8280062505/50202571769)
(-59997896/67387681, -641260644409/553185473329)
(683916417/264517696, -18784454671297/4302115807744)
(1849037896/6941055969, -318128427505160/578280195945297)
(51678803961/12925188721, 10663732503571536/1469451780501769)
(-270896443865/384768368209, 66316334575107447/23867066449493807 3)
```

Even the simplest solution can be large

$$y^2 + y = x^3 - 5115523309x - 140826120488927$$

Numerator of x-coordinate of smallest solution (5454 digits):



Denominator:

The theorem of Mordell and Weil

The set $E(\mathbb{Q})$ of rational solutions has the structure of a finitely generated abelian group.

The rank of E is defined as the rank of this finitely generated abelian group:

$$E(\mathbb{Q}) = (\mathbb{Z})^{rank(E)} \oplus T.$$

It is essentially the number of independent rational solutions.

The rank of E is defined as the rank of this finitely generated abelian group:

$$E(\mathbb{Q}) = (\mathbb{Z})^{rank(E)} \oplus T.$$

It is essentially the number of independent rational solutions.

- rank $(E) = 0$ means there are finitely many solutions.

The rank of E is defined as the rank of this finitely generated abelian group:

$$E(\mathbb{Q}) = (\mathbb{Z})^{rank(E)} \oplus T.$$

It is essentially the number of independent rational solutions.

- rank $(E) = 0$ means there are finitely many solutions.
- rank $(E) > 0$ means there are infinitely many solutions.

The rank of E is defined as the rank of this finitely generated abelian group:

$$E(\mathbb{Q}) = (\mathbb{Z})^{rank(E)} \oplus T.$$

It is essentially the number of independent rational solutions.

- rank $(E) = 0$ means there are finitely many solutions.
- rank $(E) > 0$ means there are infinitely many solutions.
- The curve $E(a)$ with equation

$$y(y+1) = x(x-1)(x+a)$$

has rank $= 0, 1, 2, 3, 4$ for $a = 0, 1, 2, 4, 16$.

The rank of E is defined as the rank of this finitely generated abelian group:

$$E(\mathbb{Q}) = (\mathbb{Z})^{rank(E)} \oplus T.$$

It is essentially the number of independent rational solutions.

- rank $(E) = 0$ means there are finitely many solutions.
- rank $(E) > 0$ means there are infinitely many solutions.
- The curve $E(a)$ with equation

$$y(y+1) = x(x-1)(x+a)$$

has rank $= 0, 1, 2, 3, 4$ for $a = 0, 1, 2, 4, 16$.

What are the possibilities for the finite group T?

Can the rank be arbitrarily large?

Barry Mazur proved that the only possibilities for T are

$T = \mathbb{Z}/n\mathbb{Z}$ for $1 \leq n \leq 10$ or $n = 12$.
$T = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for $n = 2, 4, 6, 8$.

The current record is rank(E) = 28

$$y^2 + xy + y = x^3 - x^2 - 2006776241557552658503320820933854275093023031217895650 2x + 3448161179503055646703298569039072037485594435931918036126600829629193948732243429$$

P_1 = [-212415009125438107329213746 3, 259854492051899599030515511070780628911531]
P_2 = [233450986603470175688475453 7, 188720041954944691808683165528036279315 31]
P_3 = [-167173605406236906387903866 3, 251709377261144287808506947241319126049131]
P_4 = [213913026013915666649298213 7, 366395091714397292024214596929412975275 31]
P_5 = [153470676446712072388547733 7, 854295853460176942890210328627810727995 31]
P_6 = [-273107948787567703334157506 3, 262521815484332191641284072623902143387531]
P_7 = [277572626684457164970545853 7, 128457554740140602488694876990826403699 31]
P_8 = [149438572932718895754183381 7, 884866055277334059861164945140492334114 51]
P_9 = [186843822862088735850906525 7, 592374032144377087127251403930593585891 31]
P_{10} = [200894510882574377486654253 7, 476906778801255528821517507815414247115 31]
P_{11} = [234836054091802516965163293 7, 174929300062005578573403324764488043635 31]
P_{12} = [-147208400709048117447000866 3, 246643450653503714199947441549759798469131]
P_{13} = [292412860770806121336328893 7, 283502644314888785014883564747673758995 31]
P_{14} = [537499389106606189329393453 7, 286188908427263386451175031916479893731531]
P_{15} = [170969076823335452333400855 7, 718988349746860894661597005292159809216 31]
P_{16} = [245095401135359314407259518 7, 444522817353263435704926255061071473653 1]
P_{17} = [296925470927355916746467493 7, 327668930753662708013336825431604696875 31]
P_{18} = [271191493494169260133288293 7, 206843661277838169865041398150659061353 1]
P_{19} = [200785860779968545287783289 37, 27796085411378066046560517256246240300915 31]
P_{20} = [215808245024073477431781069 7, 349943734019640268099696622418009012547 31]
P_{21} = [200464545824705902240322493 7, 480493297807046455224398669998884754675 31]
P_{22} = [297574945094799626494709133 7, 333989898260753223202089344101048578691 31]
P_{23} = [-210249046768628515014734786 3, 259576391459875789571677393171687203227531]
P_{24} = [311583179915063034902194537, 168104385229980603540109472915660153473931]
P_{25} = [277393100834186523144377181 7, 126321628346499210024141162737692758134 51]
P_{26} = [215658118814376840936346138 7, 351250929640229088970041505163751780873 31]
P_{27} = [386633049987241250881565913 7, 121197755655944226293036926715025847322531]
P_{28} = [223086828977357602377867873 7, 285587600305974856633870206007686400285 31]

Bryan Birch and Peter Swinnerton-Dyer made a prediction for the rank, based on the average number of solutions modulo p, for prime numbers p.

Prime numbers

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, . . .

Prime numbers

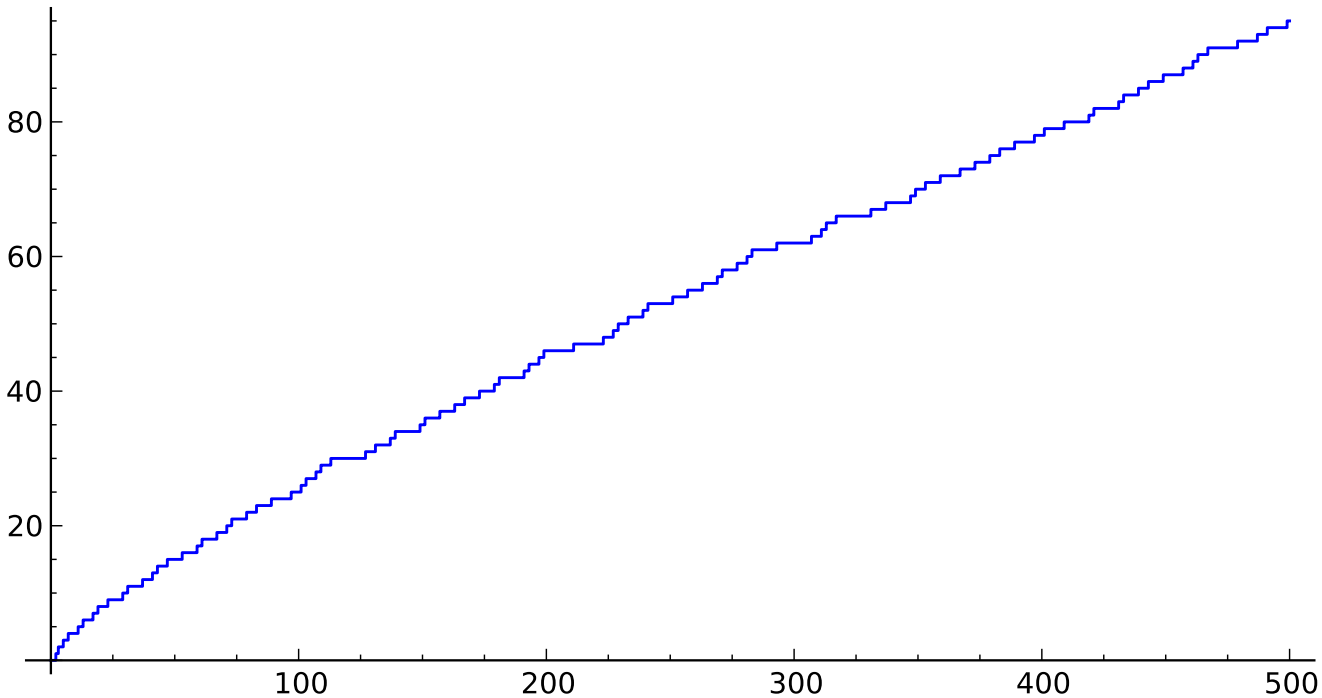
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, . . .

The largest explicit prime known is $2^{57885161} - 1$ with 17,425,170 digits.

Prime numbers

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, . . .

The largest explicit prime known is $2^{57885161} - 1$ with 17,425,170 digits.



What do we mean by a solution of the cubic equation modulo p?

What do we mean by a solution of the cubic equation modulo p?

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

$(x, y) \equiv (3, 1)$ is a solution modulo $p = 11$

What do we mean by a solution of the cubic equation modulo p?

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

$(x, y) \equiv (3, 1)$ is a solution modulo $p = 11$

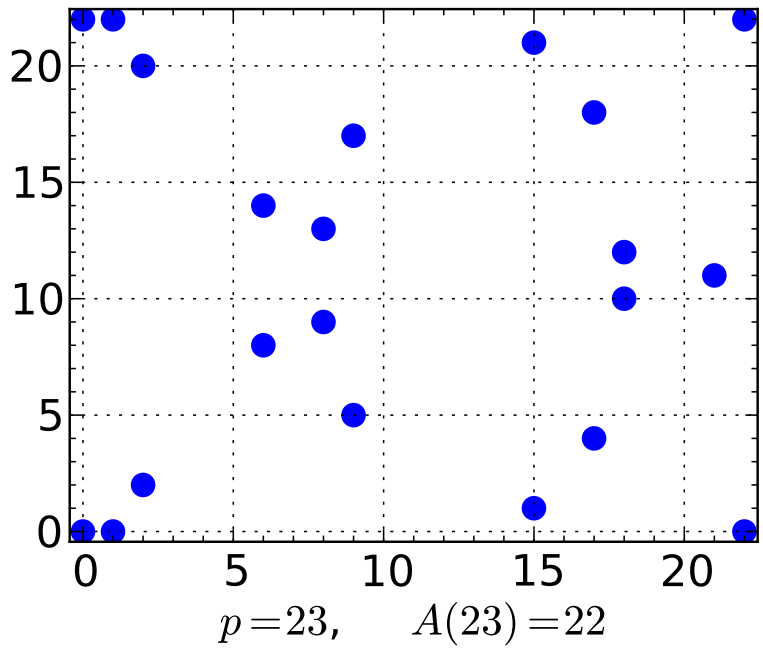
There are finitely many solutions $A(p)$ at each prime p.

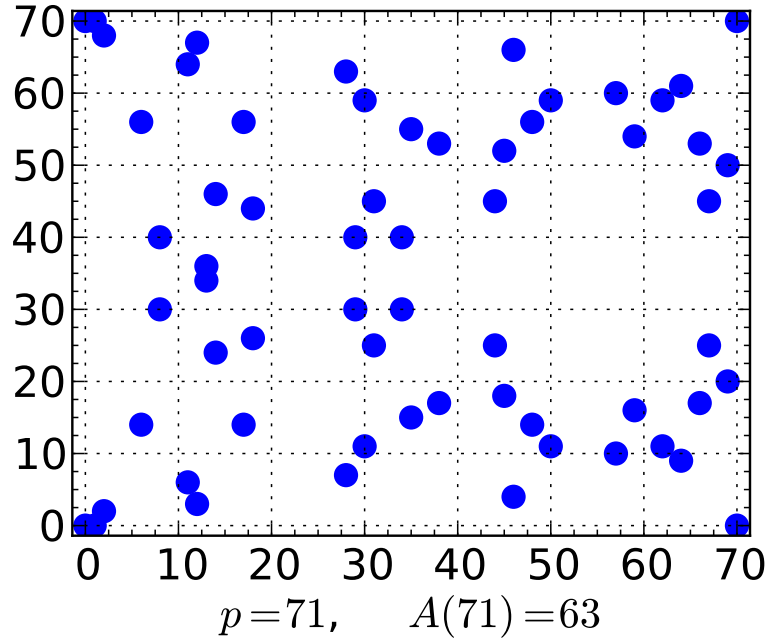
What do we mean by a solution of the cubic equation modulo p?

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

$(x, y) \equiv (3, 1)$ is a solution modulo $p = 11$

There are finitely many solutions $A(p)$ at each prime p.





It is common to write

$$A(p) = p + 1 - a(p)$$

It is common to write

$$A(p) = p + 1 - a(p)$$

We define the L-function of E by the infinite product

$$L(E, s) = \prod_p (1 - a(p)p^{-s} + p^{1-2s})^{-1} = \sum a(n)n^{-s}$$

It is common to write

$$A(p) = p + 1 - a(p)$$

We define the L-function of E by the infinite product

$$L(E, s) = \prod_p (1 - a(p)p^{-s} + p^{1-2s})^{-1} = \sum a(n)n^{-s}$$

However, this product only converges in the region $s > 3/2$.

It is common to write

$$A(p) = p + 1 - a(p)$$

We define the L-function of E by the infinite product

$$L(E, s) = \prod_p (1 - a(p)p^{-s} + p^{1-2s})^{-1} = \sum a(n)n^{-s}$$

However, this product only converges in the region $s > 3/2$.

If we formally set $s = 1$ in the product, we get

$$\prod_p (1 - a(p)p^{-1} + p^{-1})^{-1} = \prod_p p/A(p)$$

$$\text{"}L(E,1)\text{"} = \prod_p (1 - a(p)p^{-1} + p^{-1})^{-1} = \prod_p p/A(p)$$

$$\text{"}L(E,1)\text{"} = \prod_p (1 - a(p)p^{-1} + p^{-1})^{-1} = \prod_p p/A(p)$$

If $A(p)$ is large on average compared with p, this product will approach 0.

$$\text{"}L(E,1)\text{"} = \prod_p (1 - a(p)p^{-1} + p^{-1})^{-1} = \prod_p p/A(p)$$

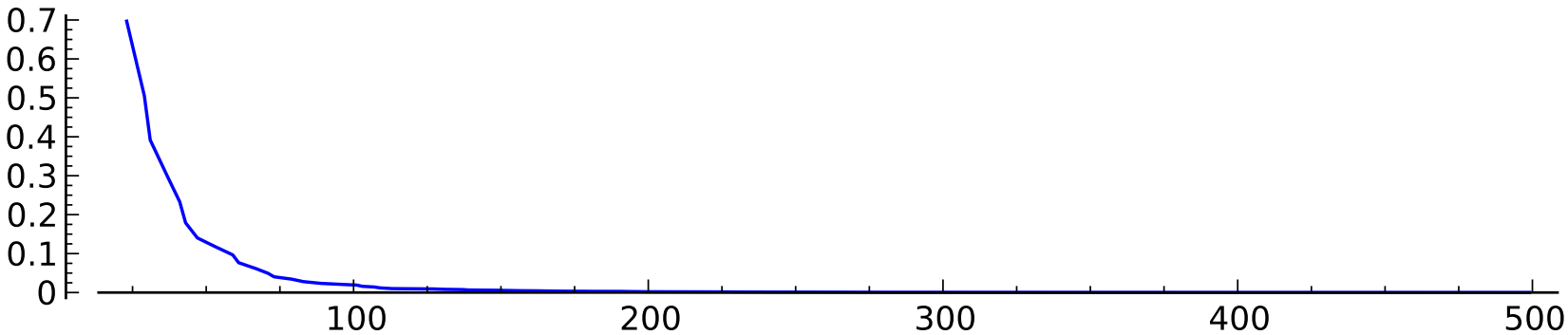
If $A(p)$ is large on average compared with p, this product will approach 0.

The larger $A(p)$ is on average, the faster it will tend to 0.

$$\text{"}L(E,1)\text{"} = \prod_p (1 - a(p)p^{-1} + p^{-1})^{-1} = \prod_p p/A(p)$$

If $A(p)$ is large on average compared with p, this product will approach 0.

The larger $A(p)$ is on average, the faster it will tend to 0.



The conjecture of Birch and Swinnerton-Dyer

1. The function $L(E, s)$ has an analytic continuation to a neighborhood of $s = 1$.

The conjecture of Birch and Swinnerton-Dyer

1. The function $L(E, s)$ has an analytic continuation to a neighborhood of $s = 1$.
2. The order of vanishing of $L(E, s)$ at $s = 1$ is equal to the rank of E.

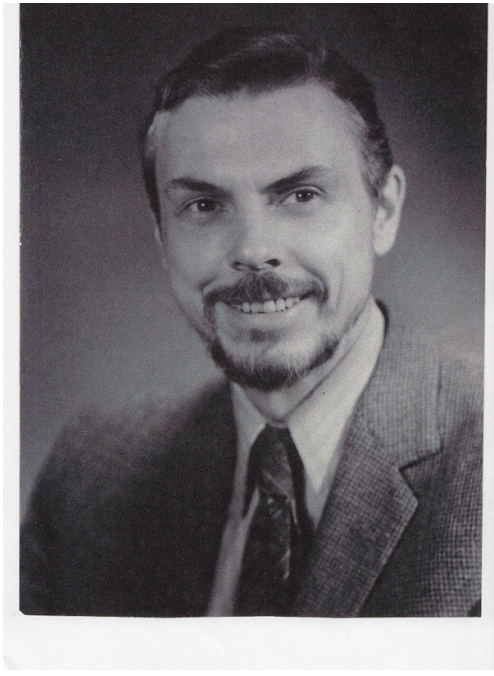
The conjecture of Birch and Swinnerton-Dyer

1. The function $L(E, s)$ has an analytic continuation to a neighborhood of $s = 1$.
2. The order of vanishing of $L(E, s)$ at $s = 1$ is equal to the rank of E.
3. The leading term $c(E)$ in the Taylor expansion of $L(E, s)$ at $s = 1$ is given by a formula involving arithmetic invariants of E.

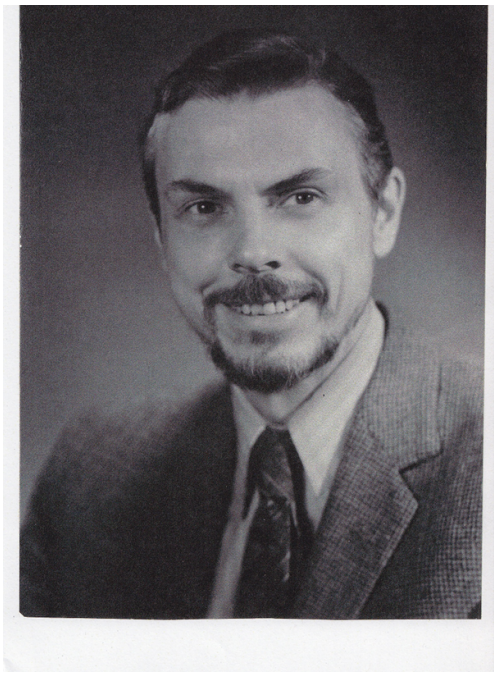
$$L(E, s) = c(E)(s - 1)^{rank(E)} + ...$$

The most mysterious arithmetic invariant is an abelian group $Ш(E)$ studied by John Tate and Igor Shafarevich. This measures the obstruction in passing from a solution over all completions of the rational numbers to a rational solution.

The most mysterious arithmetic invariant is an abelian group $Ш(E)$ studied by John Tate and Igor Shafarevich. This measures the obstruction in passing from a solution over all completions of the rational numbers to a rational solution.



The most mysterious arithmetic invariant is an abelian group $Ш(E)$ studied by John Tate and Igor Shafarevich. This measures the obstruction in passing from a solution over all completions of the rational numbers to a rational solution.



They conjectured that $Ш(E)$ is finite. Its order appears in the formula for the leading term $c(E)$.

The analytic continuation of $L(E, s) = \sum a(n)n^{-s}$ was obtained by Andrew Wiles and Richard Taylor (1995).

The analytic continuation of $L(E, s) = \sum a(n)n^{-s}$ was obtained by Andrew Wiles and Richard Taylor (1995). They proved that the function defined by the infinite series

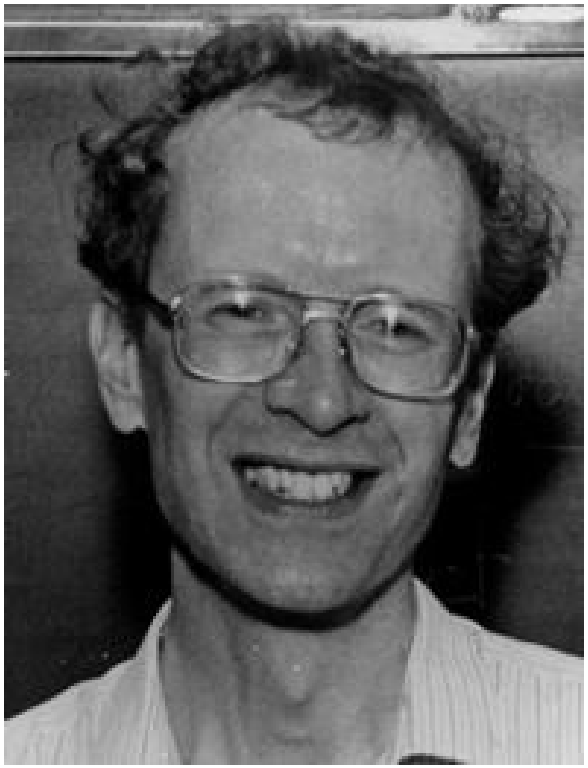
$$F(\tau) = \sum a(n)e^{2\pi in\tau}$$

is a modular form for a congruence subgroup of $SL_2(\mathbb{Z})$.

The analytic continuation of $L(E, s) = \sum a(n)n^{-s}$ was obtained by Andrew Wiles and Richard Taylor (1995). They proved that the function defined by the infinite series

$$F(\tau) = \sum a(n)e^{2\pi in\tau}$$

is a modular form for a congruence subgroup of $SL_2(\mathbb{Z})$.



Combining a limit formula I proved with Don Zagier (1983) with work of Victor Kolyvagin (1986) we can now show the following.

Combining a limit formula I proved with Don Zagier (1983) with work of Victor Kolyvagin (1986) we can now show the following.

If $L(E, 1) \neq 0$ the rank of $E(\mathbb{Q})$ is zero, so there are finitely many solutions.

Combining a limit formula I proved with Don Zagier (1983) with work of Victor Kolyvagin (1986) we can now show the following.

If $L(E, 1) \neq 0$ the rank of $E(\mathbb{Q})$ is zero, so there are finitely many solutions.

If $L(E, 1) = 0$ and $L'(E, 1) \neq 0$ the rank of $E(\mathbb{Q})$ is one, so there are infinitely many solutions.

Combining a limit formula I proved with Don Zagier (1983) with work of Victor Kolyvagin (1986) we can now show the following.

If $L(E,1) \neq 0$ the rank of $E(\mathbb{Q})$ is zero, so there are finitely many solutions.

If $L(E,1) = 0$ and $L'(E,1) \neq 0$ the rank of $E(\mathbb{Q})$ is one, so there are infinitely many solutions.

In both of these cases, the group $Ш(E)$ is finite, and the conjecture for the leading term is (almost) true.

Combining a limit formula I proved with Don Zagier (1983) with work of Victor Kolyvagin (1986) we can now show the following.

If $L(E, 1) \neq 0$ the rank of $E(\mathbb{Q})$ is zero, so there are finitely many solutions.

If $L(E, 1) = 0$ and $L'(E, 1) \neq 0$ the rank of $E(\mathbb{Q})$ is one, so there are infinitely many solutions.

In both of these cases, the group $Ш(E)$ is finite, and the conjecture for the leading term is (almost) true.

When the order of $L(E, s)$ at $s = 1$ is greater than one we cannot prove anything in general...

When the order of $L(E, s)$ at $s = 1$ is greater than one we cannot prove anything in general...

But the computer has been a great guide.

When the order of $L(E, s)$ at $s = 1$ is greater than one we cannot prove anything in general...

But the computer has been a great guide.

Here is a summary of the evidence for the simplest rank 2 curve E with equation

$$y(y + 1) = x(x - 1)(x + 2)$$

When the order of $L(E, s)$ at $s = 1$ is greater than one we cannot prove anything in general...

But the computer has been a great guide.

Here is a summary of the evidence for the simplest rank 2 curve E with equation

$$y(y + 1) = x(x - 1)(x + 2)$$

- the order of vanishing of $L(E, s)$ at $s = 1$ is equal to 2
- most primes up to 50,000 do not divide the order of $Ш(E)$

When the order of $L(E, s)$ at $s = 1$ is greater than one we cannot prove anything in general...

But the computer has been a great guide.

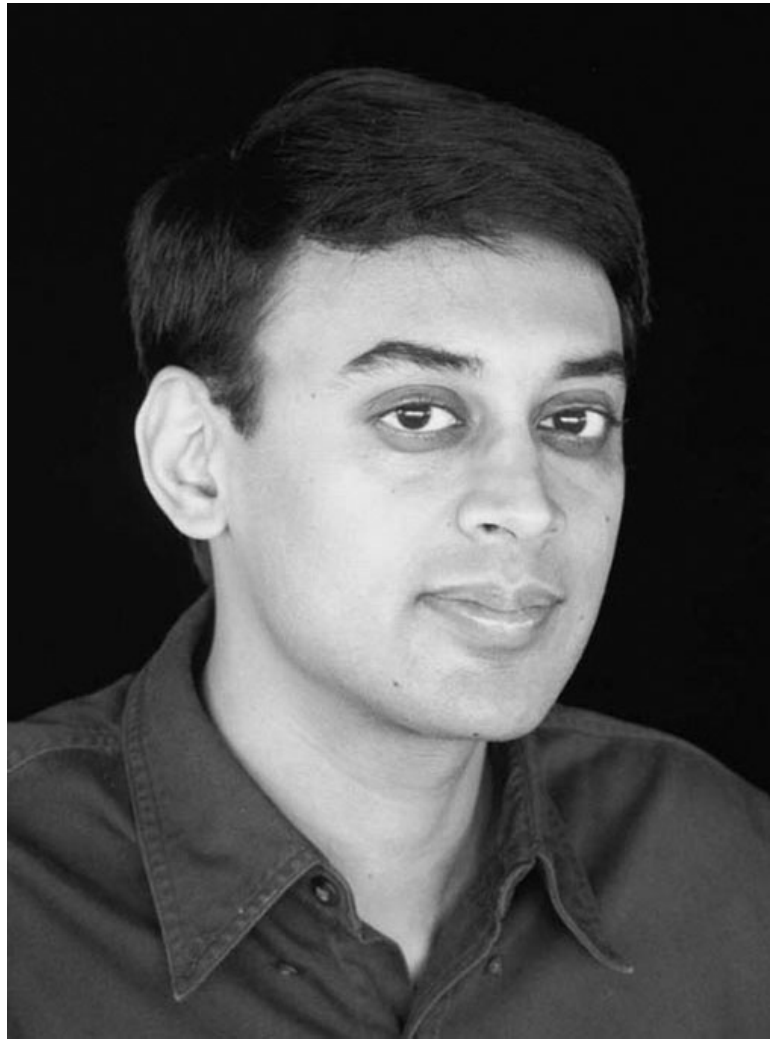
Here is a summary of the evidence for the simplest rank 2 curve E with equation

$$y(y + 1) = x(x - 1)(x + 2)$$

- the order of vanishing of $L(E, s)$ at $s = 1$ is equal to 2
- most primes up to 50,000 do not divide the order of $Ш(E)$

Manjul Bhargava has recently made progress on the study of the average rank, for all elliptic curves with rational coefficients.

Manjul Bhargava has recently made progress on the study of the average rank, for all elliptic curves with rational coefficients.



Enumerating elliptic curves over $\mathbb{Q}$

- Every such curve has a unique equation of the form $y^2 = x^3 + Ax + B$ where A and B are integers (not divisible by p^4 and p^6, for any prime p), and $\Delta = -4A^3 - 27B^2 \neq 0$

Enumerating elliptic curves over $\mathbb{Q}$

- Every such curve has a unique equation of the form $y^2 = x^3 + Ax + B$ where A and B are integers (not divisible by p^4 and p^6, for any prime p), and $\Delta = -4A^3 - 27B^2 \neq 0$
- Define the height $H(E)$ as the maximum of the positive integers $|A|^3$ and $|B|^2$.

Enumerating elliptic curves over $\mathbb{Q}$

- Every such curve has a unique equation of the form $y^2 = x^3 + Ax + B$ where A and B are integers (not divisible by p^4 and p^6, for any prime p), and $\Delta = -4A^3 - 27B^2 \neq 0$
- Define the height $H(E)$ as the maximum of the positive integers $|A|^3$ and $|B|^2$.
- For any positive real number X, there are only finitely many curves with $H(E) \leq X$.

Enumerating elliptic curves over $\mathbb{Q}$

- Every such curve has a unique equation of the form $y^2 = x^3 + Ax + B$ where A and B are integers (not divisible by p^4 and p^6, for any prime p), and $\Delta = -4A^3 - 27B^2 \neq 0$
- Define the height $H(E)$ as the maximum of the positive integers $|A|^3$ and $|B|^2$.
- For any positive real number X, there are only finitely many curves with $H(E) \leq X$.
- Call this number $N(X)$. It grows at the same rate as $(X)^{1/2}(X)^{1/3} = X^{5/6}$.

- Define the average rank by the limit as $X \to \infty$ of

$$\frac{1}{N(X)} \sum_{H(E) \leq X} rank(E)$$

- Define the average rank by the limit as $X \to \infty$ of

$$\frac{1}{N(X)} \sum_{H(E) \leq X} rank(E)$$

- We suspect that this limit exists, and is equal to $1/2$.

- Define the average rank by the limit as $X \to \infty$ of

$$\frac{1}{N(X)} \sum_{H(E) \leq X} rank(E)$$

- We suspect that this limit exists, and is equal to $1/2$.
- Bhargava and Arul Shankar have shown why there is an upper bound on the limit, and have obtained a specific upper bound which is less than 1.

- Define the average rank by the limit as $X \to \infty$ of

$$\frac{1}{N(X)} \sum_{H(E) \leq X} rank(E)$$

- We suspect that this limit exists, and is equal to $1/2$.
- Bhargava and Arul Shankar have shown why there is an upper bound on the limit, and have obtained a specific upper bound which is less than 1.
- They show that a positive proportion of curves have rank zero, and (with Chris Skinner) that a positive proportion of curves have rank one.

Their method combines the invariant theory of integral representations with techniques from the geometry of numbers.

Their method combines the invariant theory of integral representations with techniques from the geometry of numbers.

It applies more generally to hyperelliptic curves of genus $n \geq 1$ with a rational Weierstrass point.

$$y^2 = x^{2n+1} + c_1 x^{2n} + c_2 x^{2n-1} + \ldots c_{2n+1}$$

Their method combines the invariant theory of integral representations with techniques from the geometry of numbers.

It applies more generally to hyperelliptic curves of genus $n \geq 1$ with a rational Weierstrass point.

$$y^2 = x^{2n+1} + c_1 x^{2n} + c_2 x^{2n-1} + \ldots c_{2n+1}$$

Bhargava and I have shown that the average rank of their Jacobians is less than $3/2$.

Their method combines the invariant theory of integral representations with techniques from the geometry of numbers.

It applies more generally to hyperelliptic curves of genus $n \geq 1$ with a rational Weierstrass point.

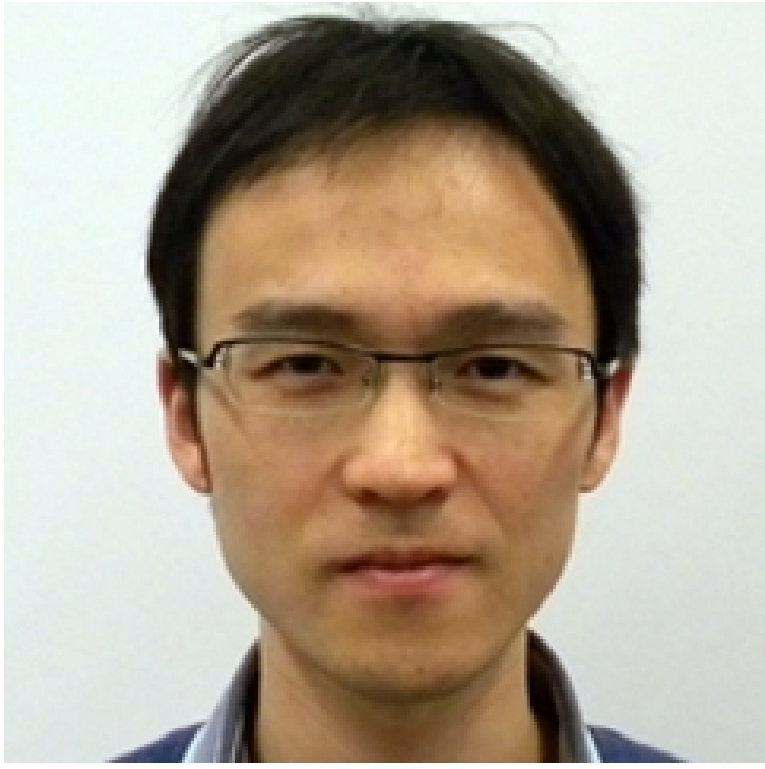
$$y^2 = x^{2n+1} + c_1 x^{2n} + c_2 x^{2n-1} + \ldots c_{2n+1}$$

Bhargava and I have shown that the average rank of their Jacobians is less than $3/2$.

Bjorn Poonen and Michael Stoll then conclude that a positive proportion of these curves have only one rational point, the point above $x = \infty$, once $2n + 1 \geq 5$

Bhargava, Skinner, and Wei Zhang have recently shown that the conjecture of Birch and Swinnerton-Dyer is true for at least 66% of all elliptic curves over $\mathbb{Q}$!

Bhargava, Skinner, and Wei Zhang have recently shown that the conjecture of Birch and Swinnerton-Dyer is true for at least 66% of all elliptic curves over $\mathbb{Q}$!



For curves of rank ≥ 2 almost nothing is known.

For curves of rank ≥ 2 almost nothing is known.

THANK YOU!