The rank of elliptic curves

Benedict Gross

October, 2012
After linear and quadratic equations come cubic equations, or elliptic curves.

\[ x^3 + y^3 = 1 \quad \text{and} \quad y^2 + y = x^3 - x \]
After linear and quadratic equations come cubic equations, or elliptic curves.

\[ x^3 + y^3 = 1 \quad \text{and} \quad y^2 + y = x^3 - x \]

There may either be a finite or an infinite number of rational solutions.
After linear and quadratic equations come cubic equations, or elliptic curves.

\[ x^3 + y^3 = 1 \quad y^2 + y = x^3 - x \]

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)
(1849037896/694105596, -318128427505160/578280195945297)
(51678803961/12925188721, 10663732503571536/1469451780501769)
(-270896443865/384768368209, 66316334575107447/238670664494938073)
Even the simplest solution can be large

\[ y^2 + y = x^3 \quad 5115523309x - 140826120488927 \]

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:

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

It is essentially the number of independent rational solutions.
The rank of $E$ is defined as the rank of this finitely generated abelian group:

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

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:

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

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:

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

It is essentially the number of independent rational solutions.

- $\text{rank}(E) = 0$ means there are finitely many solutions.
- $\text{rank}(E) > 0$ 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 $a = 0, 1, 2, 4, 16$. 

Can the rank be arbitrarily large?
The rank of \( E \) is defined as the rank of this finitely generated abelian group:

\[
E(\mathbb{Q}) = (\mathbb{Z})^{\text{rank}(E)} \oplus T.
\]

It is essentially the number of independent rational solutions.

- \( \text{rank} \ (E) = 0 \) means there are finitely many solutions.
- \( \text{rank} \ (E) > 0 \) 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 \( a = 0, 1, 2, 4, 16 \).

Can the rank be arbitrarily large?
The current record is rank\( (E) = 28 \)

\[
y^2 + xy + y = x^3 - x^2 - 2006772415575526585033208209338542750930230312178956502x + 34481611795030556467032985690390720374855944359319180361266008296291939448732243429
\]

\[
P_1 = [-2124150091254381073292137463, 259854492051899599030515511070780628911531] 
\]

\[
P_2 = [2334509866034701756884754537, 18872004195494469180868316552803627931531] 
\]

\[
P_3 = [-167136054062369063879038663, 25170937726114287808506947241319126049131] 
\]

\[
P_4 = [2139130260139156666492982137, 36639509171439729202421459692941297527531] 
\]

\[
P_5 = [1534706764647120723885477337, 854299585346017694289021032368278107279953] 
\]

\[
P_6 = [-273107948785767033341575063, 262521815484332191641284072623902143387531] 
\]

\[
P_7 = [2775726266844571649705458537, 12845755474014060248869487699082640369931] 
\]

\[
P_8 = [1494385729327188957541833817, 8848660552773340598611649451409233414151] 
\]

\[
P_9 = [18684382282088735850965257, 59237403214437708712725140393059358589131] 
\]

\[
P_{10} = [2008945108825743774866542537, 47690677880125552882151750781541424711531] 
\]

\[
P_{11} = [234386059190825169651632937, 1749293006200557857340332476448804363531] 
\]

\[
P_{12} = [-14720840070904948117470008663, 24664345065350371419994744154979798469131] 
\]

\[
P_{13} = [2924128607708061213363288937, 283502644314888878501488356474767375899531] 
\]

\[
P_{14} = [5374993891066061893293934537, 28618890842762363864511750347807993731531] 
\]

\[
P_{15} = [170690976823354523324008557, 71896834974686089466159700529215980291631] 
\]

\[
P_{16} = [2450954011353593144072595187, 4445228173532634357049262550610714736531] 
\]

\[
P_{17} = [2969254709273559176464674937, 3276689307536627080133638254316049687531] 
\]

\[
P_{18} = [2711914934941962601332882937, 2068436612778381698650413981506590613531] 
\]

\[
P_{19} = [20078560779968554258778328937, 2779608541137806604656051725626426403091531] 
\]

\[
P_{20} = [2158082450240734774317810697, 3499437340196402680969662241800901254731] 
\]

\[
P_{21} = [200464545247059022403224937, 480493297807046552434999888475467531] 
\]

\[
P_{22} = [29757494594979626449709133, 3398898982607532232208934410104857869131] 
\]

\[
P_{23} = [-2102490467686285150147347863, 259576391459875789571677393171687203227531] 
\]

\[
P_{24} = [311583179915063034902194537, 168104385229980603540109472915660153473931] 
\]

\[
P_{25} = [27739310083418652314437718127, 12632162834649921002421116273769275813451] 
\]

\[
P_{26} = [2156581188143786409363461387, 35125092964022908970043150516375178087331] 
\]

\[
P_{27} = [3866330499872412508215659137, 121197775655944226293036926715025847322531] 
\]

\[
P_{28} = [22308682879773576023778678737, 2855876003597485663387020600768640028531] 
\]
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, \ldots
Prime numbers


The largest explicit prime known is $2^{43112609} - 1$ with 12,978,189 digits.
Prime numbers


The largest explicit prime known is $2^{43112609} - 1$ with 12,978,189 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 $p$?

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

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

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

$p = 23, \ A(23) = 22$

$p = 71, \ A(71) = 63$
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

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

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

However, this product only converges in the region \( s > 3/2 \).

If we formally set \( s = 1 \) in the product, we get

\[ \prod_p \left( 1 - a(p)p^{-1} + p^{-1} \right)^{-1} = \prod_p p/A(p) \]
\[ L(E, 1) = \prod_p (1 - a(p)p^{-1} + p^{-1})^{-1} = \prod_p p/A(p) \]
\[
L(E, 1) = \prod_{p} (1 - a(p)p^{-1} + p^{-1})^{-1} = \prod_{p} \frac{p}{A(p)}
\]

If \( A(p) \) is large on average compared with \( p \), this product will approach 0.
"L(E, 1)" = \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.
"\( L(E, 1) \)" = \( \prod_p (1 - a(p)p^{-1} + p^{-1})^{-1} = \prod_p p/A(p) \)

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 $E$.

$$L(E, s) = c(E)(s - 1)^{\text{rank}(E)} + \ldots$$
The most mysterious arithmetic invariant is an abelian group $\text{III}(E)$ 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 $\Sha(E)$ 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 $\Sha(E)$ 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 \( SL_2(\mathbb{Z}) \).
When combined with earlier work of Ken Ribet (1986), this led to a proof of Fermat’s last theorem.
When combined with earlier work of Ken Ribet (1986), this led to a proof of Fermat’s last theorem.

What about the rest of the Birch and Swinnerton-Dyer conjecture?
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 $X(E)$ is finite, and the conjecture for the leading term is 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 \( X(E) \) is finite, and the conjecture for the leading term is 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.
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 \( \text{III}(E) \) is finite, and the conjecture for the leading term is 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 $\Sha(E)$ is finite, and the conjecture for the leading term is 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 $\text{III}(E)$
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 $\lambda(E)$
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 $|B|^2$. 

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 $X^{1/2} = X^{5/6}$. 


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

\[
\frac{1}{N(X)} \sum_{H(E) \leq X} \text{rank}(E)
\]
Define the average rank by the limit as $X \to \infty$ of

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

We suspect that this limit exists, and is equal to $1/2$. 
Define the average rank by the limit as $X \to \infty$ of

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

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

In fact, we think that on average half the elliptic curves have rank zero and half the elliptic curves have rank one.
Define the average rank by the limit as $X \to \infty$ of

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

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

In fact, we think that on average half the elliptic curves have rank zero and half the elliptic curves have rank one.

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 study the 2-Selmer group

\[
E(\mathbb{Q})/2E(\mathbb{Q}) \rightarrow Sel(E, 2) \rightarrow H^1(\mathbb{Q}, E[2])
\]
They study the 2-Selmer group

\[ E(\mathbb{Q})/2E(\mathbb{Q}) \to Sel(E, 2) \to H^1(\mathbb{Q}, E[2]) \]

They prove that the average order of \( Sel(E, 2) \) is equal to 3, so the average rank (if the limit exists) is less than 3/2.
They study the 2-Selmer group

\[ E(\mathbb{Q})/2E(\mathbb{Q}) \rightarrow Sel(E, 2) \rightarrow H^1(\mathbb{Q}, E[2]) \]

They prove that the average order of \( Sel(E, 2) \) is equal to 3, so the average rank (if the limit exists) is less than \( 3/2 \).

To calculate the limit as \( X \rightarrow \infty \) of

\[
\frac{1}{N(X)} \sum_{H(E) \leq X} \#Sel(E, 2)
\]

they study the orbits of \( PGL_2(\mathbb{Z}) \) on binary quartic forms

\[ ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 \]
Their method combines invariant theory with techniques from the geometry of numbers.
Their method combines invariant theory with techniques from the geometry of numbers.

This applies more generally, for example to hyperelliptic curves of genus $n \geq 2$ with a marked Weierstrass point.
Their method combines invariant theory with techniques from the geometry of numbers.

This applies more generally, for example to hyperelliptic curves of genus $n \geq 2$ with a marked Weierstrass point.

These curves have equations of the form

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

and I’ll speak about them in the next two lectures.
Their method combines invariant theory with techniques from the geometry of numbers.

This applies more generally, for example to hyperelliptic curves of genus $n \geq 2$ with a marked Weierstrass point.

These curves have equations of the form

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

and I’ll speak about them in the next two lectures.

Thank you.