The Birch and Swinnerton-Dyer conjecture

Christian Wuthrich

31 January $2^2 \cdot 5 \cdot 101$

Question

Solve

$$y^2 = x^3 + x + 101$$

Question

Solve

$$y^2 = x^3 + x + 101$$

for x and y in $\mathbb{Q}$.

Question

Solve

$$y^2 = x^3 + x + 101$$

for x and y in $\mathbb{Q}$.

You may spot $(4, 13)$ is a solution. And $(4, -13)$, too.

Question

Solve

$$y^2 = x^3 + x + 101$$

for x and y in $\mathbb{Q}$.

You may spot $(4, 13)$ is a solution. And $(4, -13)$, too.
A computer search:

$$\left(-\frac{20}{9}, \pm\frac{253}{27}\right), \quad \left(-\frac{23}{16}, \pm\frac{629}{64}\right) \quad \left(-\frac{3007}{676}, , \pm\frac{51351}{17576}\right)$$

Question

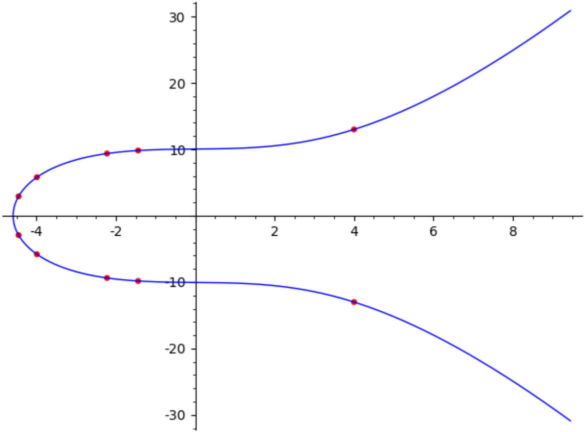
Solve
$$y^2 = x^3 + x + 101$$
for x and y in $\mathbb{Q}$.

You may spot $(4, 13)$ is a solution. And $(4, -13)$, too.
A computer search:

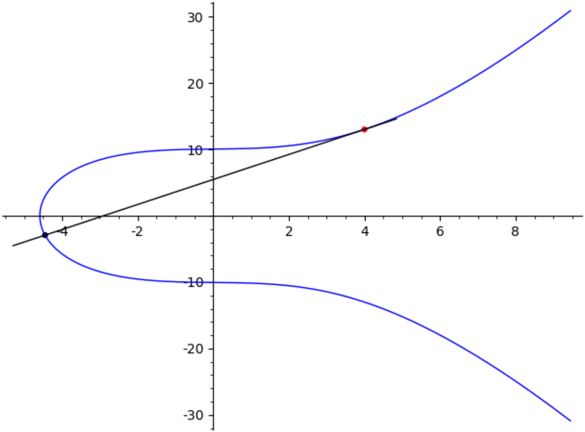
$$\left(-\frac{20}{9}, \pm\frac{253}{27}\right), \quad \left(-\frac{23}{16}, \pm\frac{629}{64}\right) \quad \left(-\frac{3007}{676}, , \pm\frac{51351}{17576}\right)$$

Magic (?) : There is one with

$$x = -\frac{4612857350259810993468068597304177602477150769682387182585 61}{1597430887445158640748414605995145667213850960420230708998 4}.$$



$$y^2 = x^3 + x + 101$$



Tangent at $(4, 13)$ meets again at $\left(-\frac{3007}{676}, -\frac{51351}{17576}\right)$

$$y^2 = x^3 + x + 101$$

$$y^2 = x^3 + x + 101$$

If $y = \lambda x + \nu$ is the tangent at x_0, then

$$-(\lambda x + \nu)^2 + (x^3 + x + 101) = 0$$

has a double solution at $x = x_0$.

$$y^2 = x^3 + x + 101$$

If $y = \lambda x + \nu$ is the tangent at x_0, then

$$-(\lambda x + \nu)^2 + (x^3 + x + 101) = 0$$

has a double solution at $x = x_0$.
It factors as

$$(x - x_0)^2 \cdot (x - x_1) = 0$$

$$y^2 = x^3 + x + 101$$

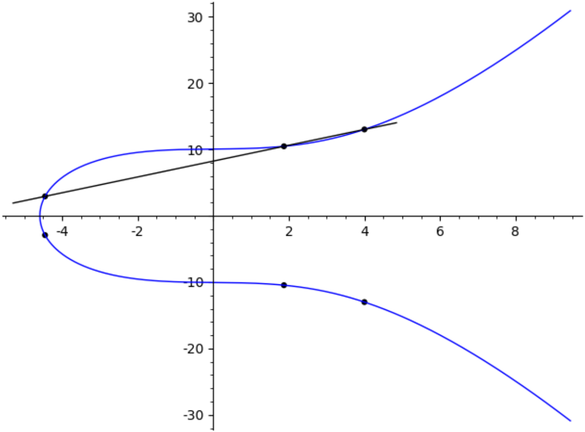
If $y = \lambda x + \nu$ is the tangent at x_0, then

$$-(\lambda x + \nu)^2 + (x^3 + x + 101) = 0$$

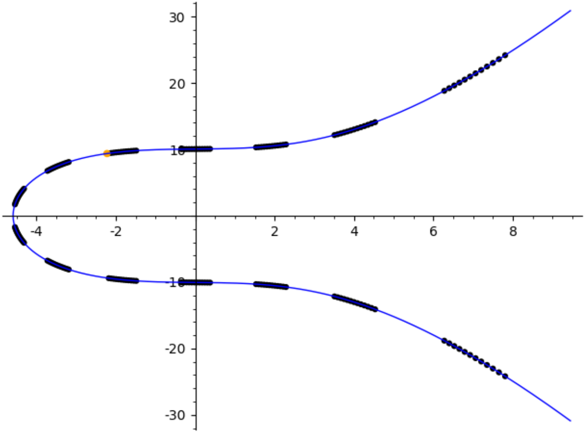
has a double solution at $x = x_0$.
It factors as

$$(x - x_0)^2 \cdot (x - x_1) = 0$$

and x_0, λ, ν and $x_1 \in \mathbb{Q}$.



Chords = Secants work, too



$Q = \left(-\frac{20}{9}, \frac{253}{27}\right)$ cannot be reached from $P = (4, 13)$

Question

Are there infinitely many rational solutions over $\mathbb{Q}$?

Question

Are there infinitely many rational solutions over $\mathbb{Q}$?

Example

$$E_2: \qquad y^2 = x^3 + x + 2$$

Question

Are there infinitely many rational solutions over $\mathbb{Q}$?

Example

$$E_2 : \qquad y^2 = x^3 + x + 2$$

has only three solutions $(-1, 0)$, $(1, -2)$, and $(1, 2)$.

Question

Are there infinitely many rational solutions over $\mathbb{Q}$?

Example

$$E_1: \qquad y^2 = x^3 + x + 1$$

Question

Are there infinitely many rational solutions over $\mathbb{Q}$?

Example

$$E_1: \qquad y^2 = x^3 + x + 1$$

has infinitely many solutions. $(0,1)$, $(\frac{1}{4}, \frac{9}{4})$, $(72, 611)$, ...

Question

Are there infinitely many rational solutions over $\mathbb{Q}$?

Example

$$E_1: \qquad y^2 = x^3 + x + 1$$

has infinitely many solutions. $(0,1)$, $(\frac{1}{4}, \frac{9}{4})$, $(72, 611)$, ...
The following x-coordinates are

$$-\frac{287}{1296}, \quad \frac{43992}{82369}, \quad \frac{26862913}{1493284}, \quad \frac{139455877527}{1824793048}, \quad -\frac{3596697936}{8760772801},$$
$$\frac{7549090222465}{8662944250944}, \quad \frac{51865013741670864}{6504992707996225}, \quad -\frac{173161424238594532415}{310515636774481238884}, \quad \ldots$$

An elliptic curve E over a field K is

An elliptic curve E over a field K is

- a projective curve of genus 1 with a specified base-point $O \in E(K)$.

An elliptic curve E over a field K is

- a projective curve of genus 1 with a specified base-point $O \in E(K)$.
- an non-singular equation of the form

$$E: \qquad y^2 = x^3 + A\,x + B$$

for some A and B in K.

An elliptic curve E over a field K is

- a projective curve of genus 1 with a specified base-point $O \in E(K)$.
- an non-singular equation of the form

$$E: \qquad y^2 = x^3 + A\,x + B$$

for some A and B in K if $\mathrm{char}(K) > 3$.

An elliptic curve E over a field K is

- a projective curve of genus 1 with a specified base-point $O \in E(K)$.
- an non-singular equation of the form

$$E: \qquad y^2 = x^3 + A\,x + B$$

  for some A and B in K if $\mathrm{char}(K) > 3$.
- a projective curve with an algebraic group structure.

An elliptic curve E over a field K is

- a projective curve of genus 1 with a specified base-point $O \in E(K)$.
- an non-singular equation of the form

$$E: \qquad y^2 = x^3 + A\,x + B$$

  for some A and B in K if $\mathrm{char}(K) > 3$.
- a projective curve with an algebraic group structure.

Our main question

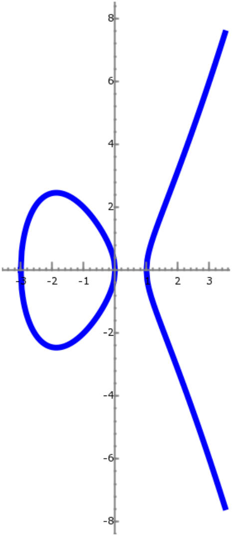
How can we determine the set of solutions $E(K)$ with coordinates in K ?

Addition on elliptic curves

$$E: \quad y^2 = x^3 + A\,x + B$$

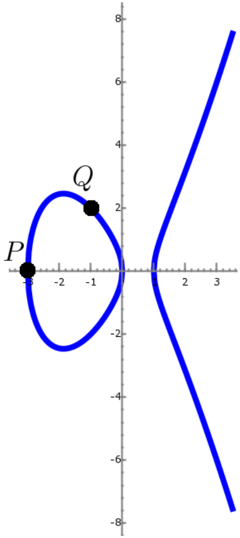
Addition on elliptic curves

$$E: \quad y^2 = x^3 + Ax + B$$



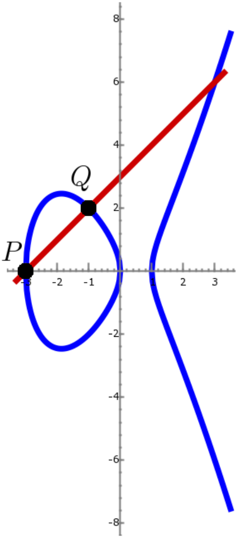
Addition on elliptic curves

$$E: \quad y^2 = x^3 + Ax + B$$



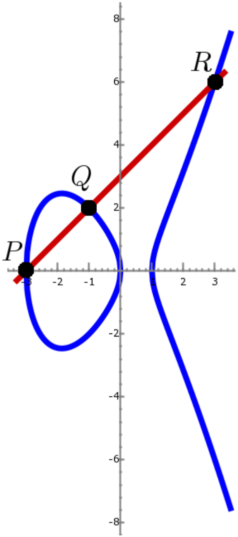
Addition on elliptic curves

$$E: \quad y^2 = x^3 + Ax + B$$



Addition on elliptic curves

$$E: \quad y^2 = x^3 + Ax + B$$

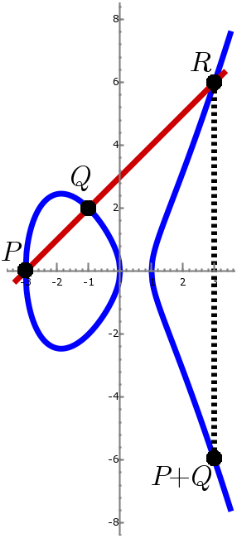


Addition on elliptic curves

$$E: \quad y^2 = x^3 + Ax + B$$

This is an abelian group law on $E(K)$:

- $(P+Q)+R = P+(Q+R)$
- $P+O = P$
- $P+(-P) = O$
- $P+Q = Q+P$

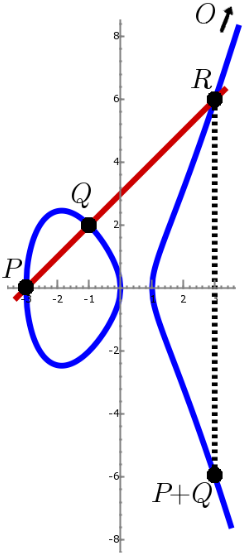


Addition on elliptic curves

$$E: \quad y^2 = x^3 + Ax + B$$

This is an abelian group law on $E(K)$:

- $(P+Q)+R = P+(Q+R)$
- $P+O = P$
- $P+(-P) = O$
- $P+Q = Q+P$



Elliptic curves over finite fields

p a prime number.
$A, B \in \mathbb{F}_p$, the field with p elements.

$$y^2 = x^3 + Ax + B$$

Then $E(\mathbb{F}_p)$ is a finite group.

Elliptic curves over finite fields

p a prime number.
$A, B \in \mathbb{F}_p$, the field with p elements.

$$y^2 = x^3 + Ax + B$$

Then $E(\mathbb{F}_p)$ is a finite group.

Example

$y^2 = x^3 + x + 101$ has 88 solutions modulo 103.

Elliptic curves over finite fields

p a prime number.
$A, B \in \mathbb{F}_p$, the field with p elements.

$$y^2 = x^3 + Ax + B$$

Then $E(\mathbb{F}_p)$ is a finite group.

Example

$y^2 = x^3 + x + 101$ has 88 solutions modulo 103.

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

Elliptic curves over finite fields

Curve sepc160k1

$$E:\; y^2 = x^3 + 7 \qquad \text{with } K = \mathbb{F}_p$$

$$p = 1461501637330902918203684832716283019651637554291$$

$$N_p = 1461501637330902918203686915170869725397159163571$$

Elliptic curves over finite fields

Curve sepc160k1

$$E: \; y^2 = x^3 + 7 \qquad \text{with } K = \mathbb{F}_p$$

$$p = 1461501637330902918203684832716283019651637554291$$

$$N_p = 1461501637330902918203686915170869725397159163571$$

Hasse-Weil bound

An elliptic curve E over $\mathbb{F}_p$ satisfies

$$N_p = \#E(\mathbb{F}_p) = p + 1 - a_p$$

with $\quad |a_p| < 2\sqrt{p}$.

Elliptic curves over $\mathbb{Q}$

Mordell's theorem

One can obtain all $E(\mathbb{Q})$ from a finite set of points.

Elliptic curves over $\mathbb{Q}$

Mordell's theorem

One can obtain all $E(\mathbb{Q})$ from a finite set of points.

Mordell-Weil theorem

An elliptic curve E over $\mathbb{Q}$ then $E(K) = \text{(finite)} \times \mathbb{Z}^r$.

- The finite torsion group is easy to determine.

Elliptic curves over $\mathbb{Q}$

Mordell's theorem

One can obtain all $E(\mathbb{Q})$ from a finite set of points.

Mordell-Weil theorem

An elliptic curve E over $\mathbb{Q}$ then $E(K) =$ (finite) $\times \mathbb{Z}^r$.

- The finite torsion group is easy to determine.
- The rank r of $E(K)$ is difficult, but often small.

Elliptic curves over $\mathbb{Q}$

Mordell's theorem

One can obtain all $E(\mathbb{Q})$ from a finite set of points.

Mordell-Weil theorem

An elliptic curve E over $\mathbb{Q}$ then $E(K) =$ (finite) $\times \mathbb{Z}^r$.

- The finite torsion group is easy to determine.
- The rank r of $E(K)$ is difficult, but often small.
- E_2 has rank 0 and $E_2(\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}\,(1,2)$, while

Elliptic curves over $\mathbb{Q}$

Mordell's theorem

One can obtain all $E(\mathbb{Q})$ from a finite set of points.

Mordell-Weil theorem

An elliptic curve E over $\mathbb{Q}$ then $E(K) =$ (finite) $\times \mathbb{Z}^r$.

- The finite torsion group is easy to determine.
- The rank r of $E(K)$ is difficult, but often small.
- E_2 has rank 0 and $E_2(\mathbb{Q}) = {}^{\mathbb{Z}}/_{4\mathbb{Z}}\,(1,2)$, while
- E_1 has rank 1 and $E_1(\mathbb{Q}) = \mathbb{Z}\,(0,1)$.

Elliptic curves over $\mathbb{Q}$

Mordell's theorem

One can obtain all $E(\mathbb{Q})$ from a finite set of points.

Mordell-Weil theorem

An elliptic curve E over $\mathbb{Q}$ then $E(K) =$ (finite) $\times \mathbb{Z}^r$.

- The finite torsion group is easy to determine.
- The rank r of $E(K)$ is difficult, but often small.
- E_2 has rank 0 and $E_2(\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}\,(1,2)$, while
- E_1 has rank 1 and $E_1(\mathbb{Q}) = \mathbb{Z}\,(0,1)$.
- E_{101} has rank 2 and $E_1(\mathbb{Q}) = \mathbb{Z}\,(4,13) \times \mathbb{Z}(-\frac{20}{9}, \frac{253}{27})$.

Bryan Birch and Sir Peter Swinnerton-Dyer

Let E be an elliptic curve over $\mathbb{Q}$ with $A, B \in \mathbb{Z}$.

Let E be an elliptic curve over $\mathbb{Q}$ with $A, B \in \mathbb{Z}$.
Let N_p be the number of solutions of E modulo p.

Let E be an elliptic curve over $\mathbb{Q}$ with $A, B \in \mathbb{Z}$.
Let N_p be the number of solutions of E modulo p.
Consider the function

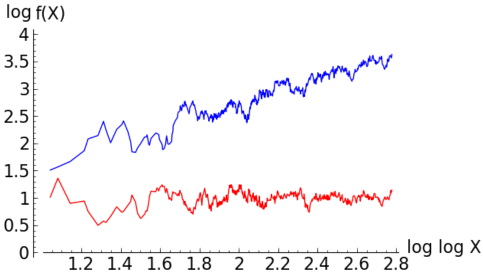
$$f(X) = \prod_{\text{primes } p \leqslant X} \frac{N_p}{p}$$

Let E be an elliptic curve over $\mathbb{Q}$ with $A, B \in \mathbb{Z}$.
Let N_p be the number of solutions of E modulo p.
Consider the function

$$f(X) = \prod_{\text{primes } p \leqslant X} \frac{N_p}{p}$$

Conjecture

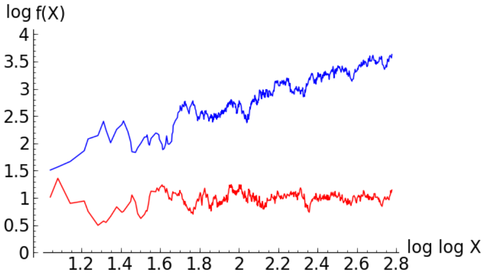
$f(X)$ stays bounded if and only if there are only finitely many solutions in $\mathbb{Q}$.



$E_1 : y^2 = x^3 + x + 1.$
$E_2 : y^2 = x^3 + x + 2.$

Conjecture

$f(X)$ grows like $\log(X)^r$, where r is the rank of $E(\mathbb{Q})$.

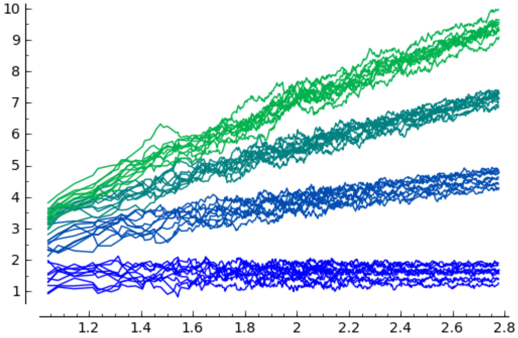


$E_1 : y^2 = x^3 + x + 1.$

$E_2 : y^2 = x^3 + x + 2.$

Conjecture

$f(X)$ grows like $\log(X)^r$, where r is the rank of $E(\mathbb{Q})$.

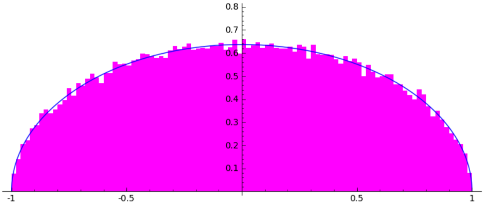


Sato-Tate by Taylor et al.

If E does not admit complex multiplication, then the values of $a_p/(2\sqrt{p}) \in [-1, 1]$ are distributed like $\frac{2}{\pi}\sqrt{1 - t^2}dt$.

Sato-Tate by Taylor et al.

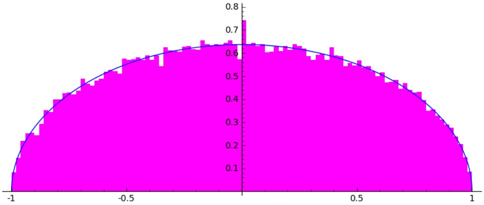
If E does not admit complex multiplication, then the values of $a_p/(2\sqrt{p}) \in [-1,1]$ are distributed like $\frac{2}{\pi}\sqrt{1-t^2}dt$.



Sato-Tate for E_1

Sato-Tate by Taylor et al.

If E does not admit complex multiplication, then the values of $a_p/(2\sqrt{p}) \in [-1, 1]$ are distributed like $\frac{2}{\pi}\sqrt{1-t^2}dt$.



Sato-Tate for E_2

The L-series

Define

$$L(E,s) = \prod_{p \text{ good}} \frac{1}{1 - a_p \cdot p^{-s} + p \cdot p^{-2s}} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

for $\mathrm{Re}(s) > \frac{3}{2}$.

The L-series

Define

$$L(E,s) = \prod_{p \text{ good}} \frac{1}{1 - a_p \cdot p^{-s} + p \cdot p^{-2s}} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

for $\mathrm{Re}(s) > \frac{3}{2}$. Note

$$\text{“ } L(E,1) = \prod_p \frac{p}{N_p} = \frac{1}{f(\infty)} \text{ ”.}$$

The L-series

Define

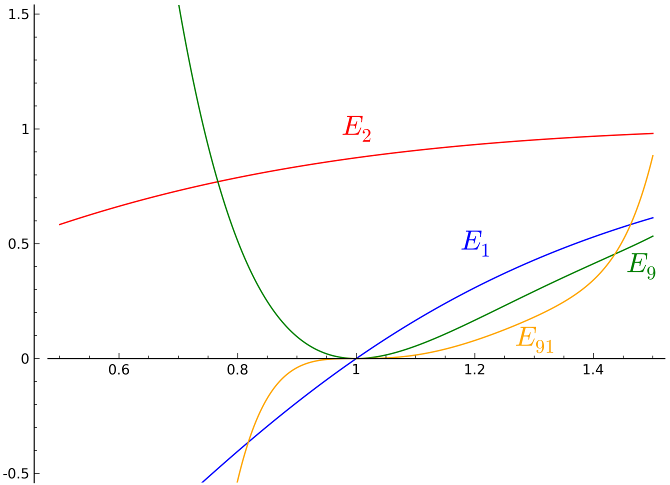
$$L(E,s) = \prod_{p \text{ good}} \frac{1}{1 - a_p \cdot p^{-s} + p \cdot p^{-2s}} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

for $\mathrm{Re}(s) > \frac{3}{2}$. Note

$$\text{“ } L(E,1) = \prod_{p} \frac{p}{N_p} = \frac{1}{f(\infty)} \text{ ”.}$$

Weak Birch and Swinnerton-Dyer conjecture 1000000$

The function $L(E,s)$ has a zero of order r, the rank of $E(\mathbb{Q})$, at $s = 1$.


1.5
1
0.5
0
-0.5
0.6
0.8
1
1.2
1.4
E_2
E_1
E_9
E_{91}

Results

Taylor-Wiles et al.

If $E/\mathbb{Q}$, then $L(E,s)$ has an analytic continuation to $\mathbb{C}$.
In fact, $L(E,s) = L(f,s)$ for a modular form f.

Results

Taylor-Wiles et al.

If $E/\mathbb{Q}$, then $L(E,s)$ has an analytic continuation to $\mathbb{C}$.
In fact, $L(E,s) = L(f,s)$ for a modular form f.

Coates-Wiles, Gross-Zagier-Kolyvagin

If $r_{\text{an}} = \operatorname{ord}_{s=1} L(E,s) \leqslant 1$, then $r_{\text{an}} = r$.

The conjecture also predicts the leading term

$$L(E,s) = L^*(E) \cdot (s-1)^r + \cdots$$

in analogy to the class number formula.

The conjecture also predicts the leading term

$$L(E,s) = L^*(E)\cdot(s-1)^r + \cdots$$

in analogy to the class number formula.

Birch and Swinnerton-Dyer conjecture

$$L^*(E) = \frac{\prod_p c_p \cdot \Omega \cdot \mathrm{Reg}(E/\mathbb{Q}) \cdot \#Ш(E/\mathbb{Q})}{\left(\#E(\mathbb{Q})_{\text{tors}}\right)^2}$$

Birch and Swinnerton-Dyer conjecture

$$\frac{L^*(E)}{\Omega \cdot \mathrm{Reg}(E/\mathbb{Q})} = \frac{\prod_p c_p \cdot \#Ш(E/\mathbb{Q})}{\left(\#E(\mathbb{Q})_{\text{tors}}\right)^2}$$

Birch and Swinnerton-Dyer conjecture

$$\frac{L^*(E)}{\Omega \cdot \mathrm{Reg}(E/\mathbb{Q})} = \frac{\prod_p c_p \cdot \#Ш(E/\mathbb{Q})}{\left(\#E(\mathbb{Q})_{\text{tors}}\right)^2}$$

- $\Omega \in \mathbb{R}$ is a period.

Birch and Swinnerton-Dyer conjecture

$$\frac{L^*(E)}{\Omega \cdot \mathrm{Reg}(E/\mathbb{Q})} = \frac{\prod_p c_p \cdot \#Ш(E/\mathbb{Q})}{\left(\#E(\mathbb{Q})_{\text{tors}}\right)^2}$$

- $\Omega \in \mathbb{R}$ is a period.
- $\mathrm{Reg}(E/\mathbb{Q}) \in \mathbb{R}$ is the regulator.

Birch and Swinnerton-Dyer conjecture

$$\frac{L^*(E)}{\Omega \cdot \mathrm{Reg}(E/\mathbb{Q})} = \frac{\prod_p c_p \cdot \#Ш(E/\mathbb{Q})}{\left(\#E(\mathbb{Q})_{\text{tors}}\right)^2}$$

- $\Omega \in \mathbb{R}$ is a period.
- $\mathrm{Reg}(E/\mathbb{Q}) \in \mathbb{R}$ is the regulator.
- $c_p \in \mathbb{Z}$ is a Tamagawa number.

Birch and Swinnerton-Dyer conjecture

$$\frac{L^*(E)}{\Omega \cdot \mathrm{Reg}(E/\mathbb{Q})} = \frac{\prod_p c_p \cdot \#Ш(E/\mathbb{Q})}{\left(\#E(\mathbb{Q})_{\text{tors}}\right)^2}$$

- $\Omega \in \mathbb{R}$ is a period.
- $\mathrm{Reg}(E/\mathbb{Q}) \in \mathbb{R}$ is the regulator.
- $c_p \in \mathbb{Z}$ is a Tamagawa number.
- $Ш(E/\mathbb{Q})$ is the mysterious Tate-Shafarevich group.

The Tate-Shafarevich group

$$Ш(E/K) = \ker\left(H^1(K,E) \to \prod_v H^1(K_v,E)\right)$$

- $Ш(E/K)$ is an abelian torsion group.

The Tate-Shafarevich group

$$Ш(E/K) = \ker\left(H^1(K,E) \to \prod_v H^1(K_v,E) \right)$$

- $Ш(E/K)$ is an abelian torsion group.
- It is believed to be finite.

The Tate-Shafarevich group

$$Ш(E/K) = \ker\left(H^1(K,E) \to \prod_v H^1(K_v,E)\right)$$

- $Ш(E/K)$ is an abelian torsion group.
- It is believed to be finite.
- It is known to be finite for $\mathbb{Q}$ if and only if $r_{\text{an}} \leqslant 1$.

The Tate-Shafarevich group

$$Ш(E/K) = \ker\Big(H^1(K,E) \to \prod_v H^1(K_v,E) \Big)$$

- $Ш(E/K)$ is an abelian torsion group.
- It is believed to be finite.
- It is known to be finite for $\mathbb{Q}$ if and only if $r_{\text{an}} \leqslant 1$.
- If it is then the parity $r_{\text{an}} \equiv r \pmod{2}$ holds.

$$\frac{L^*(E)}{\Omega \cdot \mathrm{Reg}(E/\mathbb{Q})} = \frac{\prod_p c_p \cdot \#\text{Ш}(E/\mathbb{Q})}{\left(\#E(\mathbb{Q})_{\text{tors}}\right)^2}$$

$$E_2 \; : \; y^2 \; = \; x^3 \; + \; x \; + \; 2, \qquad r_{\text{an}} = r = 0$$

- $L(E,1) \cong 0.874549$
- $\Omega \cong 3.49819$
- $\mathrm{Reg}(E/\mathbb{Q}) = 1$
- $L(E,1)/\Omega \cong 0.250000$.
- In fact $L(E,1)/\Omega = \frac{1}{4}$.

- $c_2 = 4$ and $c_p = 1 \, \forall_{p \neq 2}$.
- $\#E(\mathbb{Q}) = 4$
- $\text{Ш}(E/\mathbb{Q})$ is trivial.

$$\frac{L^*(E)}{\Omega \cdot \mathrm{Reg}(E/\mathbb{Q})} = \frac{\prod_p c_p \cdot \#\text{Ш}(E/\mathbb{Q})}{\left(\#E(\mathbb{Q})_{\text{tors}}\right)^2}$$

$$E_2 \; : \; y^2 \; = \; x^3 \; + \; x \; + \; 2, \qquad r_{\text{an}} = r = 1$$

- $L'(E,1) \cong 1.78581$
- $\Omega \cong 3.74994$
- $\mathrm{Reg}(E/\mathbb{Q}) \cong 0.476223$
- $\mathrm{LHS} \cong 1.00000$.
- In fact it is 1.

- $c_p = 1$.
- $E(\mathbb{Q}) = \mathbb{Z}$
- $\text{Ш}(E/\mathbb{Q})$ is trivial.

$$\frac{L^*(E)}{\Omega \cdot \operatorname{Reg}(E/\mathbb{Q})} = \frac{\prod_p c_p \cdot \#Ш(E/\mathbb{Q})}{\left(\#E(\mathbb{Q})_{\text{tors}}\right)^2}$$

$$E_9 \,:\, y^2 = x^3 + x + 101, \qquad r_{\text{an}} = r = 2$$

- $L^*(E) \cong 16.37120$
- $\Omega \cong 1.94006$
- $\operatorname{Reg}(E/\mathbb{Q}) \cong 8.43852$
- LHS $\cong 1.00000$.
- $c_p = 1$.
- $E(\mathbb{Q}) = \mathbb{Z}^2$
- $Ш(E/\mathbb{Q})$ should be trivial.

Generalisations

- for higher genus curves
- for abelian varieties
- for general motives (Bloch-Kato conjectures)
- p-adic versions
- equivariant version

p-adic version

Let $E/\mathbb{Q}$ be an elliptic curve and p a good prime with $p \nmid a_p$.

p-adic version

Let $E/\mathbb{Q}$ be an elliptic curve and p a good prime with $p \nmid a_p$. There is a p-adic L-series $L_p(E,s) \in \mathbb{Z}_p$ for $s \in \mathbb{Z}_p$ such that $L_p(E,1) = L(E,1)/\Omega$.

p-adic version

Let $E/\mathbb{Q}$ be an elliptic curve and p a good prime with $p \nmid a_p$. There is a p-adic L-series $L_p(E,s) \in \mathbb{Z}_p$ for $s \in \mathbb{Z}_p$ such that $L_p(E,1) = L(E,1)/\Omega$.

p-adic Birch and Swinnerton-Dyer conjecture

$\operatorname{ord}_{s=1} L_p(E,s) = \operatorname{rank}(E)$ and there is a formula for the leading term.

p-adic version

Let $E/\mathbb{Q}$ be an elliptic curve and p a good prime with $p \nmid a_p$. There is a p-adic L-series $L_p(E,s) \in \mathbb{Z}_p$ for $s \in \mathbb{Z}_p$ such that $L_p(E,1) = L(E,1)/\Omega$.

p-adic Birch and Swinnerton-Dyer conjecture

$\operatorname{ord}_{s=1} L_p(E,s) = \operatorname{rank}(E)$ and there is a formula for the leading term.

Kato's Euler system

We have $\operatorname{ord}_{s=1} L_p(E,s) \geqslant \operatorname{rank}(E)$.

p-adic Birch and Swinnerton-Dyer conjecture

$\operatorname{ord}_{s=1} L_p(E,s) = \operatorname{rank}(E)$ and there is a formula for the leading term.

p-adic Birch and Swinnerton-Dyer conjecture

$\mathrm{ord}_{s=1} L_p(E,s) = \mathrm{rank}(E)$ and there is a formula for the leading term.

Theorem

If $E/\mathbb{Q}$ is semistable and $L(E,1) \neq 0$, then BSD holds up to a power of 2.

p-adic Birch and Swinnerton-Dyer conjecture

$\mathrm{ord}_{s=1} L_p(E,s) = \mathrm{rank}(E)$ and there is a formula for the leading term.

Theorem

If $E/\mathbb{Q}$ is semistable and $L(E,1) \neq 0$, then BSD holds up to a power of 2.

Shark

Given p, we have an algorithm giving an upper bound on r and the order of the p-primary part of $\text{Ш}(E/\mathbb{Q})$.

We can show that $\text{Ш}(E_{101}/\mathbb{Q})$ has no 5-torsion.