The Birch and Swinnerton-Dyer conjecture

Christian Wuthrich

17 Jan 2012

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

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

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

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

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

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

  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

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

  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 ?

Question

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

Question

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

Example

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

.

Question

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

Example

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

.

Question

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

Example

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

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

.

Question

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

Example

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

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

$$-\frac{287}{1296}, \quad \frac{43992}{82369}, \quad \frac{26862913}{1493284}, \quad \frac{139455877527}{1824793048}, \quad -\frac{3596697936}{8760772801},$$
$$\frac{7549090222465}{8662944250944}, \quad \frac{51865013741670864}{6504992707996225}, \quad -\frac{173161424238594532415}{3105156367744812388 84}, \quad \ldots$$

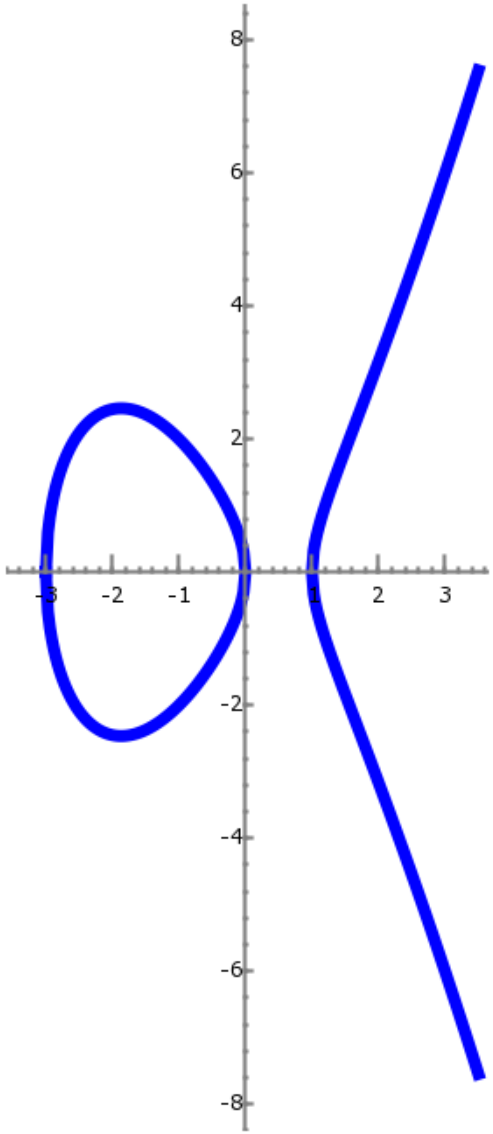
.

Addition on elliptic curves

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

Addition on elliptic curves

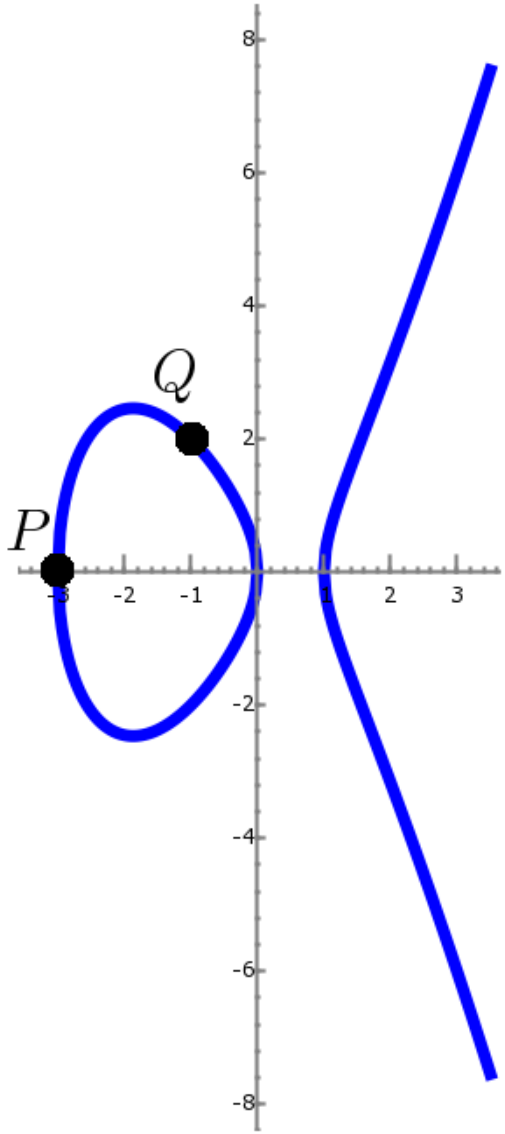
$$E: \quad y^2 = x^3 + Ax + B$$



Addition on elliptic curves

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

Any two points P and Q on E

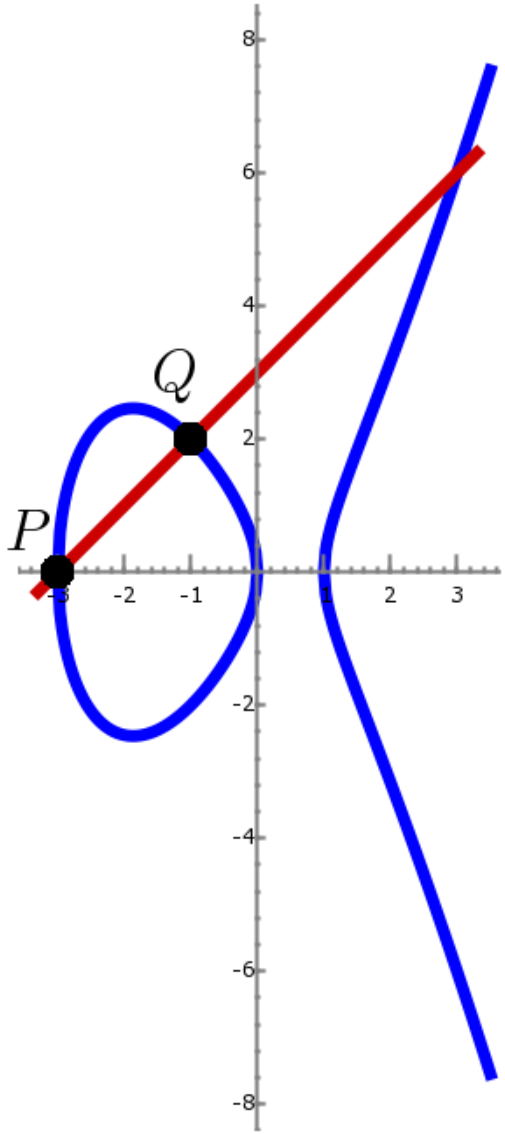


Addition on elliptic curves

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

Any two points P and Q on E

are linked by a line



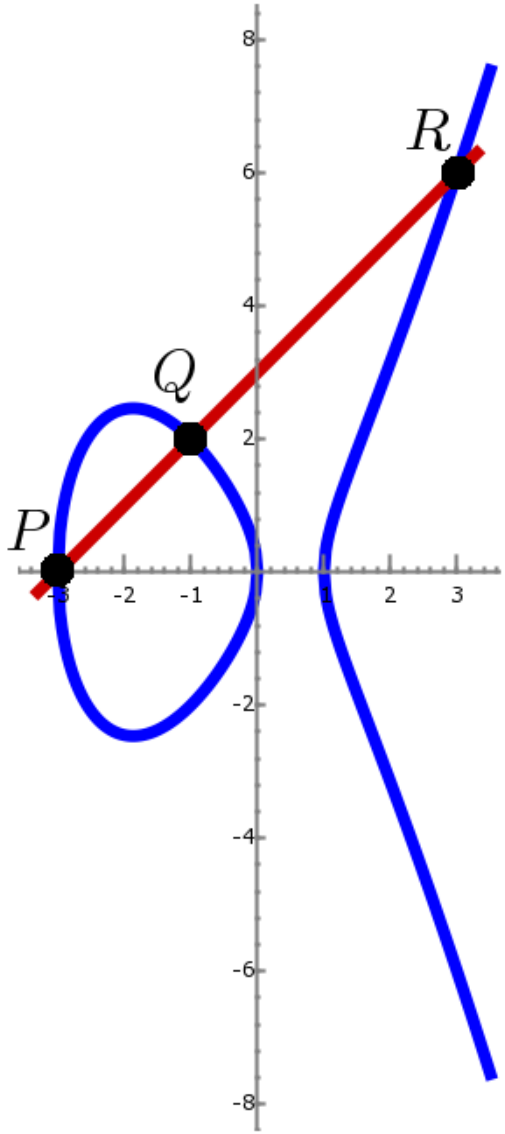
Addition on elliptic curves

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

Any two points P and Q on E

are linked by a line

intersecting the curve in a third point $R = (x, y)$.



Addition on elliptic curves

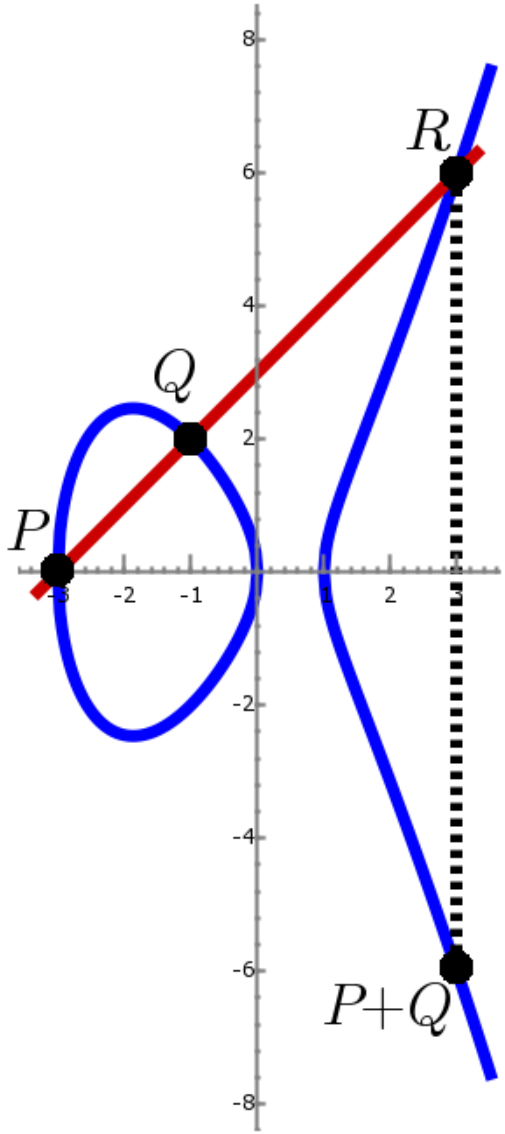
$E: \quad y^2 = x^3 + Ax + B$

Any two points P and Q on E

are linked by a line

intersecting the curve in a third point $R = (x, y)$.

Set $P + Q = (x, -y)$.



Addition on elliptic curves

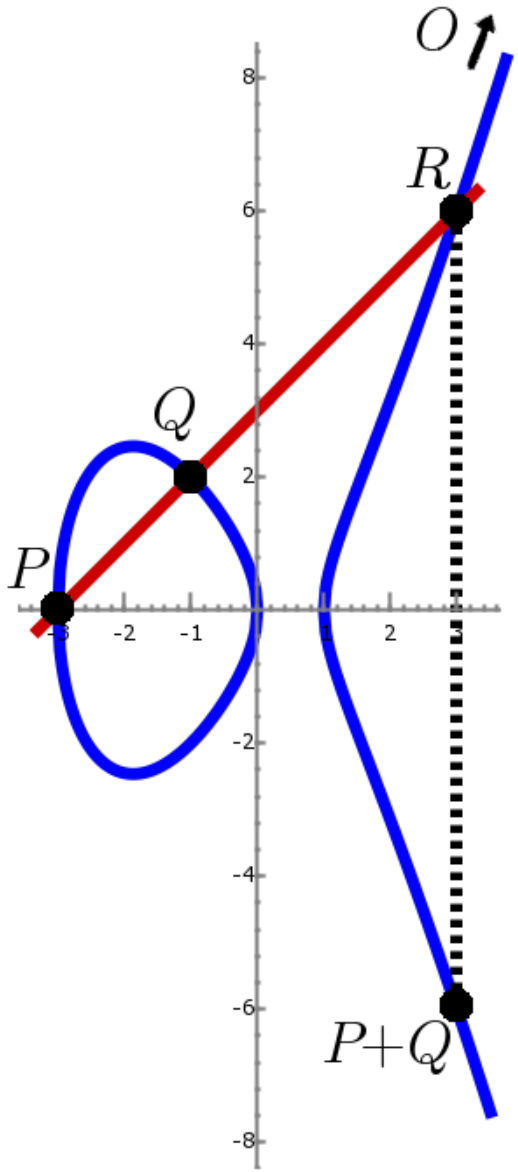
$E: \quad y^2 = x^3 + Ax + B$

Any two points P and Q on E

are linked by a line

intersecting the curve in a third point $R = (x, y)$.

Set $P + Q = (x, -y)$.



Elliptic curves over finite fields

Hasse-Weil bound

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

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

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

Elliptic curves over finite fields

Hasse-Weil bound

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

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

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

Curve sepc160k1

$$E: \ y^2 = x^3 + 7 \qquad \text{with}$$

$$p = 1461501637330902918203684832716283019651637554291$$

$$N_p = 1461501637330902918203686915170869725397159163571$$

Elliptic curves over number fields

Mordell-Weil theorem

An elliptic curve E over a number field K then $E(K)$ is a finitely generated abelian group.

Elliptic curves over number fields

Mordell-Weil theorem

An elliptic curve E over a number field K then $E(K)$ is a finitely generated abelian group.

- The finite torsion group is easy to determine.

Elliptic curves over number fields

Mordell-Weil theorem

An elliptic curve E over a number field K then $E(K)$ is a finitely generated abelian group.

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

Elliptic curves over number fields

Mordell-Weil theorem

An elliptic curve E over a number field K then $E(K)$ is a finitely generated abelian group.

- 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 number fields

Mordell-Weil theorem

An elliptic curve E over a number field K then $E(K)$ is a finitely generated abelian group.

- 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 $E_1(\mathbb{Q}) = \mathbb{Z}\,(0,1)$.

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

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

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

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

Conjecture

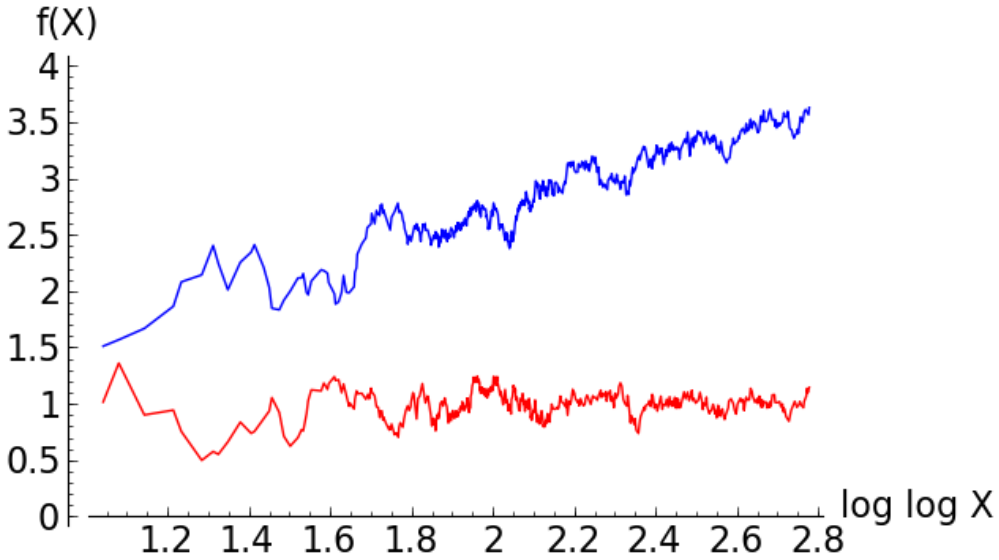
$f(X)$ stays bounded if and only if there are only finitely many solutions in $\mathbb{Q}$.

Conjecture

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

Conjecture

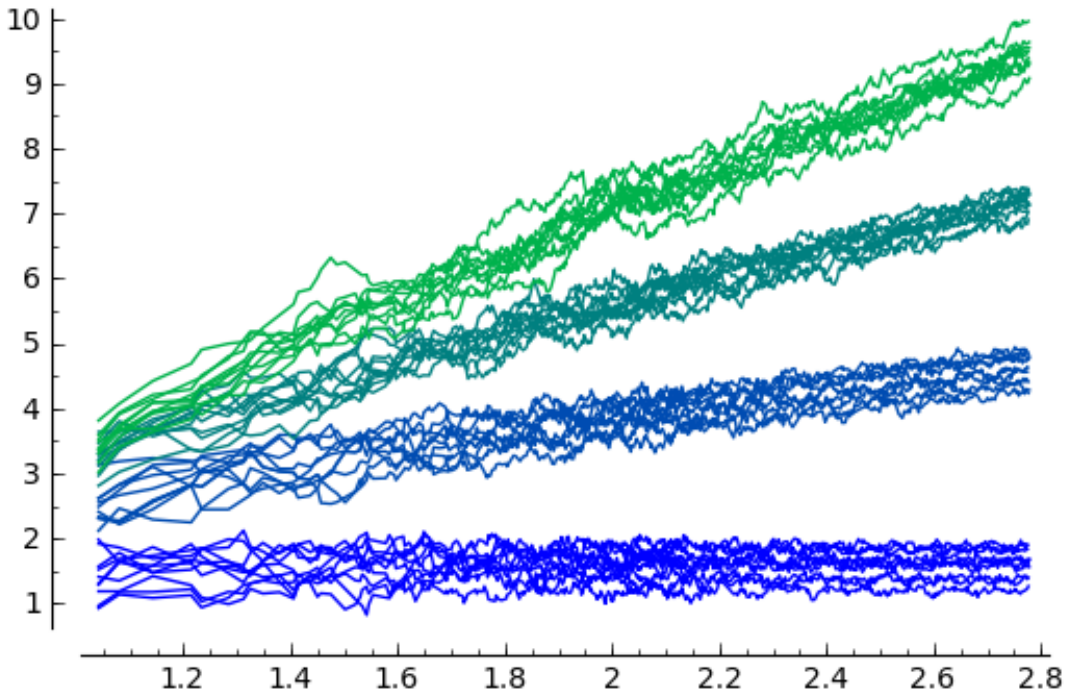
$f(X)$ grows like $r \cdot \log(\log(X))$, where r is the rank of $E(\mathbb{Q})$.



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

Conjecture

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



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

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

The L-series

Define

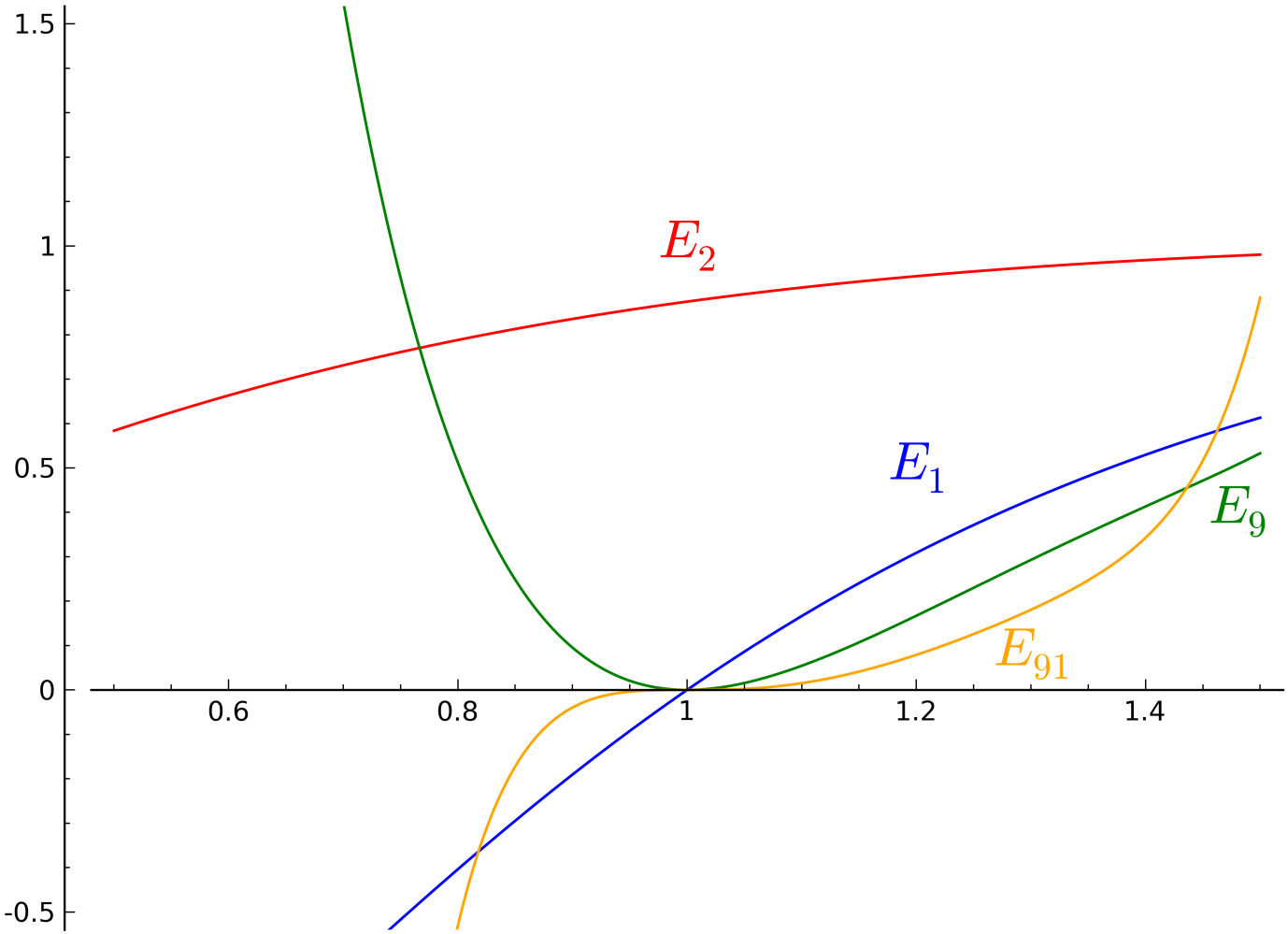
$$L(E,s) = \prod_{p \text{ good}} \frac{1}{1 - a_p \cdot p^{-s} + p \cdot p^{-2s}} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

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

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

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

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

If $r_{\text{an}} = 1$, a Heegner point can be constructed from 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 $r_{\text{an}} = \text{ord}_{s=1} L(E,s) \leqslant 1$, then $r_{\text{an}} = r$.

If $r_{\text{an}} = 1$, a Heegner point can be constructed from f.
If $r_{\text{an}} > 1$, ???

Let E be an elliptic curve over a number field K. Define

$$L(E/K,s) = \prod_v \frac{1}{1 - a_v q_v^s + q_v^{1-2s}},$$

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

Let E be an elliptic curve over a number field K. Define

$$L(E/K,s) = \prod_v \det\left(1 - \mathrm{Frob}_v\, q_v^{-s} \,\middle|\, V_\ell E^{I_v}\right)^{-1},$$

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

Let E be an elliptic curve over a number field K. Define

$$L(E/K,s) = \prod_v \det\left(1 - \mathrm{Frob}_v\, q_v^{-s} \,\middle|\, V_\ell E^{I_v}\right)^{-1},$$

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

Weak Birch and Swinnerton-Dyer conjecture

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

Let E be an elliptic curve over a number field K. Define

$$L(E/K,s) = \prod_v \det\left(1 - \mathrm{Frob}_v\, q_v^{-s} \,\middle|\, V_\ell E^{I_v}\right)^{-1},$$

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

Weak Birch and Swinnerton-Dyer conjecture

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

Tate

If K is the function field of a curve over a finite field, e.g. $K = \mathbb{F}_p(T)$, then $\mathrm{ord}_{s=1} L(E/K,s) \geqslant \mathrm{rank}\, E(K)$.

Let E be an elliptic curve over a number field K. Define

$$L(E/K,s) = \prod_v \det\left(1 - \mathrm{Frob}_v\, q_v^{-s} \,\middle|\, V_\ell E^{I_v}\right)^{-1},$$

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

Weak Birch and Swinnerton-Dyer conjecture

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

Tate

If K is the function field of a curve over a finite field, e.g. $K = \mathbb{F}_p(T)$, then $\mathrm{ord}_{s=1} L(E/K,s) \geqslant \mathrm{rank}\, E(K)$.

Nekovář, T&V Dokchitser

If . . . , then $\mathrm{ord}_{s=1} L(E/K,s) \equiv \mathrm{rank}\, E(K) \pmod 2$

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

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

Birch and Swinnerton-Dyer conjecture

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

Birch and Swinnerton-Dyer conjecture

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

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

Birch and Swinnerton-Dyer conjecture

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

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

Birch and Swinnerton-Dyer conjecture

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

- $\Omega \in \mathbb{R}$ 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

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

- $\Omega \in \mathbb{R}$ 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.
- If it is then the parity $r_{\text{an}} \equiv r \pmod 2$ holds.

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.
- If it is then the parity $r_{\text{an}} \equiv r \pmod 2$ holds.
- If it is for a function field K then BSD is true for K.

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.
- If it is then the parity $r_{\text{an}} \equiv r \pmod 2$ holds.
- If it is for a function field K then BSD is true for K.
- It is known to be finite for $\mathbb{Q}$ if and only if $r_{\text{an}} \leqslant 1$.

Birch and Swinnerton-Dyer conjecture

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

Birch and Swinnerton-Dyer conjecture

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

- If $L(E,1) \neq 0$, then $L(E,1)/\Omega \in \mathbb{Q}$. (Winding number)

Birch and Swinnerton-Dyer conjecture

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

- If $L(E,1) \neq 0$, then $L(E,1)/\Omega \in \mathbb{Q}$. (Winding number)
- It is invariant under morphisms $E \to E'$ over $\mathbb{Q}$.

Birch and Swinnerton-Dyer conjecture

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

- If $L(E,1) \neq 0$, then $L(E,1)/\Omega \in \mathbb{Q}$. (Winding number)
- It is invariant under morphisms $E \to E'$ over $\mathbb{Q}$.
- If $r_{\mathrm{an}} \leqslant 1$, the group $Ш(E/\mathbb{Q})$ is finite and the conjecture can be proven `sage: E.prove_bsd()`.

Birch and Swinnerton-Dyer conjecture

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

- If $L(E,1) \neq 0$, then $L(E,1)/\Omega \in \mathbb{Q}$. (Winding number)
- It is invariant under morphisms $E \to E'$ over $\mathbb{Q}$.
- If $r_{\mathrm{an}} \leqslant 1$, the group $Ш(E/\mathbb{Q})$ is finite and the conjecture can be proven `sage: E.prove_bsd()`.
- Lots of numerical evidence for $r_{\mathrm{an}} \geqslant 2$.

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

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

- $L(E,1) \cong 0.874549$
- $\Omega \cong 3.49819$
- $\mathrm{Reg}(E/\mathbb{Q}) = 1$
- $L(E,1)/\Omega \cong 0.250000.$
- In fact $L(E,1)/\Omega = \frac{1}{4}$.
- $c_2 = 4$ and $c_p = 1 \, \forall_{p \neq 2}$.
- $\#E(\mathbb{Q}) = 4$
- $Ш(E/\mathbb{Q})$ is trivial.

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

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

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

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

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

$$E_9 \ : \ y^2 \ = \ x^3 \ + \ x \ + \ 9, \qquad r_{\mathrm{an}} = r = 2$$

- $L^*(E) \cong 7.16561$
- $\Omega \cong 2.84721$
- $\mathrm{Reg}(E/\mathbb{Q}) \cong 2.51672$
- $\mathrm{LHS} \cong 1.00000.$
- $c_p = 1.$
- $E(\mathbb{Q}) = \mathbb{Z}^2$
- $Ш(E/\mathbb{Q})$ should be trivial.

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

$$E_{-47} \ : \ y^2 \ = \ x^3 \ + \ x \ - \ 47, \qquad r_{\mathsf{an}} = r = 0$$

- $L(E,1) \cong 5.15400$
- $\Omega \cong 1.28850$
- $\mathrm{Reg}(E/\mathbb{Q}) = 1$
- $L(E,1)/\Omega = 4.$

- $c_p = 1$
- $E(\mathbb{Q}) = 0$
- $Ш(E/\mathbb{Q}) = {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \oplus {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}.$

Generalisations

- for abelian varieties

Generalisations

- for abelian varieties
- for general motives (Bloch-Kato conjectures)

Generalisations

- for abelian varieties
- for general motives (Bloch-Kato conjectures)
- p-adic versions

Generalisations

- 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 such that $p \nmid a_p$.

p-adic version

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

p-adic version

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

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.

p-adic version

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

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.

Kato's Euler system

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

p-adic version

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

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.

Kato's Euler system

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

Recent work of Skinner-Urban: If $Ш(E/\mathbb{Q})$ is finite and $\mathrm{Reg}_p(E/\mathbb{Q}) \neq 0$, then the p-adic BSD holds.

Equivariant version

Let $K/\mathbb{Q}$ be a finite Galois extension of group G.

Equivariant version

Let $K/\mathbb{Q}$ be a finite Galois extension of group G.
Artin formalisms gives

$$L(E/K,s) = \prod_{\rho \in \mathrm{Irr}(G)} L(E,\rho,s)^{\dim(\rho)}.$$

Equivariant version

Let $K/\mathbb{Q}$ be a finite Galois extension of group G.
Artin formalisms gives

$$L(E/K,s) = \prod_{\rho \in \mathrm{Irr}(G)} L(E,\rho,s)^{\dim(\rho)}.$$

Similar $E(K) \otimes \mathbb{C} = \bigoplus \rho^{r_\rho}$.

Equivariant version

Let $K/\mathbb{Q}$ be a finite Galois extension of group G.
Artin formalisms gives

$$L(E/K,s) = \prod_{\rho \in \mathrm{Irr}(G)} L(E,\rho,s)^{\dim(\rho)}.$$

Similar $E(K) \otimes \mathbb{C} = \bigoplus \rho^{r_\rho}$.

Equivariant Birch and Swinnerton-Dyer conjecture

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

Equivariant version

Let $K/\mathbb{Q}$ be a finite Galois extension of group G.
Artin formalisms gives

$$L(E/K,s) = \prod_{\rho \in \mathrm{Irr}(G)} L(E,\rho,s)^{\dim(\rho)}.$$

Similar $E(K) \otimes \mathbb{C} = \bigoplus \rho^{r_\rho}$.

Equivariant Birch and Swinnerton-Dyer conjecture

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

Often there is a formula for the leading term involving the $\mathbb{Z}[G]$-structure of $Ш(E/K)$.