Numerical evidence for the Birch–Swinnerton-Dyer conjecture

John Cremona

University of Warwick

BSD conference, Cambridge
4 May 2011

Plan

1. Introduction and statement of the Birch–Swinnerton-Dyer (BSD) conjectures for elliptic curves over $\mathbb{Q}$
2. Numerical evidence and examples

Plan

1. Introduction and statement of the Birch–Swinnerton-Dyer (BSD) conjectures for elliptic curves over $\mathbb{Q}$
2. Numerical evidence[1] and examples

[1] "Should be a short talk then" RH-B

Introduction

- I will not talk about the history of the conjecture, leaving that to the afternoon's distinguished speakers!

Introduction

- I will not talk about the history of the conjecture, leaving that to the afternoon's distinguished speakers!
- To set the scene for the rest of the conference, I will first explain in some detail exactly what the BSD conjectures state, for elliptic curves defined over $\mathbb{Q}$, distinguishing between the First (or "weak") and the Second (or "strong") Conjectures.

Introduction

- I will not talk about the history of the conjecture, leaving that to the afternoon's distinguished speakers!
- To set the scene for the rest of the conference, I will first explain in some detail exactly what the BSD conjectures state, for elliptic curves defined over $\mathbb{Q}$, distinguishing between the First (or "weak") and the Second (or "strong") Conjectures.
- In the second part of the talk, I will discuss how the conjectures might be verified for individual curves, or for families of curves, using both theoretical and computational methods.

Introduction

- I will not talk about the history of the conjecture, leaving that to the afternoon's distinguished speakers!
- To set the scene for the rest of the conference, I will first explain in some detail exactly what the BSD conjectures state, for elliptic curves defined over $\mathbb{Q}$, distinguishing between the First (or "weak") and the Second (or "strong") Conjectures.
- In the second part of the talk, I will discuss how the conjectures might be verified for individual curves, or for families of curves, using both theoretical and computational methods.
- Conclusions:
  1. The full BSD conjecture is proved for many elliptic curves, all of rank 0 or 1 and all but a finite number with CM.
  2. For elliptic curves of higher rank, even numerical verification is impossible for the strong conjecture.
  3. Nevertheless the numbers are compelling!

Elliptic curves

- An *elliptic curve* defined over the field K is
  - a smooth projective curve E, of genus 1, defined over K, together with
  - a K-rational point, $\mathcal{O}_E$.

Elliptic curves

- An *elliptic curve* defined over the field K is
  - a smooth projective curve E, of genus 1, defined over K, together with
  - a K-rational point, $\mathcal{O}_E$.
- Elliptic curves all have smooth plane cubic models which are the projective completion of affine curves defined by *Weierstrass Equations*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_1, \ldots, a_6 \in K$ satisfying $\Delta_E = \Delta(a_1, a_2, a_3, a_4, a_6) \neq 0$.

Elliptic curves

- An *elliptic curve* defined over the field K is
  - a smooth projective curve E, of genus 1, defined over K, together with
  - a K-rational point, $\mathcal{O}_E$.
- Elliptic curves all have smooth plane cubic models which are the projective completion of affine curves defined by *Weierstrass Equations*

  $$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

  with $a_1, \ldots, a_6 \in K$ satisfying $\Delta_E = \Delta(a_1, a_2, a_3, a_4, a_6) \neq 0$.
- The distinguished point $\mathcal{O}_E$ is the (unique) point $[0 : 1 : 0]$ at infinity on this model.

Elliptic curves

- An *elliptic curve* defined over the field K is
  - a smooth projective curve E, of genus 1, defined over K, together with
  - a K-rational point, $\mathcal{O}_E$.
- Elliptic curves all have smooth plane cubic models which are the projective completion of affine curves defined by *Weierstrass Equations*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

  with $a_1, \ldots, a_6 \in K$ satisfying $\Delta_E = \Delta(a_1, a_2, a_3, a_4, a_6) \neq 0$.
- The distinguished point $\mathcal{O}_E$ is the (unique) point $[0 : 1 : 0]$ at infinity on this model.
- For short we denote the above equation by $[a_1, a_2, a_3, a_4, a_6]$.

The group of points of an elliptic curve

- Let E/K be an elliptic curve. For any field $L \supseteq K$ the set of L-rational points, $E(L)$, has the structure of an *Abelian group* with identity $\mathcal{O}_E$.

The group of points of an elliptic curve

- Let E/K be an elliptic curve. For any field $L \supseteq K$ the set of L-rational points, $E(L)$, has the structure of an *Abelian group* with identity $\mathcal{O}_E$.
- In the Weierstrass model, the group law is defined by the classical tangent-chord method; three points P, Q, R add to $\mathcal{O}_E$ if and only if they are the three intersection points of E with a (projective) line, counting multiplicities.

The group of points of an elliptic curve

- Let E/K be an elliptic curve. For any field $L \supseteq K$ the set of L-rational points, $E(L)$, has the structure of an *Abelian group* with identity $\mathcal{O}_E$.
- In the Weierstrass model, the group law is defined by the classical tangent-chord method; three points P, Q, R add to $\mathcal{O}_E$ if and only if they are the three intersection points of E with a (projective) line, counting multiplicities.
- Some basic questions are:
  1. what kind of a group is $E(K)$?
  2. how does $E(K)$ vary (for fixed K)?
  3. can we determine $E(K)$ (for given E)?

The group of points of an elliptic curve

- Let E/K be an elliptic curve. For any field $L \supseteq K$ the set of L-rational points, $E(L)$, has the structure of an *Abelian group* with identity $\mathcal{O}_E$.
- In the Weierstrass model, the group law is defined by the classical tangent-chord method; three points P, Q, R add to $\mathcal{O}_E$ if and only if they are the three intersection points of E with a (projective) line, counting multiplicities.
- Some basic questions are:
  1. what kind of a group is $E(K)$?
  2. how does $E(K)$ vary (for fixed K)?
  3. can we determine $E(K)$ (for given E)?

From now on we will take $K = \mathbb{Q}$.

Elliptic curves over $\mathbb{Q}$

- Mordell proved in 1922 that for every elliptic curve $E/\mathbb{Q}$ the group $E(\mathbb{Q})$ is *finitely-generated*.

Elliptic curves over $\mathbb{Q}$

- Mordell proved in 1922 that for every elliptic curve $E/\mathbb{Q}$ the group $E(\mathbb{Q})$ is *finitely-generated*.
- This was later generalised to elliptic curves over number fields, and beyond.

Elliptic curves over $\mathbb{Q}$

- Mordell proved in 1922 that for every elliptic curve $E/\mathbb{Q}$ the group $E(\mathbb{Q})$ is *finitely-generated*.
- This was later generalised to elliptic curves over number fields, and beyond.
- This essentially answers our first question:

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

where the *rank* $r(E) \geq 0$, and T is a finite group.

Elliptic curves over $\mathbb{Q}$

- Mordell proved in 1922 that for every elliptic curve $E/\mathbb{Q}$ the group $E(\mathbb{Q})$ is *finitely-generated*.
- This was later generalised to elliptic curves over number fields, and beyond.
- This essentially answers our first question:

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

  where the *rank* $r(E) \geq 0$, and T is a finite group.
- For the second question (over $K = \mathbb{Q}$), we know
  - $|T| \leq 16$ (Mazur, 1977)
  - there exists E with $r(E) \geq 28$ (Elkies, 2006)

Elliptic curves over $\mathbb{Q}$

- Mordell proved in 1922 that for every elliptic curve $E/\mathbb{Q}$ the group $E(\mathbb{Q})$ is *finitely-generated*.
- This was later generalised to elliptic curves over number fields, and beyond.
- This essentially answers our first question:

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

  where the *rank* $r(E) \geq 0$, and T is a finite group.
- For the second question (over $K = \mathbb{Q}$), we know
  - $|T| \leq 16$ (Mazur, 1977)
  - there exists E with $r(E) \geq 28$ (Elkies, 2006)
- BSD predicts the value of the “arithmetic rank” (or Mordell-Weil rank) $r(E)$ in terms of the L-function attached to E.

The L-function of $E/\mathbb{Q}$

- By suitable scaling we may assume that the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

defining an elliptic curve $E/\mathbb{Q}$ is *integral* (all $a_i \in \mathbb{Z}$) and *minimal* ($|\Delta_E|$ minimal).

The L-function of $E/\mathbb{Q}$

- By suitable scaling we may assume that the equation

  $$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

  defining an elliptic curve $E/\mathbb{Q}$ is *integral* (all $a_i \in \mathbb{Z}$) and *minimal* ($|\Delta_E|$ minimal).
- Let N_E denote the *conductor* of E: a positive integer divisible by the same primes as the minimal discriminant Δ_E.

The L-function of $E/\mathbb{Q}$

- By suitable scaling we may assume that the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

  defining an elliptic curve $E/\mathbb{Q}$ is *integral* (all $a_i \in \mathbb{Z}$) and *minimal* ($|\Delta_E|$ minimal).
- Let N_E denote the *conductor* of E: a positive integer divisible by the same primes as the minimal discriminant Δ_E. [Computed by Tate's algorithm.]

The L-function of $E/\mathbb{Q}$

- By suitable scaling we may assume that the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

  defining an elliptic curve $E/\mathbb{Q}$ is *integral* (all $a_i \in \mathbb{Z}$) and *minimal* ($|\Delta_E|$ minimal).
- Let N_E denote the *conductor* of E: a positive integer divisible by the same primes as the minimal discriminant Δ_E. [Computed by Tate's algorithm.]
- The L-function of E is a function of the complex variable s defined by the following *Euler product*:

$$L(E,s) = \prod_{p \nmid N_E} (1 - a_p p^{-s} + p^{1-2s})^{-1} \cdot \prod_{p \mid N_E} (1 - a_p p^{-s})^{-1}$$

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

The L-function of $E/\mathbb{Q}$ (continued)

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

- Since $|a_p| \le 2\sqrt{p}$ for all $p \nmid N_E$ (Hasse), the series converges in the half-plane $\Re(s) > 3/2$.

The L-function of $E/\mathbb{Q}$ (continued)

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

- Since $|a_p| \le 2\sqrt{p}$ for all $p \nmid N_E$ (Hasse), the series converges in the half-plane $\Re(s) > 3/2$.
- When $p \mid N_E$ we have $a_p = +1, -1, 0$ according to whether E has split or non-split multiplicative, or additive reduction at p.

The L-function of $E/\mathbb{Q}$ (continued)

$$L(E,s) = \prod_{p\nmid N_E}(1-a_pp^{-s}+p^{1-2s})^{-1}\cdot\prod_{p\mid N_E}(1-a_pp^{-s})^{-1} = \sum_{n=1}^{\infty}\frac{a_n}{n^s}$$

- Since $|a_p|\le 2\sqrt{p}$ for all $p\nmid N_E$ (Hasse), the series converges in the half-plane $\Re(s)>3/2$.
- When $p\mid N_E$ we have $a_p=+1,-1,0$ according to whether E has split or non-split multiplicative, or additive reduction at p.
- **First consequence of modularity:** $L(E,s)$ has *analytic continuation* to all of $\mathbb{C}$, and satisfies a *functional equation* relating $L(E,s)$ and $L(E,2-s)$:

$$\Lambda_E(s) := N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s) = w(E/\mathbb{Q})\Lambda_E(2-s)$$

The L-function of $E/\mathbb{Q}$ (continued)

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

- Since $|a_p| \le 2\sqrt{p}$ for all $p \nmid N_E$ (Hasse), the series converges in the half-plane $\Re(s) > 3/2$.
- When $p \mid N_E$ we have $a_p = +1, -1, 0$ according to whether E has split or non-split multiplicative, or additive reduction at p.
- **First consequence of modularity:** $L(E,s)$ has *analytic continuation* to all of $\mathbb{C}$, and satisfies a *functional equation* relating $L(E,s)$ and $L(E,2-s)$:

$$\Lambda_E(s) := N_E^{s/2} (2\pi)^{-s} \Gamma(s) L(E,s) = w(E/\mathbb{Q}) \Lambda_E(2-s)$$

where *root number* $w(E/\mathbb{Q}) = \pm 1$ is the *sign of the functional equation* (SFE) of E.

The analytic rank

- In particular, it makes sense to define the *analytic rank* $r_{an}(E)$:

$$r_{an}(E) := \mathrm{ord}_{s=1} L(E, s) \qquad (\geq 0)$$

The analytic rank

- In particular, it makes sense to define the *analytic rank* $r_{an}(E)$:

$$r_{an}(E) := \operatorname{ord}_{s=1} L(E, s) \qquad (\geq 0)$$

- The SFE is $w(E/\mathbb{Q}) = (-1)^{r_{an}(E)}$; in practice this means that the *parity* of $r_{an}(E)$ is easy to determine.

The analytic rank

- In particular, it makes sense to define the *analytic rank* $r_{an}(E)$:

$$r_{an}(E) := \mathrm{ord}_{s=1} L(E,s) \qquad (\geq 0)$$

- The SFE is $w(E/\mathbb{Q}) = (-1)^{r_{an}(E)}$; in practice this means that the *parity* of $r_{an}(E)$ is easy to determine.
- $r_{an}(E) = 0 \iff L(E,1) \neq 0$.

The analytic rank

- In particular, it makes sense to define the *analytic rank* $r_{an}(E)$:

$$r_{an}(E) := \operatorname{ord}_{s=1} L(E,s) \qquad (\geq 0)$$

- The SFE is $w(E/\mathbb{Q}) = (-1)^{r_{an}(E)}$; in practice this means that the *parity* of $r_{an}(E)$ is easy to determine.
- $r_{an}(E) = 0 \iff L(E,1) \neq 0$.
- Determining the exact value of $r_{an}(E)$ is currently only possible when $r_{an}(E) \leq 3$! More on this later.

The analytic rank

- In particular, it makes sense to define the *analytic rank* $r_{an}(E)$:

$$r_{an}(E) := \operatorname{ord}_{s=1} L(E,s) \qquad (\geq 0)$$

- The SFE is $w(E/\mathbb{Q}) = (-1)^{r_{an}(E)}$; in practice this means that the *parity* of $r_{an}(E)$ is easy to determine.
- $r_{an}(E) = 0 \iff L(E,1) \neq 0$.
- Determining the exact value of $r_{an}(E)$ is currently only possible when $r_{an}(E) \leq 3$! More on this later.
- How are the arithmetic rank $r(E)$ and the analytic rank $r_{an}(E)$ related?

The analytic rank

- In particular, it makes sense to define the *analytic rank* $r_{an}(E)$:

$$r_{an}(E) := \mathrm{ord}_{s=1} L(E,s) \qquad (\geq 0)$$

- The SFE is $w(E/\mathbb{Q}) = (-1)^{r_{an}(E)}$; in practice this means that the *parity* of $r_{an}(E)$ is easy to determine.
- $r_{an}(E) = 0 \iff L(E,1) \neq 0$.
- Determining the exact value of $r_{an}(E)$ is currently only possible when $r_{an}(E) \leq 3$! More on this later.
- How are the arithmetic rank $r(E)$ and the analytic rank $r_{an}(E)$ related?
  That is the million-dollar question!

The first Birch–Swinnerton-Dyer conjecture for elliptic curves over $\mathbb{Q}$

Conjecture (Birch and Swinnerton-Dyer, 1963)

Let E be an elliptic curve defined over $\mathbb{Q}$. Then the arithmetic and analytic ranks of E are equal:

$$r(E) = r_{an}(E).$$

The first Birch–Swinnerton-Dyer conjecture for elliptic curves over $\mathbb{Q}$

Conjecture (Birch and Swinnerton-Dyer, 1963)

Let E be an elliptic curve defined over $\mathbb{Q}$. Then the arithmetic and analytic ranks of E are equal:

$$r(E) = r_{an}(E).$$

For example, this implies that $E(\mathbb{Q})$ is infinite if and only $L(E, 1) = 0$.

The first Birch–Swinnerton-Dyer conjecture for elliptic curves over $\mathbb{Q}$

Conjecture (Birch and Swinnerton-Dyer, 1963)

Let E be an elliptic curve defined over $\mathbb{Q}$. Then the arithmetic and analytic ranks of E are equal:

$$r(E) = r_{an}(E).$$

For example, this implies that $E(\mathbb{Q})$ is infinite if and only $L(E, 1) = 0$.

We'll see later how to verify this conjecture for a given curve: though this is not possible in general, even in principle, for all elliptic curves given the present state of knowledge!

What's known?

- To date, here is what we know about the first conjecture:

Theorem (Kolyvagin; Murty & Murty; Bump, Friedberg & Hoffstein; Coates & Wiles; Gross & Zagier)

Let E be an elliptic curve defined over $\mathbb{Q}$. Then

$$r_{an}(E) \leq 1 \implies r(E) = r_{an}(E).$$

What's known?

- To date, here is what we know about the first conjecture:

Theorem (Kolyvagin; Murty & Murty; Bump, Friedberg & Hoffstein; Coates & Wiles; Gross & Zagier)

Let E be an elliptic curve defined over $\mathbb{Q}$. Then

$$r_{an}(E) \le 1 \implies r(E) = r_{an}(E).$$

- We will see later that when $r_{an}(E) \le 3$ it is possible (both in principle, and in practice) to determine the value of $r_{an}(E)$.

What's known?

- To date, here is what we know about the first conjecture:

Theorem (Kolyvagin; Murty & Murty; Bump, Friedberg & Hoffstein; Coates & Wiles; Gross & Zagier)

Let E be an elliptic curve defined over $\mathbb{Q}$. Then

$$r_{an}(E) \leq 1 \implies r(E) = r_{an}(E).$$

- We will see later that when $r_{an}(E) \leq 3$ it is possible (both in principle, and in practice) to determine the value of $r_{an}(E)$.
- We can often also determine $r(E)$, and hence verify the conjecture in (many) individual cases when $r_{an}(E) \leq 3$.

What's known?

- To date, here is what we know about the first conjecture:

Theorem (Kolyvagin; Murty & Murty; Bump, Friedberg & Hoffstein; Coates & Wiles; Gross & Zagier)

Let E be an elliptic curve defined over $\mathbb{Q}$. Then

$$r_{an}(E) \leq 1 \implies r(E) = r_{an}(E).$$

- We will see later that when $r_{an}(E) \leq 3$ it is possible (both in principle, and in practice) to determine the value of $r_{an}(E)$.
- We can often also determine $r(E)$, and hence verify the conjecture in (many) individual cases when $r_{an}(E) \leq 3$.
- Further results are known about the conjecture "modulo 2".

The Parity conjecture

- Reducing BSD modulo 2 we obtain

Conjecture (The Parity Conjecture)

$r(E) \equiv r_{an}(E) \pmod 2$. *Equivalently,* $w(E/\mathbb{Q}) = (-1)^{r(E)}$.

The Parity conjecture

- Reducing BSD modulo 2 we obtain

Conjecture (The Parity Conjecture)

$r(E) \equiv r_{an}(E) \pmod 2.$ *Equivalently,* $w(E/\mathbb{Q}) = (-1)^{r(E)}.$

This is much easier to verify for individual curves (by descent). But that is hardly necessary, since …

The Parity conjecture

- Reducing BSD modulo 2 we obtain

Conjecture (The Parity Conjecture)

$r(E) \equiv r_{an}(E) \pmod 2$. *Equivalently,* $w(E/\mathbb{Q}) = (-1)^{r(E)}$.

This is much easier to verify for individual curves (by descent). But that is hardly necessary, since ...

- Dokchitser & Dokchitser have proved many strong results in the direction of the parity conjecture; over number fields, they show that it follows from finiteness of the Tate-Shafarevich group Ш.

The Parity conjecture

- Reducing BSD modulo 2 we obtain

Conjecture (The Parity Conjecture)

$r(E) \equiv r_{an}(E) \pmod 2$. *Equivalently,* $w(E/\mathbb{Q}) = (-1)^{r(E)}$.

This is much easier to verify for individual curves (by descent). But that is hardly necessary, since …

- Dokchitser & Dokchitser have proved many strong results in the direction of the parity conjecture; over number fields, they show that it follows from finiteness of the Tate-Shafarevich group $Ш$.
- Over $\mathbb{Q}$ there is a stronger result:

Theorem (T. & V. Dokchitser 2009)

If the p-primary part of $Ш(E/\mathbb{Q})$ is finite for at least one prime p then the parity conjecture for $E/\mathbb{Q}$ holds.

The refined conjecture

- The refined, or strong form of BSD predicts the “special value” of $L(E,s)$ at $s = 1$.

The refined conjecture

- The refined, or strong form of BSD predicts the "special value" of $L(E,s)$ at $s=1$.
- This is the nonzero number c_E such that (with $r = r_{an}(E)$)

$$L(E,s) \sim c_E(s-1)^r \qquad \text{as } s \to 1;$$

equivalently,

$$c_E = \lim_{s\to 1} \frac{L(E,s)}{(s-1)^r} = \frac{1}{r!} L^{(r)}(E,1).$$

The refined conjecture

- The refined, or strong form of BSD predicts the “special value” of $L(E, s)$ at $s = 1$.
- This is the nonzero number c_E such that (with $r = r_{an}(E)$)

  $$L(E, s) \sim c_E (s-1)^r \qquad \text{as } s \to 1;$$

  equivalently,

  $$c_E = \lim_{s \to 1} \frac{L(E, s)}{(s-1)^r} = \frac{1}{r!} L^{(r)}(E, 1).$$

- The conjectured formula for c_E involves many other quantities associated to $E/\mathbb{Q}$, including the order of the Tate-Shafarevich group $Ш(E/\mathbb{Q})$ – whose finiteness had been conjectured around 1958-59 by Shafarevitch, Tate, Cassels, Birch and Swinnerton-Dyer, but is not known in general.

The second Birch–Swinnerton-Dyer conjecture for elliptic curves over $\mathbb{Q}$

Conjecture (Birch and Swinnerton-Dyer, 1963)

Let E be an elliptic curve defined over $\mathbb{Q}$. Then

1. $r(E) = r_{an}(E)$;
2. $Ш(E/\mathbb{Q})$ *is finite, and*

$$c_E = \lim_{s\to 1} \frac{L(E,s)}{(s-1)^{r(E)}} = \frac{\Omega(E)\,\mathrm{Reg}(E)(\prod_p c_p)|Ш(E/\mathbb{Q})|}{|E(\mathbb{Q})_{\mathrm{tors}}|^2}.$$

The second Birch–Swinnerton-Dyer conjecture for elliptic curves over $\mathbb{Q}$

Conjecture (Birch and Swinnerton-Dyer, 1963)

Let E be an elliptic curve defined over $\mathbb{Q}$. Then

1. $r(E) = r_{an}(E)$;
2. $\text{Ш}(E/\mathbb{Q})$ *is finite, and*

$$c_E = \lim_{s\to 1} \frac{L(E,s)}{(s-1)^{r(E)}} = \frac{\Omega(E)\,\mathrm{Reg}(E)(\prod_p c_p)|\text{Ш}(E/\mathbb{Q})|}{|E(\mathbb{Q})_{\mathrm{tors}}|^2}.$$

We will next explain what the various factors on the right-hand side are.

Invariants associated to $E(\mathbb{R})$ and $E(\mathbb{Q}_p)$

- $\Omega(E)$ is the *real period* of E multiplied by the number of components of $E(\mathbb{R})$ ($= 1$ or 2).

Invariants associated to $E(\mathbb{R})$ and $E(\mathbb{Q}_p)$

- $\Omega(E)$ is the *real period* of E multiplied by the number of components of $E(\mathbb{R})$ ($=1$ or 2).
  Equivalently, $\Omega(E) = \int_{E(\mathbb{R})} \omega_E$ where (in terms of a minimal Weierstrass model of E), ω_E is the differential

$$\omega_E = \frac{dx}{2y + a_1 x + a_3}.$$

Invariants associated to $E(\mathbb{R})$ and $E(\mathbb{Q}_p)$

- $\Omega(E)$ is the *real period* of E multiplied by the number of components of $E(\mathbb{R})$ ($= 1$ or 2).
  Equivalently, $\Omega(E) = \int_{E(\mathbb{R})} \omega_E$ where (in terms of a minimal Weierstrass model of E), ω_E is the differential

$$\omega_E = \frac{dx}{2y + a_1 x + a_3}.$$

  This is easy to compute to any desired precision using the doubly exponential AGM algorithm.

Invariants associated to $E(\mathbb{R})$ and $E(\mathbb{Q}_p)$

- $\Omega(E)$ is the *real period* of E multiplied by the number of components of $E(\mathbb{R})$ ($=1$ or 2).
  Equivalently, $\Omega(E) = \int_{E(\mathbb{R})} \omega_E$ where (in terms of a minimal Weierstrass model of E), ω_E is the differential
  $$\omega_E = \frac{dx}{2y + a_1 x + a_3}.$$
  This is easy to compute to any desired precision using the doubly exponential AGM algorithm.
- For each prime p, c_p is the *Tamagawa number* $[E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)]$, that is, the order of the group of components of $E(\mathbb{Q}_p)$; this is 1 for all primes of good reduction.

Invariants associated to $E(\mathbb{R})$ and $E(\mathbb{Q}_p)$

- $\Omega(E)$ is the *real period* of E multiplied by the number of components of $E(\mathbb{R})$ ($=1$ or 2).
  Equivalently, $\Omega(E) = \int_{E(\mathbb{R})} \omega_E$ where (in terms of a minimal Weierstrass model of E), ω_E is the differential

  $$\omega_E = \frac{dx}{2y + a_1x + a_3}.$$

  This is easy to compute to any desired precision using the doubly exponential AGM algorithm.
- For each prime p, c_p is the *Tamagawa number* $[E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)]$, that is, the order of the group of components of $E(\mathbb{Q}_p)$; this is 1 for all primes of good reduction. These are easy to compute using Tate's algorithm (again).

Invariants associated to $E(\mathbb{Q})$

- $\mathrm{Reg}(E)$ is the *regulator* of E, which is the determinant of the height pairing. This can be computed to any desired precision *provided that* generators for the group $E(\mathbb{Q})$ are known.

Invariants associated to $E(\mathbb{Q})$

- $\mathrm{Reg}(E)$ is the *regulator* of E, which is the determinant of the height pairing. This can be computed to any desired precision *provided that* generators for the group $E(\mathbb{Q})$ are known.
- Finding the order of the torsion subgroup $E(\mathbb{Q})_{\mathrm{tors}}$ is no problem.

Invariants associated to $E(\mathbb{Q})$

- $\mathrm{Reg}(E)$ is the *regulator* of E, which is the determinant of the height pairing. This can be computed to any desired precision *provided that* generators for the group $E(\mathbb{Q})$ are known.
- Finding the order of the torsion subgroup $E(\mathbb{Q})_{\mathrm{tors}}$ is no problem.
- $Ш(E/\mathbb{Q})$ is defined as

$$Ш(E/\mathbb{Q}) = \ker\left(H^1(G_{\mathbb{Q}}, E) \to \prod_p H^1(G_{\mathbb{Q}_p}, E)\right).$$

Invariants associated to $E(\mathbb{Q})$

- $\mathrm{Reg}(E)$ is the *regulator* of E, which is the determinant of the height pairing. This can be computed to any desired precision *provided that* generators for the group $E(\mathbb{Q})$ are known.
- Finding the order of the torsion subgroup $E(\mathbb{Q})_{\mathrm{tors}}$ is no problem.
- $\text{Ш}(E/\mathbb{Q})$ is defined as

$$\text{Ш}(E/\mathbb{Q}) = \ker\left(H^1(G_{\mathbb{Q}}, E) \to \prod_p H^1(G_{\mathbb{Q}_p}, E) \right).$$

  $\text{Ш}(E/\mathbb{Q})$ consists of twists of E, up to isomorphism, which have rational points everywhere locally.

Invariants associated to $E(\mathbb{Q})$

- $\mathrm{Reg}(E)$ is the *regulator* of E, which is the determinant of the height pairing. This can be computed to any desired precision *provided that* generators for the group $E(\mathbb{Q})$ are known.
- Finding the order of the torsion subgroup $E(\mathbb{Q})_{\mathrm{tors}}$ is no problem.
- $Ш(E/\mathbb{Q})$ is defined as

$$Ш(E/\mathbb{Q}) = \ker\left(H^1(G_{\mathbb{Q}}, E) \to \prod_p H^1(G_{\mathbb{Q}_p}, E)\right).$$

  $Ш(E/\mathbb{Q})$ consists of twists of E, up to isomorphism, which have rational points everywhere locally.
  It is the most mysterious object in this theory, and very hard to get one's hands on, or even to write down elements of.

The Tate-Shafarevich group

$$Ш(E/\mathbb{Q}) = \ker\left(H^1(G_{\mathbb{Q}}, E) \to \prod_p H^1(G_{\mathbb{Q}_p}, E)\right).$$

- $Ш(E/\mathbb{Q})$ is a torsion abelian group.

The Tate-Shafarevich group

$$Ш(E/\mathbb{Q}) = \ker\left(H^1(G_\mathbb{Q}, E) \to \prod_p H^1(G_{\mathbb{Q}_p}, E)\right).$$

- $Ш(E/\mathbb{Q})$ is a torsion abelian group.
- Finding $|Ш(E/\mathbb{Q})|$ computationally is impossible in general!

The Tate-Shafarevich group

$$Ш(E/\mathbb{Q}) = \ker\left(H^1(G_{\mathbb{Q}}, E) \to \prod_p H^1(G_{\mathbb{Q}_p}, E)\right).$$

- $Ш(E/\mathbb{Q})$ is a torsion abelian group.
- Finding $|Ш(E/\mathbb{Q})|$ computationally is impossible in general!
- Let $Ш(p) = Ш(E/\mathbb{Q})(p)$ denote the p-primary part of $Ш(E/\mathbb{Q})$.

The Tate-Shafarevich group

$$Ш(E/\mathbb{Q}) = \ker\left(H^1(G_{\mathbb{Q}}, E) \to \prod_p H^1(G_{\mathbb{Q}_p}, E)\right).$$

- $Ш(E/\mathbb{Q})$ is a torsion abelian group.
- Finding $|Ш(E/\mathbb{Q})|$ computationally is impossible in general!
- Let $Ш(p) = Ш(E/\mathbb{Q})(p)$ denote the p-primary part of $Ш(E/\mathbb{Q})$. Finding $|Ш(E/\mathbb{Q})|$ involves finding $|Ш(p)|$ for all primes p. In practice, what one can hope to do is to show that $Ш(p)$ is trivial for p outside some finite set and then use p-descent and p-adic methods to determine $|Ш(p)|$ for the remaining primes.

The Tate-Shafarevich group

$$Ш(E/\mathbb{Q}) = \ker\left(H^1(G_{\mathbb{Q}}, E) \to \prod_p H^1(G_{\mathbb{Q}_p}, E)\right).$$

- $Ш(E/\mathbb{Q})$ is a torsion abelian group.
- Finding $|Ш(E/\mathbb{Q})|$ computationally is impossible in general!
- Let $Ш(p) = Ш(E/\mathbb{Q})(p)$ denote the p-primary part of $Ш(E/\mathbb{Q})$.
  Finding $|Ш(E/\mathbb{Q})|$ involves finding $|Ш(p)|$ for all primes p.
  In practice, what one can hope to do is to show that $Ш(p)$ is trivial for p outside some finite set and then use p-descent and p-adic methods to determine $|Ш(p)|$ for the remaining primes.
  The first of these steps is possible (currently) *only* when $r_{an}(E) \leq 1$.

The Tate-Shafarevich group

$$Ш(E/\mathbb{Q}) = \ker\left(H^1(G_{\mathbb{Q}}, E) \to \prod_p H^1(G_{\mathbb{Q}_p}, E)\right).$$

- $Ш(E/\mathbb{Q})$ is a torsion abelian group.
- Finding $|Ш(E/\mathbb{Q})|$ computationally is impossible in general!
- Let $Ш(p) = Ш(E/\mathbb{Q})(p)$ denote the p-primary part of $Ш(E/\mathbb{Q})$. Finding $|Ш(E/\mathbb{Q})|$ involves finding $|Ш(p)|$ for all primes p.
  In practice, what one can hope to do is to show that $Ш(p)$ is trivial for p outside some finite set and then use p-descent and p-adic methods to determine $|Ш(p)|$ for the remaining primes.
  The first of these steps is possible (currently) *only* when $r_{an}(E) \leq 1$.
  The second is often possible for individual primes, when $r_{an}(E) \geq 2$.

Verifying the conjecture

There are serious problems involved in verifying the conjecture for specific curves (let alone for infinite families, or for all curves).

- The strong conjecture involves the order of a group $Ш(E/\mathbb{Q})$ which is only known to be finite when $r_{an}(E) \leq 1$.

Verifying the conjecture

There are serious problems involved in verifying the conjecture for specific curves (let alone for infinite families, or for all curves).

- The strong conjecture involves the order of a group $\text{Ш}(E/\mathbb{Q})$ which is only known to be finite when $r_{an}(E) \leq 1$.
  But the situation is better than when Tate made his famous comment about the BSD conjecture relating the order of a group not known to be finite with the value of a function at a point where it is not known to be defined, since we *do* now know that $L(E,s)$ is defined for all $s \in \mathbb{C}$!

Verifying the conjecture

There are serious problems involved in verifying the conjecture for specific curves (let alone for infinite families, or for all curves).

- The strong conjecture involves the order of a group $Ш(E/\mathbb{Q})$ which is only known to be finite when $r_{an}(E) \leq 1$.
  But the situation is better than when Tate made his famous comment about the BSD conjecture relating the order of a group not known to be finite with the value of a function at a point where it is not known to be defined, since we *do* now know that $L(E, s)$ is defined for all $s \in \mathbb{C}$!
- However, the theorem of Kolyvagin *et al.* also states that $Ш(E/\mathbb{Q})$ is finite when $r_{an}(E) \leq 1$.

Verifying the conjecture

There are serious problems involved in verifying the conjecture for specific curves (let alone for infinite families, or for all curves).

- The strong conjecture involves the order of a group $Ш(E/\mathbb{Q})$ which is only known to be finite when $r_{an}(E) \leq 1$.
  But the situation is better than when Tate made his famous comment about the BSD conjecture relating the order of a group not known to be finite with the value of a function at a point where it is not known to be defined, since we *do* now know that $L(E, s)$ is defined for all $s \in \mathbb{C}$!
- However, the theorem of Kolyvagin *et al.* also states that $Ш(E/\mathbb{Q})$ is finite when $r_{an}(E) \leq 1$. (The statement is more precise, as we will see later.)

Verifying the conjecture

There are serious problems involved in verifying the conjecture for specific curves (let alone for infinite families, or for all curves).

- The strong conjecture involves the order of a group $\text{Ш}(E/\mathbb{Q})$ which is only known to be finite when $r_{an}(E) \leq 1$.
  But the situation is better than when Tate made his famous comment about the BSD conjecture relating the order of a group not known to be finite with the value of a function at a point where it is not known to be defined, since we *do* now know that $L(E, s)$ is defined for all $s \in \mathbb{C}$!
- However, the theorem of Kolyvagin *et al.* also states that $\text{Ш}(E/\mathbb{Q})$ is finite when $r_{an}(E) \leq 1$. (The statement is more precise, as we will see later.)
- For no curve of analytic rank ≥ 2 is Ш known to be finite; so we have no hope of verifying BSD II in such cases.

Verifying the conjecture

There are serious problems involved in verifying the conjecture for specific curves (let alone for infinite families, or for all curves).

- The strong conjecture involves the order of a group $Ш(E/\mathbb{Q})$ which is only known to be finite when $r_{an}(E) \leq 1$.
  But the situation is better than when Tate made his famous comment about the BSD conjecture relating the order of a group not known to be finite with the value of a function at a point where it is not known to be defined, since we *do* now know that $L(E, s)$ is defined for all $s \in \mathbb{C}$!
- However, the theorem of Kolyvagin *et al.* also states that $Ш(E/\mathbb{Q})$ is finite when $r_{an}(E) \leq 1$. (The statement is more precise, as we will see later.)
- For no curve of analytic rank ≥ 2 is $Ш$ known to be finite; so we have no hope of verifying BSD II in such cases. This will not stop us talking about “numerical evidence”!

Verifying the first conjecture

- To start with let us see whether we can verify, for indiviual curves E, that the first conjecture holds: $r(E) = r_{an}(E)$.

Verifying the first conjecture

- To start with let us see whether we can verify, for indiviual curves E, that the first conjecture holds: $r(E) = r_{an}(E)$.
- We know that this is true when $r_{an}(E) \leq 1$, but how may we determine $r_{an}(E)$?

Verifying the first conjecture

- To start with let us see whether we can verify, for indiviual curves E, that the first conjecture holds: $r(E) = r_{an}(E)$.
- We know that this is true when $r_{an}(E) \leq 1$, but how may we determine $r_{an}(E)$?
- This may seem like a problem in numerical analysis, but we can do a lot better than just computing the value $L(E, 1)$ numerically to see if it looks like 0.0000.

Verifying the first conjecture

- To start with let us see whether we can verify, for indiviual curves E, that the first conjecture holds: $r(E) = r_{an}(E)$.
- We know that this is true when $r_{an}(E) \leq 1$, but how may we determine $r_{an}(E)$?
- This may seem like a problem in numerical analysis, but we can do a lot better than just computing the value $L(E, 1)$ numerically to see if it looks like 0.0000.
- First of all, we can compute the root number $w(E/\mathbb{Q})$ exactly (as a product of local root numbers). This tells us the parity of $r_{an}(E)$. But also…

Verifying the first conjecture

- To start with let us see whether we can verify, for indiviual curves E, that the first conjecture holds: $r(E) = r_{an}(E)$.
- We know that this is true when $r_{an}(E) \leq 1$, but how may we determine $r_{an}(E)$?
- This may seem like a problem in numerical analysis, but we can do a lot better than just computing the value $L(E,1)$ numerically to see if it looks like 0.0000.
- First of all, we can compute the root number $w(E/\mathbb{Q})$ exactly (as a product of local root numbers). This tells us the parity of $r_{an}(E)$. But also…
- **Second consequence of modularity:** The ratio $L(E,1)/\Omega(E)$ is a rational number whose value may be determined *exactly* using modular symbols.

Verifying the first conjecture

- To start with let us see whether we can verify, for indiviual curves E, that the first conjecture holds: $r(E) = r_{an}(E)$.
- We know that this is true when $r_{an}(E) \leq 1$, but how may we determine $r_{an}(E)$?
- This may seem like a problem in numerical analysis, but we can do a lot better than just computing the value $L(E, 1)$ numerically to see if it looks like 0.0000.
- First of all, we can compute the root number $w(E/\mathbb{Q})$ exactly (as a product of local root numbers). This tells us the parity of $r_{an}(E)$. But also...
- **Second consequence of modularity:** The ratio $L(E, 1)/\Omega(E)$ is a rational number whose value may be determined *exactly* using modular symbols. In particular, we can determine via a *discrete algorithm* whether or not $L(E, 1)$ is zero; equivalently, whether $r_{an}(E) = 0$.

Determining $r_{an}(E)$ (continued)

- Putting these together, we can determine (discretely) whether

$$r_{an}(E) = 0 \qquad \text{or} \qquad r_{an}(E) = 1, 3, 5, \ldots \qquad \text{or} \qquad r_{an}(E) = 2, 4, 6, \ldots$$

Determining $r_{an}(E)$ (continued)

- Putting these together, we can determine (discretely) whether

$$r_{an}(E) = 0 \qquad \text{or} \qquad r_{an}(E) = 1, 3, 5, \ldots \qquad \text{or} \qquad r_{an}(E) = 2, 4, 6, \ldots$$

- If $r_{an}(E)$ is odd then evaluating $L'(E, 1)$ approximately can prove that it is nonzero, and hence that $r_{an}(E) = 1$ (if it is).

Determining $r_{an}(E)$ (continued)

- Putting these together, we can determine (discretely) whether

$$r_{an}(E) = 0 \qquad \text{or} \qquad r_{an}(E) = 1, 3, 5, \dots \qquad \text{or} \qquad r_{an}(E) = 2, 4, 6, \dots$$

- If $r_{an}(E)$ is odd then evaluating $L'(E, 1)$ approximately can prove that it is nonzero, and hence that $r_{an}(E) = 1$ (if it is).
- Similarly, if $r_{an}(E)$ is even and positive, then evaluating $L''(E, 1)$ approximately can prove that it is nonzero, and hence that $r_{an}(E) = 2$ (if it is).

Determining $r_{an}(E)$ (continued)

- Putting these together, we can determine (discretely) whether

$$r_{an}(E) = 0 \qquad \text{or} \qquad r_{an}(E) = 1, 3, 5, \dots \qquad \text{or} \qquad r_{an}(E) = 2, 4, 6, \dots$$

- If $r_{an}(E)$ is odd then evaluating $L'(E, 1)$ approximately can prove that it is nonzero, and hence that $r_{an}(E) = 1$ (if it is).
- Similarly, if $r_{an}(E)$ is even and positive, then evaluating $L''(E, 1)$ approximately can prove that it is nonzero, and hence that $r_{an}(E) = 2$ (if it is).
- Further, if $r_{an}(E)$ is odd and $L'(E, 1)$ is *approximately* zero, then we can prove that it is *exactly* zero: by finding (at least) two independent points in $E(\mathbb{Q})$, we can show that $r(E) > 1$, and hence that $r_{an}(E) > 1$. Now computing $L'''(E, 1)$ approximately can establish that $r_{an}(E) = 3$ (if it is).

Verifying the first conjecture: summary

- If $r_{an}(E) \leq 3$ then we can find the exact value of $r_{an}(E)$, using
  1. the root number (to obtain the parity);
  2. modular symbols (to establish whether $r_{an}(E) = 0$);
  3. Kolyvagin and Gross-Zagier (to distinguish $r_{an}(E) = 1$ from $r_{an}(E) = 3$);
  4. Numerical evaluation of $L^{(j)}(E, 1)$.

Verifying the first conjecture: summary

- If $r_{an}(E) \leq 3$ then we can find the exact value of $r_{an}(E)$, using
  1. the root number (to obtain the parity);
  2. modular symbols (to establish whether $r_{an}(E) = 0$);
  3. Kolyvagin and Gross-Zagier (to distinguish $r_{an}(E) = 1$ from $r_{an}(E) = 3$);
  4. Numerical evaluation of $L^{(j)}(E, 1)$.
- *But* if $r_{an}(E) > 3$ then we have no way of determining it rigorously!

Verifying the first conjecture: summary

- If $r_{an}(E) \leq 3$ then we can find the exact value of $r_{an}(E)$, using
  1. the root number (to obtain the parity);
  2. modular symbols (to establish whether $r_{an}(E) = 0$);
  3. Kolyvagin and Gross-Zagier (to distinguish $r_{an}(E) = 1$ from $r_{an}(E) = 3$);
  4. Numerical evaluation of $L^{(j)}(E, 1)$.
- *But* if $r_{an}(E) > 3$ then we have no way of determining it rigorously!
- If $r_{an}(E) = 4$ then we can tell that it is positive and even, and compute that $L''(E, 1)$ is very close to zero, but have no way of showing that $L''(E, 1) = 0$.

Verifying the first conjecture: summary

- If $r_{an}(E) \leq 3$ then we can find the exact value of $r_{an}(E)$, using
  1. the root number (to obtain the parity);
  2. modular symbols (to establish whether $r_{an}(E) = 0$);
  3. Kolyvagin and Gross-Zagier (to distinguish $r_{an}(E) = 1$ from $r_{an}(E) = 3$);
  4. Numerical evaluation of $L^{(j)}(E, 1)$.
- *But* if $r_{an}(E) > 3$ then we have no way of determining it rigorously!
- If $r_{an}(E) = 4$ then we can tell that it is positive and even, and compute that $L''(E, 1)$ is very close to zero, but have no way of showing that $L''(E, 1) = 0$.
- Similarly, If $r_{an}(E) = 5$ then we can tell that it is odd and at least 3, and compute that $L'''(E, 1)$ is very close to zero, but have no way of showing that $L'''(E, 1) = 0$.

Verifying the first conjecture: examples

There are 614308 isogeny classes of elliptic curves with conductor $N_E \leq 140000$.

Verifying the first conjecture: examples

There are 614308 isogeny classes of elliptic curves with conductor $N_E \leq 140000$. All have $r_{an}(E) \leq 3$, and in every case $r_{an}(E) = r(E)$.

range of N_E	#	$r=0$	$r=1$	$r=2$	$r=3$
0-9999	38042	16450	19622	1969	1
10000-19999	43175	17101	22576	3490	8
20000-29999	44141	17329	22601	4183	28
30000-39999	44324	16980	22789	4517	38
40000-49999	44519	16912	22826	4727	54
50000-59999	44301	16728	22400	5126	47
60000-69999	44361	16568	22558	5147	88
70000-79999	44449	16717	22247	5400	85
80000-89999	44861	17052	22341	5369	99
90000-99999	45053	16923	22749	5568	83
100000-109999	44274	16599	22165	5369	141
110000-119999	44071	16307	22173	5453	138
120000-129999	44655	16288	22621	5648	98
130000-139999	44082	16025	22201	5738	118
0-139999	614308	233979	311599	67704	1026

A case with $r = 0$

- The curve $E = 11a1$ has coefficients $[0, -1, 1, -10, -20]$ and conductor 11.

A case with $r = 0$

- The curve $E = 11a1$ has coefficients $[0, -1, 1, -10, -20]$ and conductor 11.
- Using modular symbols we find that $L(E, 1)/\Omega(E) = \frac{1}{5}$ (exactly!). So $r_{an}(E) = 0$, and hence we know that $r_{an}(E) = r(E)$.

A case with $r = 0$

- The curve $E = 11a1$ has coefficients $[0, -1, 1, -10, -20]$ and conductor 11.
- Using modular symbols we find that $L(E, 1)/\Omega(E) = \frac{1}{5}$ (exactly!). So $r_{an}(E) = 0$, and hence we know that $r_{an}(E) = r(E)$.
- Also $\prod_p c_p = c_{11} = 5$ and $\#E(\mathbb{Q})_{\text{tors}} = 5$.

A case with $r = 0$

- The curve $E = 11a1$ has coefficients $[0, -1, 1, -10, -20]$ and conductor 11.
- Using modular symbols we find that $L(E, 1)/\Omega(E) = \frac{1}{5}$ (exactly!). So $r_{an}(E) = 0$, and hence we know that $r_{an}(E) = r(E)$.
- Also $\prod_p c_p = c_{11} = 5$ and $\#E(\mathbb{Q})_{\text{tors}} = 5$.
- BSD predicts that $\#Ш(E/\mathbb{Q}) = \frac{L(E,1)/\Omega(E)}{\prod c_p/\#T^2} = \frac{1/5}{5/5^2} = 1$.

A case with $r = 0$

- The curve $E = 11a1$ has coefficients $[0, -1, 1, -10, -20]$ and conductor 11.
- Using modular symbols we find that $L(E, 1)/\Omega(E) = \frac{1}{5}$ (exactly!). So $r_{an}(E) = 0$, and hence we know that $r_{an}(E) = r(E)$.
- Also $\prod_p c_p = c_{11} = 5$ and $\#E(\mathbb{Q})_{\text{tors}} = 5$.
- BSD predicts that $\#Ш(E/\mathbb{Q}) = \frac{L(E,1)/\Omega(E)}{\prod c_p/\#T^2} = \frac{1/5}{5/5^2} = 1$.
- This can be verified by careful application of known results: see R. L. Miller, *Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one*, `arXiv:1010.2431v2 [math.NT]` for details of this and similar examples, including *all* curves of rank at most 1 and conductor less than 5000. Or …

A case with $r = 0$

- The curve $E = 11a1$ has coefficients $[0, -1, 1, -10, -20]$ and conductor 11.
- Using modular symbols we find that $L(E, 1)/\Omega(E) = \frac{1}{5}$ (exactly!). So $r_{an}(E) = 0$, and hence we know that $r_{an}(E) = r(E)$.
- Also $\prod_p c_p = c_{11} = 5$ and $\#E(\mathbb{Q})_{\text{tors}} = 5$.
- BSD predicts that $\#Ш(E/\mathbb{Q}) = \frac{L(E,1)/\Omega(E)}{\prod c_p/\#T^2} = \frac{1/5}{5/5^2} = 1$.
- This can be verified by careful application of known results: see R. L. Miller, *Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one*, `arXiv:1010.2431v2 [math.NT]` for details of this and similar examples, including *all* curves of rank at most 1 and conductor less than 5000. Or ...
- `sage: EllipticCurve('11a1').prove_BSD()`!

A case with $r = 1$

- The curve $E = 12480o1$ has coefficients $[0, -1, 0, -260, -1530]$ and conductor $12480 = 2^6 \cdot 3 \cdot 5 \cdot 13$.

A case with $r = 1$

- The curve $E = 12480o1$ has coefficients $[0, -1, 0, -260, -1530]$ and conductor $12480 = 2^6 \cdot 3 \cdot 5 \cdot 13$.
- The root number is -1, so $r_{an}(E)$ is odd.

A case with $r = 1$

- The curve $E = 12480o1$ has coefficients $[0, -1, 0, -260, -1530]$ and conductor $12480 = 2^6 \cdot 3 \cdot 5 \cdot 13$.
- The root number is -1, so $r_{an}(E)$ is odd.
- $L'(E, 1) = 4.258599\dots$ (approximately), so $r_{an}(E) = 1$.

A case with $r = 1$

- The curve $E = 12480o1$ has coefficients $[0, -1, 0, -260, -1530]$ and conductor $12480 = 2^6 \cdot 3 \cdot 5 \cdot 13$.
- The root number is -1, so $r_{an}(E)$ is odd.
- $L'(E, 1) = 4.258599\ldots$ (approximately), so $r_{an}(E) = 1$.
- 2-descent verifies that $r(E) = 1$ and gives the generator $(27, 102)$ whose canonical height is $\mathrm{Reg}(E) = 3.5830\ldots$. It also shows that $Ш(E/\mathbb{Q})[2]$ has order 4.

A case with $r = 1$

- The curve $E = 12480o1$ has coefficients $[0, -1, 0, -260, -1530]$ and conductor $12480 = 2^6 \cdot 3 \cdot 5 \cdot 13$.
- The root number is -1, so $r_{an}(E)$ is odd.
- $L'(E, 1) = 4.258599\dots$ (approximately), so $r_{an}(E) = 1$.
- 2-descent verifies that $r(E) = 1$ and gives the generator $(27, 102)$ whose canonical height is $\mathrm{Reg}(E) = 3.5830\dots$. It also shows that $Ш(E/\mathbb{Q})[2]$ has order 4.
- An AGM computation shows that $\Omega(E) = 1.1885495\dots$;

A case with $r = 1$

- The curve $E = 12480o1$ has coefficients $[0, -1, 0, -260, -1530]$ and conductor $12480 = 2^6 \cdot 3 \cdot 5 \cdot 13$.
- The root number is -1, so $r_{an}(E)$ is odd.
- $L'(E, 1) = 4.258599\ldots$ (approximately), so $r_{an}(E) = 1$.
- 2-descent verifies that $r(E) = 1$ and gives the generator $(27, 102)$ whose canonical height is $\mathrm{Reg}(E) = 3.5830\ldots$. It also shows that $Ш(E/\mathbb{Q})[2]$ has order 4.
- An AGM computation shows that $\Omega(E) = 1.1885495\ldots$; now $L'(E, 1)/(\Omega(E)\,\mathrm{Reg}(E)) = 1.0000000000\ldots$.

A case with $r = 1$

- The curve $E = 12480o1$ has coefficients $[0, -1, 0, -260, -1530]$ and conductor $12480 = 2^6 \cdot 3 \cdot 5 \cdot 13$.
- The root number is -1, so $r_{an}(E)$ is odd.
- $L'(E, 1) = 4.258599\dots$ (approximately), so $r_{an}(E) = 1$.
- 2-descent verifies that $r(E) = 1$ and gives the generator $(27, 102)$ whose canonical height is $\mathrm{Reg}(E) = 3.5830\dots$. It also shows that $Ш(E/\mathbb{Q})[2]$ has order 4.
- An AGM computation shows that $\Omega(E) = 1.1885495\dots$; now $L'(E, 1)/(\Omega(E)\,\mathrm{Reg}(E)) = 1.0000000000\dots$.
- Using Gross-Zagier this value can be shown to be exactly 1.

A case with $r = 1$

- The curve $E = 12480o1$ has coefficients $[0, -1, 0, -260, -1530]$ and conductor $12480 = 2^6 \cdot 3 \cdot 5 \cdot 13$.
- The root number is -1, so $r_{an}(E)$ is odd.
- $L'(E, 1) = 4.258599\ldots$ (approximately), so $r_{an}(E) = 1$.
- 2-descent verifies that $r(E) = 1$ and gives the generator $(27, 102)$ whose canonical height is $\mathrm{Reg}(E) = 3.5830\ldots$. It also shows that $\text{Ш}(E/\mathbb{Q})[2]$ has order 4.
- An AGM computation shows that $\Omega(E) = 1.1885495\ldots$; now $L'(E, 1)/(\Omega(E)\,\mathrm{Reg}(E)) = 1.0000000000\ldots$.
- Using Gross-Zagier this value can be shown to be exactly 1.
- We have $\prod c_p = 1$ and $\#E(\mathbb{Q})_{\mathrm{tors}} = 2$.

A case with $r = 1$

- The curve $E = 12480o1$ has coefficients $[0, -1, 0, -260, -1530]$ and conductor $12480 = 2^6 \cdot 3 \cdot 5 \cdot 13$.
- The root number is -1, so $r_{an}(E)$ is odd.
- $L'(E, 1) = 4.258599\ldots$ (approximately), so $r_{an}(E) = 1$.
- 2-descent verifies that $r(E) = 1$ and gives the generator $(27, 102)$ whose canonical height is $\mathrm{Reg}(E) = 3.5830\ldots$. It also shows that $Ш(E/\mathbb{Q})[2]$ has order 4.
- An AGM computation shows that $\Omega(E) = 1.1885495\ldots$; now $L'(E, 1)/(\Omega(E)\,\mathrm{Reg}(E)) = 1.0000000000\ldots$.
- Using Gross-Zagier this value can be shown to be exactly 1.
- We have $\prod c_p = 1$ and $\#E(\mathbb{Q})_{\mathrm{tors}} = 2$.
- BSD predicts that $\#Ш(E/\mathbb{Q}) = \frac{L'(E,1)/\,\mathrm{Reg}(E)\Omega(E)}{\prod c_p/\#T^2} = \frac{1}{1/2^2} = 4$.

A case with $r = 1$

- The curve $E = 12480o1$ has coefficients $[0, -1, 0, -260, -1530]$ and conductor $12480 = 2^6 \cdot 3 \cdot 5 \cdot 13$.
- The root number is -1, so $r_{an}(E)$ is odd.
- $L'(E, 1) = 4.258599\dots$ (approximately), so $r_{an}(E) = 1$.
- 2-descent verifies that $r(E) = 1$ and gives the generator $(27, 102)$ whose canonical height is $\mathrm{Reg}(E) = 3.5830\dots$. It also shows that $Ш(E/\mathbb{Q})[2]$ has order 4.
- An AGM computation shows that $\Omega(E) = 1.1885495\dots$; now $L'(E, 1)/(\Omega(E)\,\mathrm{Reg}(E)) = 1.0000000000\dots$.
- Using Gross-Zagier this value can be shown to be exactly 1.
- We have $\prod c_p = 1$ and $\#E(\mathbb{Q})_{\mathrm{tors}} = 2$.
- BSD predicts that $\#Ш(E/\mathbb{Q}) = \frac{L'(E,1)/\,\mathrm{Reg}(E)\Omega(E)}{\prod c_p/\#T^2} = \frac{1}{1/2^2} = 4$.
- Kolyvagin gives $\#Ш(E/\mathbb{Q})$ finite with no odd part.

A case with $r = 1$

- The curve $E = 12480o1$ has coefficients $[0, -1, 0, -260, -1530]$ and conductor $12480 = 2^6 \cdot 3 \cdot 5 \cdot 13$.
- The root number is -1, so $r_{an}(E)$ is odd.
- $L'(E, 1) = 4.258599\ldots$ (approximately), so $r_{an}(E) = 1$.
- 2-descent verifies that $r(E) = 1$ and gives the generator $(27, 102)$ whose canonical height is $\mathrm{Reg}(E) = 3.5830\ldots$. It also shows that $Ш(E/\mathbb{Q})[2]$ has order 4.
- An AGM computation shows that $\Omega(E) = 1.1885495\ldots$; now $L'(E, 1)/(\Omega(E)\,\mathrm{Reg}(E)) = 1.0000000000\ldots$.
- Using Gross-Zagier this value can be shown to be exactly 1.
- We have $\prod c_p = 1$ and $\#E(\mathbb{Q})_{\mathrm{tors}} = 2$.
- BSD predicts that $\#Ш(E/\mathbb{Q}) = \frac{L'(E,1)/\,\mathrm{Reg}(E)\Omega(E)}{\prod c_p/\#T^2} = \frac{1}{1/2^2} = 4$.
- Kolyvagin gives $\#Ш(E/\mathbb{Q})$ finite with no odd part.
- BSD holds!

A case with $r = 2$

- $E = 389a1 = [0, 1, 1, -2, 0]$ has conductor 389.

A case with $r = 2$

- $E = 389a1 = [0, 1, 1, -2, 0]$ has conductor 389.
- $w_E = +1$, so $r_{an}(E)$ is even. Modular symbols show that $r_{an}(E) \neq 0$.

A case with $r = 2$

- $E = 389a1 = [0, 1, 1, -2, 0]$ has conductor 389.
- $w_E = +1$, so $r_{an}(E)$ is even. Modular symbols show that $r_{an}(E) \neq 0$.
- $L''(E, 1) = 1.51863300057685\ldots$ (approximately), so $r_{an}(E) = 2$.

A case with $r = 2$

- $E = 389a1 = [0, 1, 1, -2, 0]$ has conductor 389.
- $w_E = +1$, so $r_{an}(E)$ is even. Modular symbols show that $r_{an}(E) \neq 0$.
- $L''(E, 1) = 1.51863300057685\ldots$ (approximately), so $r_{an}(E) = 2$.
- $r(E) = 2$ by 2-descent, which finds generators $(0, -1)$ and $(-1, 1)$ with $\mathrm{Reg}(E) = 0.152460\ldots$, and also that $Ш(E/\mathbb{Q})[2] = 0$.

A case with $r = 2$

- $E = 389a1 = [0, 1, 1, -2, 0]$ has conductor 389.
- $w_E = +1$, so $r_{an}(E)$ is even. Modular symbols show that $r_{an}(E) \neq 0$.
- $L''(E, 1) = 1.51863300057685\ldots$ (approximately), so $r_{an}(E) = 2$.
- $r(E) = 2$ by 2-descent, which finds generators $(0, -1)$ and $(-1, 1)$ with $\mathrm{Reg}(E) = 0.152460\ldots$, and also that $\text{Ш}(E/\mathbb{Q})[2] = 0$.
- $\Omega(E) = 4.980425\ldots$

A case with $r = 2$

- $E = 389a1 = [0, 1, 1, -2, 0]$ has conductor 389.
- $w_E = +1$, so $r_{an}(E)$ is even. Modular symbols show that $r_{an}(E) \neq 0$.
- $L''(E, 1) = 1.518633000576853\ldots$ (approximately), so $r_{an}(E) = 2$.
- $r(E) = 2$ by 2-descent, which finds generators $(0, -1)$ and $(-1, 1)$ with $\mathrm{Reg}(E) = 0.152460\ldots$, and also that $\text{Ш}(E/\mathbb{Q})[2] = 0$.
- $\Omega(E) = 4.980425\ldots$
- Hence $L''(E, 1)/(2!\Omega(E)\,\mathrm{Reg}(E)) = 1.0000000000\ldots$.

A case with $r = 2$

- $E = 389a1 = [0, 1, 1, -2, 0]$ has conductor 389.
- $w_E = +1$, so $r_{an}(E)$ is even. Modular symbols show that $r_{an}(E) \neq 0$.
- $L''(E, 1) = 1.518633000576851\ldots$ (approximately), so $r_{an}(E) = 2$.
- $r(E) = 2$ by 2-descent, which finds generators $(0, -1)$ and $(-1, 1)$ with $\mathrm{Reg}(E) = 0.152460\ldots$, and also that $\text{Ш}(E/\mathbb{Q})[2] = 0$.
- $\Omega(E) = 4.980425\ldots$
- Hence $L''(E, 1)/(2!\Omega(E)\,\mathrm{Reg}(E)) = 1.0000000000\ldots$.
  This is approximate: the ratio is *not* known to be rational!

A case with $r = 2$

- $E = 389a1 = [0, 1, 1, -2, 0]$ has conductor 389.
- $w_E = +1$, so $r_{an}(E)$ is even. Modular symbols show that $r_{an}(E) \neq 0$.
- $L''(E, 1) = 1.51863300057685\ldots$ (approximately), so $r_{an}(E) = 2$.
- $r(E) = 2$ by 2-descent, which finds generators $(0, -1)$ and $(-1, 1)$ with $\mathrm{Reg}(E) = 0.152460\ldots$, and also that $Ш(E/\mathbb{Q})[2] = 0$.
- $\Omega(E) = 4.980425\ldots$
- Hence $L''(E, 1)/(2!\Omega(E)\,\mathrm{Reg}(E)) = 1.0000000000\ldots$.
  This is approximate: the ratio is *not* known to be rational!
- We have $\prod c_p = 1$ and $\#E(\mathbb{Q})_{\mathrm{tors}} = 1$.

A case with $r = 2$

- $E = 389a1 = [0, 1, 1, -2, 0]$ has conductor 389.
- $w_E = +1$, so $r_{an}(E)$ is even. Modular symbols show that $r_{an}(E) \neq 0$.
- $L''(E, 1) = 1.51863300057685\ldots$ (approximately), so $r_{an}(E) = 2$.
- $r(E) = 2$ by 2-descent, which finds generators $(0, -1)$ and $(-1, 1)$ with $\mathrm{Reg}(E) = 0.152460\ldots$, and also that $Ш(E/\mathbb{Q})[2] = 0$.
- $\Omega(E) = 4.980425\ldots$
- Hence $L''(E, 1)/(2!\Omega(E)\,\mathrm{Reg}(E)) = 1.0000000000\ldots$. This is approximate: the ratio is *not* known to be rational!
- We have $\prod c_p = 1$ and $\#E(\mathbb{Q})_{\text{tors}} = 1$.
- BSD predicts that $\#Ш(E/\mathbb{Q}) = \frac{L''(E,1)/2\,\mathrm{Reg}(E)\Omega(E)}{\prod c_p/\#T^2} = 1$.

A case with $r = 2$

- $E = 389a1 = [0, 1, 1, -2, 0]$ has conductor 389.
- $w_E = +1$, so $r_{an}(E)$ is even. Modular symbols show that $r_{an}(E) \neq 0$.
- $L''(E, 1) = 1.51863300057685\ldots$ (approximately), so $r_{an}(E) = 2$.
- $r(E) = 2$ by 2-descent, which finds generators $(0, -1)$ and $(-1, 1)$ with $\mathrm{Reg}(E) = 0.152460\ldots$, and also that $Ш(E/\mathbb{Q})[2] = 0$.
- $\Omega(E) = 4.980425\ldots$
- Hence $L''(E, 1)/(2!\Omega(E)\,\mathrm{Reg}(E)) = 1.0000000000\ldots$.
  This is approximate: the ratio is *not* known to be rational!
- We have $\prod c_p = 1$ and $\#E(\mathbb{Q})_{\mathrm{tors}} = 1$.
- BSD predicts that $\#Ш(E/\mathbb{Q}) = \frac{L''(E,1)/2\,\mathrm{Reg}(E)\Omega(E)}{\prod c_p/\#T^2} = 1$.
- So BSD holds for E if $Ш(E/\mathbb{Q})[p] = 0$ for all odd p, *and*

A case with $r = 2$

- $E = 389a1 = [0, 1, 1, -2, 0]$ has conductor 389.
- $w_E = +1$, so $r_{an}(E)$ is even. Modular symbols show that $r_{an}(E) \neq 0$.
- $L''(E, 1) = 1.518633000576\,85\ldots$ (approximately), so $r_{an}(E) = 2$.
- $r(E) = 2$ by 2-descent, which finds generators $(0, -1)$ and $(-1, 1)$ with $\mathrm{Reg}(E) = 0.152460\ldots$, and also that $\text{Ш}(E/\mathbb{Q})[2] = 0$.
- $\Omega(E) = 4.980425\ldots$
- Hence $L''(E, 1)/(2!\Omega(E)\,\mathrm{Reg}(E)) = 1.0000000000\ldots$.
  This is approximate: the ratio is *not* known to be rational!
- We have $\prod c_p = 1$ and $\#E(\mathbb{Q})_{\text{tors}} = 1$.
- BSD predicts that $\#\text{Ш}(E/\mathbb{Q}) = \frac{L''(E,1)/2\,\mathrm{Reg}(E)\Omega(E)}{\prod c_p/\#T^2} = 1$.
- So BSD holds for E if $\text{Ш}(E/\mathbb{Q})[p] = 0$ for all odd p, *and* the above ratio is exactly 1.

A case with $r = 3$

- $E = 234446a1 = [1, 1, 0, -696, 6784]$ has conductor 234446.

A case with $r = 3$

- $E = 234446a1 = [1, 1, 0, -696, 6784]$ has conductor 234446.
- $w_E = -1$, so $r_{an}(E)$ is odd.

A case with $r = 3$

- $E = 234446a1 = [1, 1, 0, -696, 6784]$ has conductor 234446.
- $w_E = -1$, so $r_{an}(E)$ is odd.
- $|L'(E, 1)| < 10^{-22}$ so we suspect $r_{an}(E) \geq 3$.

A case with $r = 3$

- $E = 234446a1 = [1, 1, 0, -696, 6784]$ has conductor 234446.
- $w_E = -1$, so $r_{an}(E)$ is odd.
- $|L'(E, 1)| < 10^{-22}$ so we suspect $r_{an}(E) \geq 3$.
- $r(E) = 3$ by 2-descent, which finds generators $(15, -7)$, $(16, -16)$ and $(19, 20)$ with $\mathrm{Reg}(E) = 2.159011\ldots$, and also that $Ш(E/\mathbb{Q})[2] = 0$.

A case with $r = 3$

- $E = 234446a1 = [1, 1, 0, -696, 6784]$ has conductor 234446.
- $w_E = -1$, so $r_{an}(E)$ is odd.
- $|L'(E, 1)| < 10^{-22}$ so we suspect $r_{an}(E) \geq 3$.
- $r(E) = 3$ by 2-descent, which finds generators $(15, -7)$, $(16, -16)$ and $(19, 20)$ with $\mathrm{Reg}(E) = 2.159011\dots$, and also that $Ш(E/\mathbb{Q})[2] = 0$.
- So (Kolyvagin, Gross-Zagier) $r_{an}(E) > 1$. Now $L'''(E, 1) = 59.09365958\dots$ (approximately) implies $r_{an}(E) = 3$.

A case with $r = 3$

- $E = 234446a1 = [1, 1, 0, -696, 6784]$ has conductor 234446.
- $w_E = -1$, so $r_{an}(E)$ is odd.
- $|L'(E, 1)| < 10^{-22}$ so we suspect $r_{an}(E) \geq 3$.
- $r(E) = 3$ by 2-descent, which finds generators $(15, -7)$, $(16, -16)$ and $(19, 20)$ with $\mathrm{Reg}(E) = 2.159011\dots$, and also that $Ш(E/\mathbb{Q})[2] = 0$.
- So (Kolyvagin, Gross-Zagier) $r_{an}(E) > 1$. Now $L'''(E, 1) = 59.09365958\dots$ (approximately) implies $r_{an}(E) = 3$.
- $\Omega(E) = 2.2808923\dots$ and hence

A case with $r = 3$

- $E = 234446a1 = [1, 1, 0, -696, 6784]$ has conductor 234446.
- $w_E = -1$, so $r_{an}(E)$ is odd.
- $|L'(E, 1)| < 10^{-22}$ so we suspect $r_{an}(E) \geq 3$.
- $r(E) = 3$ by 2-descent, which finds generators $(15, -7)$, $(16, -16)$ and $(19, 20)$ with $\mathrm{Reg}(E) = 2.159011\ldots$, and also that $Ш(E/\mathbb{Q})[2] = 0$.
- So (Kolyvagin, Gross-Zagier) $r_{an}(E) > 1$. Now $L'''(E, 1) = 59.09365958\ldots$ (approximately) implies $r_{an}(E) = 3$.
- $\Omega(E) = 2.2808923\ldots$ and hence
- $L'''(E, 1)/(3!\Omega(E)\,\mathrm{Reg}(E)) = 2.0000000000\ldots$ (approximately).

A case with $r = 3$

- $E = 234446a1 = [1, 1, 0, -696, 6784]$ has conductor 234446.
- $w_E = -1$, so $r_{an}(E)$ is odd.
- $|L'(E, 1)| < 10^{-22}$ so we suspect $r_{an}(E) \geq 3$.
- $r(E) = 3$ by 2-descent, which finds generators $(15, -7)$, $(16, -16)$ and $(19, 20)$ with $\mathrm{Reg}(E) = 2.159011\ldots$, and also that $Ш(E/\mathbb{Q})[2] = 0$.
- So (Kolyvagin, Gross-Zagier) $r_{an}(E) > 1$. Now $L'''(E, 1) = 59.09365958\ldots$ (approximately) implies $r_{an}(E) = 3$.
- $\Omega(E) = 2.2808923\ldots$ and hence
- $L'''(E, 1)/(3!\Omega(E)\,\mathrm{Reg}(E)) = 2.0000000000\ldots$ (approximately).
- We have $\prod c_p = 2 \cdot 1 = 2$ and $\#E(\mathbb{Q})_{\mathrm{tors}} = 1$.

A case with $r = 3$

- $E = 234446a1 = [1, 1, 0, -696, 6784]$ has conductor 234446.
- $w_E = -1$, so $r_{an}(E)$ is odd.
- $|L'(E, 1)| < 10^{-22}$ so we suspect $r_{an}(E) \geq 3$.
- $r(E) = 3$ by 2-descent, which finds generators $(15, -7)$, $(16, -16)$ and $(19, 20)$ with $\mathrm{Reg}(E) = 2.159011\ldots$, and also that $Ш(E/\mathbb{Q})[2] = 0$.
- So (Kolyvagin, Gross-Zagier) $r_{an}(E) > 1$. Now $L'''(E, 1) = 59.09365958\ldots$ (approximately) implies $r_{an}(E) = 3$.
- $\Omega(E) = 2.2808923\ldots$ and hence
- $L'''(E, 1)/(3!\Omega(E)\,\mathrm{Reg}(E)) = 2.0000000000\ldots$ (approximately).
- We have $\prod c_p = 2 \cdot 1 = 2$ and $\#E(\mathbb{Q})_{\text{tors}} = 1$.
- BSD predicts that $\#Ш(E/\mathbb{Q}) = \frac{L'''(E,1)/6\,\mathrm{Reg}(E)\Omega(E)}{\prod c_p/\#T^2} = 1$.

A case with $r = 3$

- $E = 234446a1 = [1, 1, 0, -696, 6784]$ has conductor 234446.
- $w_E = -1$, so $r_{an}(E)$ is odd.
- $|L'(E, 1)| < 10^{-22}$ so we suspect $r_{an}(E) \geq 3$.
- $r(E) = 3$ by 2-descent, which finds generators $(15, -7)$, $(16, -16)$ and $(19, 20)$ with $\mathrm{Reg}(E) = 2.159011\ldots$, and also that $Ш(E/\mathbb{Q})[2] = 0$.
- So (Kolyvagin, Gross-Zagier) $r_{an}(E) > 1$. Now $L'''(E, 1) = 59.09365958\ldots$ (approximately) implies $r_{an}(E) = 3$.
- $\Omega(E) = 2.2808923\ldots$ and hence
- $L'''(E, 1)/(3!\Omega(E)\,\mathrm{Reg}(E)) = 2.0000000000\ldots$ (approximately).
- We have $\prod c_p = 2 \cdot 1 = 2$ and $\#E(\mathbb{Q})_{\mathrm{tors}} = 1$.
- BSD predicts that $\#Ш(E/\mathbb{Q}) = \frac{L'''(E,1)/6\,\mathrm{Reg}(E)\Omega(E)}{\prod c_p/\#T^2} = 1$.
- Again, BSD holds for E if $Ш(E/\mathbb{Q})[p] = 0$ for all odd p, and the above ratio is exactly 2.

A case with $r = 4$

- $E = 234446b1 = [1, -1, 0, -79, 289]$ also has conductor 234446.

A case with $r = 4$

- $E = 234446b1 = [1, -1, 0, -79, 289]$ also has conductor 234446.
- $w_E = +1$, so $r_{an}(E)$ is even, and positive (modular symbols).

A case with $r = 4$

- $E = 234446b1 = [1, -1, 0, -79, 289]$ also has conductor 234446.
- $w_E = +1$, so $r_{an}(E)$ is even, and positive (modular symbols).
- $|L''(E, 1)| < 10^{-21}$ so we suspect $r_{an}(E) \geq 4$.

A case with $r = 4$

- $E = 234446b1 = [1, -1, 0, -79, 289]$ also has conductor 234446.
- $w_E = +1$, so $r_{an}(E)$ is even, and positive (modular symbols).
- $|L''(E, 1)| < 10^{-21}$ so we suspect $r_{an}(E) \geq 4$.
- $r(E) = 4$ by 2-descent, which finds generators $(-9, 19)$, $(-8, 23)$, $(-7, 25)$ and $(4, -7)$ with $\mathrm{Reg}(E) = 1.5043\ldots$, and also that $Ш(E/\mathbb{Q})[2] = 0$.

A case with $r = 4$

- $E = 234446b1 = [1, -1, 0, -79, 289]$ also has conductor 234446.
- $w_E = +1$, so $r_{an}(E)$ is even, and positive (modular symbols).
- $|L''(E, 1)| < 10^{-21}$ so we suspect $r_{an}(E) \geq 4$.
- $r(E) = 4$ by 2-descent, which finds generators $(-9, 19)$, $(-8, 23)$, $(-7, 25)$ and $(4, -7)$ with $\mathrm{Reg}(E) = 1.5043\ldots$, and also that $Ш(E/\mathbb{Q})[2] = 0$.
- If $L''(E, 1) = 0$ exactly, then $L^{(4)}(E, 1) = 214.6523375\ldots$ (approximately) and $r_{an}(E) = 4$; but we cannot show that $r_{an}(E) \neq 2$!

A case with $r = 4$

- $E = 234446b1 = [1, -1, 0, -79, 289]$ also has conductor 234446.
- $w_E = +1$, so $r_{an}(E)$ is even, and positive (modular symbols).
- $|L''(E, 1)| < 10^{-21}$ so we suspect $r_{an}(E) \geq 4$.
- $r(E) = 4$ by 2-descent, which finds generators $(-9, 19)$, $(-8, 23)$, $(-7, 25)$ and $(4, -7)$ with $\mathrm{Reg}(E) = 1.5043\ldots$, and also that $Ш(E/\mathbb{Q})[2] = 0$.
- If $L''(E, 1) = 0$ exactly, then $L^{(4)}(E, 1) = 214.6523375\ldots$ (approximately) and $r_{an}(E) = 4$; but we cannot show that $r_{an}(E) \neq 2$!
- $\Omega(E) = 2.97267\ldots$

A case with $r = 4$

- $E = 234446b1 = [1, -1, 0, -79, 289]$ also has conductor 234446.
- $w_E = +1$, so $r_{an}(E)$ is even, and positive (modular symbols).
- $|L''(E, 1)| < 10^{-21}$ so we suspect $r_{an}(E) \geq 4$.
- $r(E) = 4$ by 2-descent, which finds generators $(-9, 19)$, $(-8, 23)$, $(-7, 25)$ and $(4, -7)$ with $\mathrm{Reg}(E) = 1.5043\ldots$, and also that $Ш(E/\mathbb{Q})[2] = 0$.
- If $L''(E, 1) = 0$ exactly, then $L^{(4)}(E, 1) = 214.6523375\ldots$ (approximately) and $r_{an}(E) = 4$; but we cannot show that $r_{an}(E) \neq 2$!
- $\Omega(E) = 2.97267\ldots$
- $L^{(4)}(E, 1)/(4!\Omega(E)\,\mathrm{Reg}(E)) = 2.0000000000\ldots$ (approximately).

A case with $r = 4$

- $E = 234446b1 = [1, -1, 0, -79, 289]$ also has conductor 234446.
- $w_E = +1$, so $r_{an}(E)$ is even, and positive (modular symbols).
- $|L''(E, 1)| < 10^{-21}$ so we suspect $r_{an}(E) \geq 4$.
- $r(E) = 4$ by 2-descent, which finds generators $(-9, 19)$, $(-8, 23)$, $(-7, 25)$ and $(4, -7)$ with $\mathrm{Reg}(E) = 1.5043\ldots$, and also that $Ш(E/\mathbb{Q})[2] = 0$.
- If $L''(E, 1) = 0$ exactly, then $L^{(4)}(E, 1) = 214.6523375\ldots$ (approximately) and $r_{an}(E) = 4$; but we cannot show that $r_{an}(E) \neq 2$!
- $\Omega(E) = 2.97267\ldots$
- $L^{(4)}(E, 1)/(4!\Omega(E)\,\mathrm{Reg}(E)) = 2.0000000000\ldots$ (approximately).
- $\prod c_p = 2 \cdot 1 = 2$ and $\#E(\mathbb{Q})_{\mathrm{tors}} = 1$.

A case with $r = 4$

- $E = 234446b1 = [1, -1, 0, -79, 289]$ also has conductor 234446.
- $w_E = +1$, so $r_{an}(E)$ is even, and positive (modular symbols).
- $|L''(E, 1)| < 10^{-21}$ so we suspect $r_{an}(E) \geq 4$.
- $r(E) = 4$ by 2-descent, which finds generators $(-9, 19)$, $(-8, 23)$, $(-7, 25)$ and $(4, -7)$ with $\operatorname{Reg}(E) = 1.5043\ldots$, and also that $Ш(E/\mathbb{Q})[2] = 0$.
- If $L''(E, 1) = 0$ exactly, then $L^{(4)}(E, 1) = 214.6523375\ldots$ (approximately) and $r_{an}(E) = 4$; but we cannot show that $r_{an}(E) \neq 2$!
- $\Omega(E) = 2.97267\ldots$
- $L^{(4)}(E, 1)/(4!\Omega(E) \operatorname{Reg}(E)) = 2.0000000000\ldots$ (approximately).
- $\prod c_p = 2 \cdot 1 = 2$ and $\#E(\mathbb{Q})_{\text{tors}} = 1$.
- BSD predicts that $\#Ш(E/\mathbb{Q}) = \frac{L^{(4)}(E,1)/24 \operatorname{Reg}(E)\Omega(E)}{\prod c_p/\#T^2} = 1$.

A case with $r = 4$

- $E = 234446b1 = [1, -1, 0, -79, 289]$ also has conductor 234446.
- $w_E = +1$, so $r_{an}(E)$ is even, and positive (modular symbols).
- $|L''(E, 1)| < 10^{-21}$ so we suspect $r_{an}(E) \geq 4$.
- $r(E) = 4$ by 2-descent, which finds generators $(-9, 19)$, $(-8, 23)$, $(-7, 25)$ and $(4, -7)$ with $\mathrm{Reg}(E) = 1.5043\ldots$, and also that $Ш(E/\mathbb{Q})[2] = 0$.
- If $L''(E, 1) = 0$ exactly, then $L^{(4)}(E, 1) = 214.6523375\ldots$ (approximately) and $r_{an}(E) = 4$; but we cannot show that $r_{an}(E) \neq 2$!
- $\Omega(E) = 2.97267\ldots$
- $L^{(4)}(E, 1)/(4!\Omega(E)\,\mathrm{Reg}(E)) = 2.0000000000\ldots$ (approximately).
- $\prod c_p = 2 \cdot 1 = 2$ and $\#E(\mathbb{Q})_{\mathrm{tors}} = 1$.
- BSD predicts that $\#Ш(E/\mathbb{Q}) = \frac{L^{(4)}(E,1)/24\,\mathrm{Reg}(E)\Omega(E)}{\prod c_p/\#T^2} = 1$.
- Again, BSD holds for E if $L''(E, 1) = 0$, $Ш(E/\mathbb{Q})[p] = 0$ for all odd p, and the above ratio is exactly 2.

Summary for curves in the database

My database currently contains all elliptic curves E of conductor $N_E < 140000$, and for each one it gives all the numbers which appear in the BSD formula, with the "analytic order of $Ш$", $Ш_{an}(E/\mathbb{Q})$, in place of $|Ш(E/\mathbb{Q})|$. This is just the value predicted by BSD, rounded.

Summary for curves in the database

My database currently contains all elliptic curves E of conductor $N_E < 140000$, and for each one it gives all the numbers which appear in the BSD formula, with the "analytic order of Ш", $Ш_{an}(E/\mathbb{Q})$, in place of $|Ш(E/\mathbb{Q})|$. This is just the value predicted by BSD, rounded.

In all cases $Ш_{an}(E/\mathbb{Q})$ is an integer (when $r_{an}(E) = 0$) or approximately an integer (when $r_{an}(E) \geq 1$), and the integer is a square.

Summary for curves in the database

My database currently contains all elliptic curves E of conductor $N_E < 140000$, and for each one it gives all the numbers which appear in the BSD formula, with the "analytic order of Ш", $Ш_{an}(E/\mathbb{Q})$, in place of $|Ш(E/\mathbb{Q})|$. This is just the value predicted by BSD, rounded.

In all cases $Ш_{an}(E/\mathbb{Q})$ is an integer (when $r_{an}(E) = 0$) or approximately an integer (when $r_{an}(E) \geq 1$), and the integer is a square.

The value is 1 in 93.31% of the cases, including all the curves of rank greater than 1.

Summary for curves in the database

My database currently contains all elliptic curves E of conductor $N_E < 140000$, and for each one it gives all the numbers which appear in the BSD formula, with the “analytic order of Ш”, $Ш_{an}(E/\mathbb{Q})$, in place of $|Ш(E/\mathbb{Q})|$. This is just the value predicted by BSD, rounded.

In all cases $Ш_{an}(E/\mathbb{Q})$ is an integer (when $r_{an}(E) = 0$) or approximately an integer (when $r_{an}(E) \geq 1$), and the integer is a square.

The value is 1 in 93.31% of the cases, including all the curves of rank greater than 1.

The largest value is $784 = 28^2$, for
$138437c1 = [1, 1, 0, -6193920002885, -5933305228440879554]$
(which has $E(\mathbb{Q}) = 0$).

Summary for curves in the database

My database currently contains all elliptic curves E of conductor $N_E < 140000$, and for each one it gives all the numbers which appear in the BSD formula, with the “analytic order of Ш”, $Ш_{an}(E/\mathbb{Q})$, in place of $|Ш(E/\mathbb{Q})|$. This is just the value predicted by BSD, rounded.

In all cases $Ш_{an}(E/\mathbb{Q})$ is an integer (when $r_{an}(E) = 0$) or approximately an integer (when $r_{an}(E) \geq 1$), and the integer is a square.

The value is 1 in 93.31% of the cases, including all the curves of rank greater than 1.

The largest value is $784 = 28^2$, for $138437c1 = [1, 1, 0, -6193920002885, -5933305228440879554]$ (which has $E(\mathbb{Q}) = 0$).

All primes up to 23 appear as factors.

Some details of the modular symbol contribution

Let f_E be the newform in $S_2(N)$ attached to E.

Some details of the modular symbol contribution

Let f_E be the newform in $S_2(N)$ attached to E.

For $\alpha, \beta \in \mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$, let $\{\alpha, \beta\}$ denote a geodesic path from α to β, and $\langle\{\alpha, \beta\}, f\rangle = \int_\alpha^\beta 2\pi i f(z) dz$.

Some details of the modular symbol contribution

Let f_E be the newform in $S_2(N)$ attached to E.

For $\alpha, \beta \in \mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$, let $\{\alpha, \beta\}$ denote a geodesic path from α to β, and $\langle\{\alpha, \beta\}, f\rangle = \int_\alpha^\beta 2\pi i f(z) dz$.

We have $L(E, 1) = L(f_E, 1) = \langle\{\infty, 0\}, f\rangle$.

Some details of the modular symbol contribution

Let f_E be the newform in $S_2(N)$ attached to E.

For $\alpha, \beta \in \mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$, let $\{\alpha, \beta\}$ denote a geodesic path from α to β, and $\langle\{\alpha, \beta\}, f\rangle = \int_\alpha^\beta 2\pi i f(z) dz$.

We have $L(E, 1) = L(f_E, 1) = \langle\{\infty, 0\}, f\rangle$.

The Hecke operator T_p satisfies
$\langle T_p\{\alpha, \beta\}, f\rangle = \langle\{\alpha, \beta\}, T_p f\rangle = \langle\{\alpha, \beta\}, a_p f\rangle = a_p \langle\{\alpha, \beta\}, f\rangle$.

Some details of the modular symbol contribution

Let f_E be the newform in $S_2(N)$ attached to E.

For $\alpha, \beta \in \mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$, let $\{\alpha, \beta\}$ denote a geodesic path from α to β, and $\langle \{\alpha, \beta\}, f \rangle = \int_\alpha^\beta 2\pi i f(z) dz$.

We have $L(E,1) = L(f_E, 1) = \langle \{\infty, 0\}, f \rangle$.

The Hecke operator T_p satisfies
$\langle T_p\{\alpha, \beta\}, f \rangle = \langle \{\alpha, \beta\}, T_p f \rangle = \langle \{\alpha, \beta\}, a_p f \rangle = a_p \langle \{\alpha, \beta\}, f \rangle$.

Applying this with $\{\alpha, \beta\} = \{\infty, 0\}$, where
$(T_p - p - 1)\{\infty, 0\} = \sum_x \{0, x/p\}$ we find that

$$(1 + p - a_p) L(E,1) = n_p \Omega(E)$$

for some $n_p \in \mathbb{Z}$. Hence

$$\frac{L(E,1)}{\Omega(E)} = \frac{n_p}{1 + p - a_p} \in \mathbb{Q}.$$

Example: $N = 11$

Let $E = 11a1$.

$\Omega(E) = \langle \{\frac{1}{2}, 0\}, f \rangle$.

From $T_2\{\infty, 0\} = \left(\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \right) \{\infty, 0\} =$
$\{\infty, 0\} + \{\infty, 0\} + \{\infty, \frac{1}{2}\} = 3\{\infty, 0\} + \{0, \frac{1}{2}\}$, it follows that
$(3 - a_2)L(E, 1) = \Omega(E)$.

But $a_2 = -2$, so $L(E, 1)/\Omega(E) = 1/5$.