Verifying some consequences of the Birch Swinnerton-Dyer Conjecture

Felipe Jacob

University College London

2017

Elliptic Curves

In this project we will be considering the arithmetic properties of **elliptic curves** $E(K)$. These are given by the set of points (x, y) with x and y in the field K such that

$$E : y^2 = f(x),$$

where $f(x)$ is a cubic polynomial with 3 distint roots.

Elliptic Curves

We always assume that we have a known point $\mathcal{O} \in E(K)$ in the projective completion $\mathbb{P}^2(K)$, which is called the **point at infinity of** E.

Elliptic Curves

We always assume that we have a known point $\mathcal{O} \in E(K)$ in the projective completion $\mathbb{P}^2(K)$, which is called the **point at infinity of** E.

When K doesn't have characteristic 2, we can assume that the curve is given by the equation

$$y^2 = x^3 + ax^2 + bx + c,$$

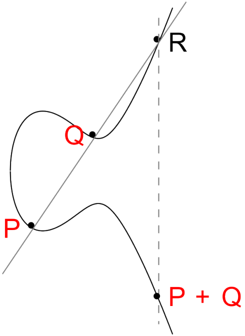
with $a, b, c \in K$, and that $\mathcal{O} = (0 : 1 : 0)$.

Group Law

Elliptic curves are interesting because on top of being a variety, they also form an abelian group. To add two distinct points P, Q, we trace the line between them and let R be the third point of intersection of this line with the curve. $P + Q$ is then the reflection of R over the x-axis.

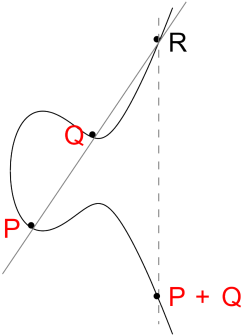
Group Law

Elliptic curves are interesting because on top of being a variety, they also form an abelian group. To add two distinct points P, Q, we trace the line between them and let R be the third point of intersection of this line with the curve. $P + Q$ is then the reflection of R over the x-axis.



Group Law

Elliptic curves are interesting because on top of being a variety, they also form an abelian group. To add two distinct points P, Q, we trace the line between them and let R be the third point of intersection of this line with the curve. $P + Q$ is then the reflection of R over the x-axis.



Under this addition, it turns out that $E(K)$ is an abelian group.

Quadratic Twists

The curves we will be interested in this project are given by

$$E_n : y^2 = x^3 - n^2 x,$$

where n is odd and squarefree.

Quadratic Twists

The curves we will be interested in this project are given by

$$E_n : y^2 = x^3 - n^2 x,$$

where n is odd and squarefree.
They are notorious for their relation with Fermat and the congruent number problem.

The Rank

The Mordell-Weil Theorem states that when $K = \mathbb{Q}$, the group $E(\mathbb{Q})$ is finitely generated. This means that we can write

$$E(\mathbb{Q}) \simeq \mathrm{Tors}(E(\mathbb{Q})) \times \mathbb{Z}^r,$$

where $\mathrm{Tors}(E(\mathbb{Q}))$ are the points of finite order, and r is a natural number, called the **rank of** E.

The Rank

The Mordell-Weil Theorem states that when $K = \mathbb{Q}$, the group $E(\mathbb{Q})$ is finitely generated. This means that we can write

$$E(\mathbb{Q}) \simeq \mathrm{Tors}(E(\mathbb{Q})) \times \mathbb{Z}^r,$$

where $\mathrm{Tors}(E(\mathbb{Q}))$ are the points of finite order, and r is a natural number, called the **rank of** E.

Computing $\mathrm{Tors}(E(\mathbb{Q}))$ is easy, but finding r for arbitrary curves is very much an open problem. In this presentation we will discuss a few techniques used in such computations.

The BSD Conjecture

The Birch Swinnerton-Dyer Conjecture relates the rank r of an elliptic curve E to the order of a zero of a certain analytic function.

The BSD Conjecture

The Birch Swinnerton-Dyer Conjecture relates the rank r of an elliptic curve E to the order of a zero of a certain analytic function. More precisely, it says that

$$L(E, s) = C(s-1)^r + O((s-1)^{r+1}),$$

where $L(E, s)$ is an analytic function called the **Hasse-Weil L-function of** E. We will see how to construct it.

Local Zeta Functions

Let p be a prime number. If V is a variety over $\mathbb{F}_p$, we can construct the **Local Zeta Functions of** V **at** p, given by

$$Z(V,p,s) = \exp\left(\sum_{k=1}^{\infty} \#V(\mathbb{F}_{p^k})\frac{z^k}{k}\right).$$

Local Zeta Functions

Let p be a prime number. If V is a variety over $\mathbb{F}_p$, we can construct the **Local Zeta Functions of V at p**, given by

$$Z(V, p, s) = \exp\left(\sum_{k=1}^{\infty} \# V(\mathbb{F}_{p^k}) \frac{z^k}{k}\right).$$

These capture the behaviour of V in all finite fields of p^k elements.

Local Zeta Functions

As an example, if V is a point, then $\#V(\mathbb{F}_{p^k}) = 1$, so we get

$$Z(V,p,s) = \exp\left(\sum_{k=1}^{\infty} \frac{z^k}{k}\right) = \exp\left(-\log(1-z)\right) = \frac{1}{1-z}$$

Local Zeta Functions

As an example, if V is a point, then $\#V(\mathbb{F}_{p^k}) = 1$, so we get

$$Z(V,p,s) = \exp\left(\sum_{k=1}^{\infty} \frac{z^k}{k}\right) = \exp\left(-\log(1-z)\right)$$
$$= \frac{1}{1-z}$$

Similarly, if $V = \mathbb{P}^n$, we know that $\#V(\mathbb{F}_{p^k}) = 1 + p^k + \cdots + p^{nk}$, so we get

$$Z(V,p,z) = \frac{1}{1-z}\frac{1}{1-pz}\cdots\frac{1}{1-p^n z}$$

Hasse-Weil L-Function

To form the **Hasse-Weil L-function of** V, we multiply the local zeta functions of V for all different primes:

$$L(V, s) = \prod_p Z(V, p, p^{-s}).$$

Hasse-Weil L-Function

To form the **Hasse-Weil L-function of** V, we multiply the local zeta functions of V for all different primes:

$$L(V, s) = \prod_p Z(V, p, p^{-s}).$$

This function captures the behaviour of V at all possible finite fields.

Hasse-Weil L-function

For the case where V is a point, we get

$$L(V, s) = \prod_p \frac{1}{1 - p^{-s}} = \zeta(s)$$

which is the classical Riemann-Zeta function.

Hasse-Weil L-function

For the case where V is a point, we get

$$L(V,s) = \prod_p \frac{1}{1-p^{-s}} = \zeta(s)$$

which is the classical Riemann-Zeta function.
If $V = \mathbb{P}^n$ we instead get

$$L(V,s) = \zeta(s)\zeta(s-1)\cdots\zeta(s-n).$$

Hasse-Weil L-function

For the family of elliptic curves E_n, the Hasse-Weil L-function takes the form

$$L(E_n, s) = \prod_{p \nmid 2n} \frac{1}{1 - 2a_{n,p}p^{-s} + p^{1-2s}},$$

where the $a_{n,p}$ are certain integers depending on n and p.

Full BSD

The full BSD conjecture also relates the constant C in the prediction

$$L(E, s) = C(s-1)^r + O((s-1)^{r+1})$$

to certain arithmetic invariants of E.

Full BSD

The full BSD conjecture also relates the constant C in the prediction

$$L(E,s) = C(s-1)^r + O((s-1)^{r+1})$$

to certain arithmetic invariants of E.

In particular, it states that

$$C = \frac{\#\mathrm{Sha}(E) R_E \Omega_E}{\#\mathrm{Tors}(E)^2} \prod_p c_p$$

where we will define each of these quantities.

Tate-Shafarevich Group

The group $\mathrm{Sha}(E)$ is called the **Tate-Shafarevich group of** E. It is an abelian group, conjectured to be finite, and measures in some sense how hard it is to find the rank by local methods.

Tate-Shafarevich Group

The group Sha(E) is called the **Tate-Shafarevich group of** E. It is an abelian group, conjectured to be finite, and measures in some sense how hard it is to find the rank by local methods.

The full definition requires the machinery of Galois Cohomology, and takes the form

$$\mathrm{Sha}(E) = \mathrm{Ker}\left(H^1(\mathbb{Q}, \bar{E}) \to \prod_{\nu} H^1(\mathbb{Q}_\nu, \bar{E}) \right).$$

Regulator

The **regulator of** E measures in a specific sense the volume of a set of generators of E.

Regulator

The **regulator of** E measures in a specific sense the volume of a set of generators of E.

It is defined by

$$R_E = \det\left(\langle P_i, P_j\rangle\right)$$

where $P_1, \ldots, P_r$ is a basis for $\frac{E(\mathbb{Q})}{\mathrm{Tors}(E(\mathbb{Q}))}$ and $\langle\cdot\rangle$ is an inner product on $E(\mathbb{Q})$ called the Neron-Tate pairing.

Real Period

The **real period of E** is given by the line integral

$$\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{2y}.$$

For the curves E_n, we have

$$\Omega_{E_n} = \frac{2}{\sqrt{n}}\beta,$$

where $\beta = \int_1^\infty \frac{dx}{\sqrt{x^3-x}} \approx 2.622.$

Tamagawa Numbers

The **Tamagawa Numbers** $c_p(E)$ capture the behaviour of E at the primes where it has bad reduction. If E is given by

$$E : y^2 = f(x)$$

and the polynomial $f(x)$ still has 3 distinct roots in $\mathbb{F}_p$, we say that E has good reduction at p. In this case there is a homomorphism of curves

$$E(\mathbb{Q}) \to E(\mathbb{F}_p)$$

given by reduction modulo p.

Tamagawa Numbers

If $\Delta(f) \equiv 0\,(p)$, the reduction map may no longer be a homomorphism. The situation can still be salvaged, however.

Tamagawa Numbers

If $\Delta(f) \equiv 0\,(p)$, the reduction map may no longer be a homomorphism. The situation can still be salvaged, however.

Let $E(\mathbb{F}_p)_{ns}$ be the set of points (x, y) where $E(\mathbb{F}_p)$ is nonsingular. Looking at the completion $\mathbb{Q}_p$ we still have a map

$$E(\mathbb{Q}_p) \to E(\mathbb{F}_p).$$

Tamagawa Numbers

If $\Delta(f) \equiv 0\,(p)$, the reduction map may no longer be a homomorphism. The situation can still be salvaged, however.

Let $E(\mathbb{F}_p)_{ns}$ be the set of points (x, y) where $E(\mathbb{F}_p)$ is nonsingular. Looking at the completion $\mathbb{Q}_p$ we still have a map

$$E(\mathbb{Q}_p) \to E(\mathbb{F}_p).$$

If we let $E(\mathbb{Q}_p)_0$ be the preimages of the nonsingular points, then the restriction

$$E(\mathbb{Q}_p)_0 \to E(\mathbb{F}_p)_{ns}$$

is still a homomorphism.

Tamagawa Numbers

The Tamagawa Numbers c_p of E are defined by

$$c_p = \left| \frac{E(\mathbb{Q}_p)}{E(\mathbb{Q}_p)_0} \right|.$$

They measure the number of singular components of E. This is usually a power of 2.

Tamagawa Numbers

The Tamagawa Numbers c_p of E are defined by

$$c_p = \left| \frac{E(\mathbb{Q}_p)}{E(\mathbb{Q}_p)_0} \right|.$$

They measure the number of singular components of E. This is usually a power of 2.

Theorem

In the project, we calculated that for n odd and squarefree, we have

$$\prod_p c_p(E_n) = 2 \cdot 4^{\omega(n)},$$

where $\omega(n)$ is the number of distinct prime factors of n.

The situation so far

From the information we currently have, the situation seems pretty hopeless. On the one hand we have $L(E_n, s)$ given by a complicated product. On the other we have a constant C that involves the transcendental number β and lots invariants of E_n.

The situation so far

From the information we currently have, the situation seems pretty hopeless. On the one hand we have $L(E_n, s)$ given by a complicated product. On the other we have a constant C that involves the transcendental number β and lots invariants of E_n.

The way forward is given by **Tunnell's Theorem**, a very deep result coming from the theory of Modular Forms, and which will allow us to compute $L(E_n, s)$ more explicitly.

Tunnell's Theorem

Let $\Theta(z) = \sum_{m \in \mathbb{Z}} q^{m^2}$ where $q = e^{2\pi i z}$ be the Theta function.

Tunnell's Theorem

Let $\Theta(z) = \sum_{m \in \mathbb{Z}} q^{m^2}$ where $q = e^{2\pi i z}$ be the Theta function.

Theorem (Tunnell's Theorem)

For n odd, the critical values $L(E_n, 1)$ are given by

$$L(E_n, 1) = \frac{\beta}{4\sqrt{n}} a_n^2.$$

Here a_n are the Fourier coefficents of the function

$$f(z) = \sum_{m \in \mathbb{Z}} a_m q^m = \Theta(z) \left(\Theta(32z) - \frac{1}{2}\Theta(8z) \right) \Theta(2z)$$

BSD Revisited

Here we are lucky to have the same β occuring on both sides of the BSD conjecture:

$$L(s, 1) = \frac{\#\mathrm{Sha}(E_n) R_{E_n} \Omega_{E_n}}{\#\mathrm{Tors}(E(\mathbb{Q}))^2}$$

becomes, at $s = 1$:

BSD Revisited

Here we are lucky to have the same β occuring on both sides of the BSD conjecture:

$$L(s,1) = \frac{\#\mathrm{Sha}(E_n) R_{E_n} \Omega_{E_n}}{\#\mathrm{Tors}(E(\mathbb{Q}))^2}$$

becomes, at $s = 1$:

$$\frac{\beta}{4\sqrt{n}} a_n^2 = \frac{\#\mathrm{Sha}(E_n) R_{E_n} 2\beta}{16\sqrt{n}} \cdot 2 \cdot 4^{\omega(n)} \cdot 0^r,$$

BSD Revisited

Here we are lucky to have the same β occuring on both sides of the BSD conjecture:

$$L(s,1) = \frac{\#\mathrm{Sha}(E_n) R_{E_n} \Omega_{E_n}}{\#\mathrm{Tors}(E(\mathbb{Q}))^2}$$

becomes, at $s = 1$:

$$\frac{\beta}{4\sqrt{n}} a_n^2 = \frac{\#\mathrm{Sha}(E_n) R_{E_n} 2\beta}{16\sqrt{n}} \cdot 2 \cdot 4^{\omega(n)} \cdot 0^r,$$

which simplifies to

$$a_n^2 = \#\mathrm{Sha}(E_n) \cdot R_{E_n} \cdot 4^{\omega(n)} \cdot 0^r.$$

BSD Revisited

We have

$$a_n^2 = \#\mathrm{Sha}(E_n) \cdot R_{E_n} \cdot 4^{\omega(n)} \cdot 0^r.$$

Since when the rank is nonzero, the BSD conjecture says nothing interesting about the right hand side, we will assume $r = 0$. In this case $R_{E_n} = 1$, so this further simplifies to

$$a_n^2 = 4^{\omega(n)} \#\mathrm{Sha}(E_n).$$

BSD Revisited

We have

$$a_n^2 = \#\mathrm{Sha}(E_n) \cdot R_{E_n} \cdot 4^{\omega(n)} \cdot 0^r.$$

Since when the rank is nonzero, the BSD conjecture says nothing interesting about the right hand side, we will assume $r = 0$. In this case $R_{E_n} = 1$, so this further simplifies to

$$a_n^2 = 4^{\omega(n)} \#\mathrm{Sha}(E_n).$$

This is now an equation of **integers**, so we can hope to use some number theory to show it is true. In the project we were able to prove that it indeed holds at least modulo 16.

Outline of Calculations

In order to verify that

$$a_n^2 \equiv 4^{\omega(n)} \# \mathrm{Sha}(E_n) \mod 16 \tag{1}$$

we

- Worked out the coefficients a_n modulo 4. This turns out to depend on n modulo 8.
- Found the Selmer Group of E_n, a computable complement of $\mathrm{Sha}(E_n)$. This also depends on n modulo 8.
- Matched both informations with Equation 1 for each residue class of n modulo 8.

Calculation of Coefficients of Theta Series

Recall that we want to compute the integers a_m modulo 4, where

$$f(z) = \sum_{m \in \mathbb{Z}} a_m q^m = \Theta(z) \left(\Theta(32z) - \frac{1}{2}\Theta(8z) \right) \Theta(2z).$$

Calculation of Coefficients of Theta Series

Recall that we want to compute the integers a_m modulo 4, where

$$f(z) = \sum_{m\in\mathbb{Z}} a_m q^m = \Theta(z)\left(\Theta(32z) - \frac{1}{2}\Theta(8z)\right)\Theta(2z).$$

But this is equivalent to

$$f(z) = \sum_{x,y,z\in\mathbb{Z}} q^{2x^2+y^2+32z^2} - \frac{1}{2}\sum_{x,y,z\in\mathbb{Z}} q^{2x^2+y^2+8z^2}.$$

Calculation of Coefficients of Theta Series

In other words, we want to know among the solutions to

$$2x^2 + y^2 + 8z^2 = n$$

how many are also solutions to

$$2x^2 + y^2 + 32z^2 = n.$$

Since we only want this mod 4, we can use many tricks.

Calculation of Selmer Group

To calculate the Selmer group, we saw in MATH3703 that we have to solve a bunch of equations of the form

$$N^2 = d_1 M^4 + \frac{4n^2}{d_1} e^4$$

in $\mathbb{Q}_p$ for each prime p.

Calculation of Selmer Group

To calculate the Selmer group, we saw in MATH3703 that we have to solve a bunch of equations of the form

$$N^2 = d_1 M^4 + \frac{4n^2}{d_1} e^4$$

in $\mathbb{Q}_p$ for each prime p.

This can be done by some extensive applications of quadratic reciprocity together with Hensel's lemma.

Conclusion

From our calculations we deduced that if p is an odd prime,

$$a_p \equiv \begin{cases} 0 \mod 4 & \text{if } p \equiv 1, 5, 7 \mod 8 \\ 2 \mod 4 & \text{if } p \equiv 3 \mod 8 \end{cases}$$

and $a_n \equiv 0\,(4)$ if n is composite.

Conclusion

From our calculations we deduced that if p is an odd prime,

$$a_p \equiv \begin{cases} 0 \mod 4 & \text{if } p \equiv 1, 5, 7 \mod 8 \\ 2 \mod 4 & \text{if } p \equiv 3 \mod 8 \end{cases}$$

and $a_n \equiv 0\,(4)$ if n is composite.

We also found that $\mathrm{Sha}(E_p)$ has an element of 2-torsion if and only if $p \not\equiv 3\,(8)$.

Conclusion

From our calculations we deduced that if p is an odd prime,

$$a_p \equiv \begin{cases} 0 \mod 4 & \text{if } p \equiv 1, 5, 7 \mod 8 \\ 2 \mod 4 & \text{if } p \equiv 3 \mod 8 \end{cases}$$

and $a_n \equiv 0\,(4)$ if n is composite.

We also found that $\mathrm{Sha}(E_p)$ has an element of 2-torsion if and only if $p \not\equiv 3\,(8)$.

Putting both results together gives

$$a_n^2 \equiv 4^{\omega(n)} \# \mathrm{Sha}(E_n) \mod 16,$$

verifying the Birch Swinnerton-Dyer conjecture modulo 16, as wanted.