Verifying some consequences of the Birch Swinnerton-Dyer Conjecture

Author: Felipe Jacob
Supervisor: Dr Richard Hill

University College London

March 22, 2017

Elliptic Curves

An **Elliptic Curve over a field** K is a projective variety E where

- E is a cubic curve over $\mathbb{P}^2(K)$
- E is nonsingular over K
- There exists a distinguished $\mathcal{O} \in E(K)$ called the **point at infinity**.

Elliptic Curves

An **Elliptic Curve over a field** K is a projective variety E where

- E is a cubic curve over $\mathbb{P}^2(K)$
- E is nonsingular over K
- There exists a distinguished $\mathcal{O} \in E(K)$ called the **point at infinity**.

Example: $E : y^2z = x^3 - xz^2$ is an elliptic curve over $\mathbb{Q}$ with $\mathcal{O} = (0 : 1 : 0)$

Elliptic Curves

If $\mathrm{char}(K) \neq 2$, we can assume E has the affine model

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

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

Group Law

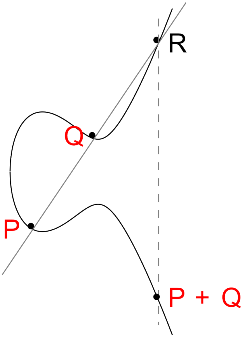
Actually, $E(K)$ has a natural addition law.

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

Actually, $E(K)$ has a natural addition law.

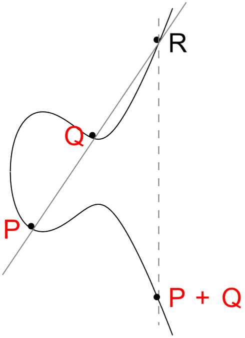
To add two distinct points P, Q, we trace the line between them and let R be the third point of intersection of this line with the curve. $P + Q$ is then the reflection of R over the x-axis.



Group Law

Actually, $E(K)$ has a natural addition law.

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 the operation $+$, it turns out $E(K)$ is an abelian group, with $0 = \mathcal{O}$.

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, Gauss and the congruent number problem.

The Rank I

Theorem 1 (Mordell-Weil)

Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is finitely generated.

The Rank I

Theorem 1 (Mordell-Weil)

Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is finitely generated.

This means we can write

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

where

- $\mathrm{Tors}(E(\mathbb{Q}))$ is finite.
- r is a natural number called the **rank of** E.

The Rank II

Theorem 2

Our curves

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

have 4 points of finite order: $\mathrm{Tors}(E(\mathbb{Q})) = \{\mathcal{O}, (0,0), (n,0), (-n,0)\}$.

The Rank II

Theorem 2

Our curves

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

have 4 points of finite order: $\mathrm{Tors}(E(\mathbb{Q})) = \{\mathcal{O}, (0,0), (n,0), (-n,0)\}$.

Finding r, however, is **hard**.

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 I

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

$$Z(v,p,z) = \prod_{M \triangleleft C_E} \frac{1}{1-||M||^{-z}}$$

where M are the maximal ideals of $C_E := \frac{\mathbb{F}_p[x,y]}{E}$

Local Zeta Functions II

We also have the computational formula

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

so we get Z from knowing how many points E has in at every finite field of p^k elements.

Local Zeta Functions III

Example: If $V = (x_0, y_0)$ is a point, then $\#V(\mathbb{F}_{p^k}) = 1$, so we get

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

Local Zeta Functions III

Example: If $V = (x_0, y_0)$ is a point, then $\#V(\mathbb{F}_{p^k}) = 1$, so we get

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

Example: $V = \mathbb{P}^n$, 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 Zeta Function I

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

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

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

Hasse-Weil Zeta Function II

Example: If V is a point, we get

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

which is the standard Riemann-Zeta function.

Hasse-Weil Zeta Function II

Example: If V is a point, we get

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

which is the standard Riemann-Zeta function.

Example: If $V = \mathbb{P}^n$ we instead get

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

Hasse-Weil Zeta Function III

Theorem 3

For the curves

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

with n is odd and squarefree, we have

$$\zeta(E_n, s) = \zeta(s)\zeta(s-1) \prod_{p \nmid 2n} (1 - 2a_p p^{-s} + p^{2-s}).$$

The a_p are integers depending on p and E_n.

Full BSD

Finally, the **Hasse-Weil L-Function of E_n** is defined by

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

Full BSD

Finally, the **Hasse-Weil L-Function of E_n** is defined by

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

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

Finally, the **Hasse-Weil L-Function of E_n** is defined by

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

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 Sha(E) is called the **Tate-Shafarevich group of** E.

- Sha(E) is an abelian group.
- It is conjectured to be finite.
- It measures how hard it is to find r.

Tate-Shafarevich Group

The group Sha(E) is called the **Tate-Shafarevich group of E**.

- Sha(E) is an abelian group.
- It is conjectured to be finite.
- It measures how hard it is to find r.

The full definition requires 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.

If $r = 0$, we have $R_E = 1$.

Real Period

The **Real Period of** E is given by the line integral

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

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 **of** E are integers which capture information at the primes where E mod p is singular.

Tamagawa Numbers

The **Tamagawa Numbers** c_p **of** E are integers which capture information at the primes where E mod p is singular.

In the project, we computed:

Theorem 4

If n is odd and squarefree,

$$c_2(E_n) = 2$$

$$c_p(E_n) = \begin{cases} 4 & \text{if } p \mid n \\ 1 & \text{otherwise.} \end{cases}$$

The situation so far

The situation so far seems pretty hopeless.

- On one hand we have $L(E_n, s)$ given by a complicated product.
- On the other we have a constant C that involves a transcendental number β and lots of invariants of E_n.

The situation so far

The situation so far seems pretty hopeless.

- On one hand we have $L(E_n, s)$ given by a complicated product.
- On the other we have a constant C that involves a transcendental number β and lots of 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 5 (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 **integers** *giving 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 I

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

$$L(E_n, s) = \left(\frac{\#\mathrm{Sha}(E_n) R_{E_n} \Omega_{E_n}}{\#\mathrm{Tors}(E(\mathbb{Q}))^2} \prod_p c_p(E_n) \right) (s-1)^r + O((s-1)^{r+1})$$

becomes, at $s = 1$:

BSD Revisited I

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

$$L(E_n, s) = \left(\frac{\#\mathrm{Sha}(E_n) R_{E_n} \Omega_{E_n}}{\#\mathrm{Tors}(E(\mathbb{Q}))^2} \prod_p c_p(E_n) \right) (s-1)^r + O((s-1)^{r+1})$$

becomes, at $s = 1$:

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

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

$$L(E_n, s) = \left(\frac{\#\text{Sha}(E_n) R_{E_n} \Omega_{E_n}}{\#\text{Tors}(E(\mathbb{Q}))^2} \prod_p c_p(E_n) \right) (s-1)^r + O((s-1)^{r+1})$$

becomes, at $s = 1$:

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

which simplifies to

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

BSD Revisited II

We have

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

- If $r \neq 0$, the BSD conjecture says nothing interesting about the RHS.

BSD Revisited II

We have

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

- If $r \neq 0$, the BSD conjecture says nothing interesting about the RHS.
- If $r = 0$, we have $R_{E_n} = 1$, so this further simplifies to

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

BSD Revisited II

We have

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

- If $r \neq 0$, the BSD conjecture says nothing interesting about the RHS.
- If $r = 0$, we have $R_{E_n} = 1$, 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.

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 2-Selmer Group $\mathrm{Sel}(E_n)$, a computable group which gather possible candidates for generators of $E_n(\mathbb{Q})$.

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 2-Selmer Group $\mathrm{Sel}(E_n)$, a computable group which gather possible candidates for generators of $E_n(\mathbb{Q})$.
- Matched both informations with Equation 1 for each residue class of n modulo 8.

Calculation of Coefficients of Theta Series I

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 I

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 II

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 Coefficients of Theta Series III

In the project, we worked out:

Theorem 6

If n is odd and squarefree, then:

- *If $n = p$ is a prime, we have*

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

- *If n is composite,*

$$a_n \equiv 0 \mod 4$$

Calculation of Selmer Group I

To calculate the $\text{Sel}(E)$, we saw in MATH3705 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 I

To calculate the $\mathrm{Sel}(E)$, we saw in MATH3705 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.

In the project, we also calculated:

Theorem 7

Let p be an odd prime. The Selmer Group of E_p has size

$$\#\mathrm{Sel}(E_p) = \begin{cases} 4 & \text{if } p \equiv 1 \mod 8 \\ 2 & \text{if } p \equiv 5,7 \mod 8 \\ 1 & \text{if } p \equiv 3 \mod 8 \end{cases}$$

Conclusion

From Theorem 6, we found that

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

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

Conclusion

From Theorem 6, we found that

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

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

From Theorem 7, we know that if $r = 0$, $\mathrm{Sha}(E_p)$ has an element of 2-torsion if and only if $p \not\equiv 3\,(8)$.

Conclusion

From Theorem 6, we found that

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

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

From Theorem 7, we know that if $r = 0$, $\mathrm{Sha}(E_p)$ 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.