CALCULATIONS

1. Introduction

The Birch Swinnerton-Dyer conjecture states that the Hasse-Weil L-function $L(E,s)$ of the elliptic curve E can be written as

$$L(E,s) = C(s-1)^r + O((s-1)^2)$$

where

$$C = \frac{|\mathrm{Sha}(E)|\,\Omega_E R_E}{|E(\mathbb{Q})|^2} \prod_p c_p$$

In particular, near 1, it predicts the value of

$$0^r|\mathrm{Sha}(E)| \prod_p c_p \in \mathbb{Z}$$

.

Definition 1.1. From now on we let $E_n : y^2 = x^3 - n^2 x$ be the family of quadratic twists of the elliptic curve $E_1 : y^2 = x^3 - x$.

From Tunnell's theorem we know that $L(E_n, s)$ has a particularly simple form in terms of Theta functions. In this section we'll show that they can be used to predict whether $0^r|\mathrm{Sha}(E)$ is even or odd, and that this agrees with what's the BSD conjecture.

2. Coefficients of Theta Series

Tunnell's theorem requires us to consider the quantities

$$A_n = \#\{(x,y,z)|n = 2x^2 + y^2 + 32z^2\}$$
$$B_n = \#\{(x,y,z)|n = 2x^2 + y^2 + 8z^2\}$$
$$C_n = \#\{(x,y,z)|n = 8x^2 + 2y^2 + 64z^2\}$$
$$D_n = \#\{(x,y,z)|n = 8x^2 + 2y^2 + 16z^2\}$$

depending on whether n is odd or even. For our calculations we'll need to compute $A_n - \frac{1}{2}B_n$ and $C_n - \frac{1}{2}D_n$ modulo 4.

Theorem 2.1. $2A_p - B_p \equiv \begin{cases} 0, & p \equiv 1,5,7\,(8) \\ 2, & p \equiv 3\,(8) \end{cases}$ (4)

Proof: In computing A_P and B_P we only need to consider solutions where at least 1 of x, y, z is 0, since if neither is 0, all of $\pm x, \pm y, \pm z$ are solutions, and hence they together don't make a contribution to the total number of solutions modulo 8. Furthermore, since we only need to consider A_n modulo 4, we can also ignore solutions where exactly 1 of x, yz are 0. But there are no remaining solutions since p is prime and if 2 of x, y, z are 0 we arrive at the contradiction $x^2 = p$, so we have $A_p \equiv 0\,(4)$.

With this we're left to consider $\frac{1}{2}B_p\,(4)$, or $B_p\,(8)$. Again we can ignore solutions where all of x, y, z are 0, so we have, by inclusion-exclusion

$A_p \equiv \#\{2x^2 + y^2 = p\} + \#\{y^2 + 8z^2 = p\} + \#\{2x^2 + 8z^2 = p\}$
$\equiv \#\{2x^2 + y^2 = p\} + \#\{y^2 + 8z^2 = p\}\,(8)$ since p is odd. To find the remaining quantities we need some algebraic number theory.

Lemma 2.2. *For p odd,* $\#\{2x^2 + y^2 = p\} = \begin{cases} 4, p \equiv 1\,(8) \\ 1, p \equiv 3\,(8) \\ 0, else \end{cases}$

Proof: We must have $2x^2 + y^2 \equiv 0\,(p)$, so we only have solutions if $(\frac{-2}{p}) = 1$, or equivalently if $p \equiv 1, 3\,(8)$. Since $\mathbb{Z}[\sqrt{2}]$ is a PID, if $p \equiv 1\,(8), p = \pi\bar{\pi}$ for some prime $\pi = x + y\sqrt{2}$ where $x^2 + 2y^2 = p$, so x is odd and $x^2 \equiv 1\,(8)$ If y is also odd, $1 + 2y^2 \equiv 1\,(8) \implies y^2 \equiv 1\,(8)$, and we have $x^2 + 2y^2 \equiv 3\,(8)$, a contradiction. If $y = 2k$ is even, we have $x^2 + 2y^2 = x^2 + 8y^3$

To conclude the proof of the theorem, we can deduce from the lemma that

- If $p \equiv 1\,(8), A_p \equiv 4 + 4 \equiv 0\,(8)$.
- If $p \equiv 3\,(8), A_p \equiv 4 + 0 \equiv 4\,(8)$.
- If $p \equiv 5, 7\,(8), A_p \equiv 0 + 0 \equiv 0\,(8)$.

Looking at $A_p - \frac{1}{2}B_p$ modulo 4 gives the result.

3. Tamagawa Numbers

The Hasse-Weil L-function of an elliptic curve doesn't capture any information about the primes where the curve is singular. The arithmetic data at those primes enters the Birch Swinnerton-Dyer conjecture by means of the Tamagawa Numbers. Let

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

. If $p \not| \Delta E = 4n^2$ then the reduction $\tilde{E} : y^2 \equiv x^3 - n^2 x\,(p)$ is also an elliptic curve. We have

Theorem 3.1 (Reduction Modulo p)**.** *The reduction map $E(\mathbb{Q}) \to \tilde{E}(\mathbb{F}_p)$ is a group homomorphism.*

If $p | \Delta E$ then $\tilde{E}(\mathbb{F}_p)$ is not a group, but $\tilde{E}(\mathbb{F}_p)_{ns} := \{P \in \tilde{E}(\mathbb{F}_p) | P \text{is nonsingular}\}$ is still a group.

Looking at E in the completion $\mathbb{Q}_p$ we still have a map $E(\mathbb{Q}_p) \to \tilde{E}(\mathbb{F}_p)$. If we let $E(\mathbb{Q}_p)_0$ be the preimage of $\tilde{E}(\mathbb{F}_p)_{ns}$ we get a group homomorphism

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

.

Definition 3.2. The Tamagawa Number of E at p is the number

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

If $p \not| \Delta$ then $c_p = 1$.

Theorem 3.3. *The Tamagawa Number of E_p at p is 4.*

Proof: Working in $\mathbb{Q}_p$, if $x \equiv 0$ then $y^2 = x^3 - p^2x \equiv 0\,(p^2) \implies y \equiv 0\,(p)$, so $(x, y) \equiv (0, 0)\,(p)$. If x has nonpositive valuation, $x = p^{-n}u, u \in \mathbb{Z}_p^\times$ and $y^2 = p^{-3n}u^3 - p^{2-n}u$, so n must be even.

Let $n = 2m$. Then $p^{6m}y^2 = u^3 - p^{2+2m}u \implies y = p^{-3m}v, v \in \mathbb{Z}_p^\times$. Since $u, v \not\equiv 0\,(p)$, this has solutions if and only if $(\frac{u}{p}) = 1$, so x is the reciprocal of a square in $\mathbb{Z}_p$.

Setting $x = \frac{1}{r^2}, r^2 \in \mathbb{Z}_p$ we get $y^2 = \frac{1}{r^6} - \frac{p^2}{r^2} = \frac{1-p^2r^4}{r^6}$, so we have a bijection

$$\mathbb{Z}_p \to E(\mathbb{Q}_p)_0$$

$$r \mapsto (\frac{1}{r^2}, \frac{\sqrt{1-p^2r^4}}{r^3})$$

$$0 \mapsto \mathcal{O}$$

To prove the theorem we will need the following lemma:

Lemma 3.4. *The torsion points $\mathcal{O}, (0, 0), (p, 0), (-p, 0)$ are a complete set of representatives for $\frac{E(\mathbb{Q}_p)}{E(\mathbb{Q}_p)_0}$.*

Proof: Let $P(r) = (\frac{1}{r^2}, \frac{\sqrt{1-p^2r^4}}{r^3}) = (x, y)$. We will compute $S := P(r)+Q$ for each torsion point Q.

- $Q = \mathcal{O}$: $P(r) + \mathcal{O} = P(r)$.
- $Q = (0, 0)$: We have $\lambda = \frac{y}{x}$, so

$$\begin{aligned} x(S) = \lambda^2 - x - 0 &= \frac{\frac{1-p^2r^4}{r^6}}{\frac{1}{r^4}} - \frac{1}{r^2} \\ &= -p^2r^2 \end{aligned}$$

- $Q = (p, 0)$: We have $\lambda = \frac{y}{x-p}$, so

$$\begin{aligned} x(S) = \lambda^2 - x - p &= \frac{\frac{1-p^2r^4}{r^6}}{\frac{(1-pr^2)^2}{r^4}} - \frac{1}{r^2} - p \\ &= \frac{1-p^2r^4}{r^2(1-pr^2)^2} - \frac{1+pr^2}{r^2} \\ &= -p + \frac{2p}{1-pr^2} \end{aligned}$$

- $Q = (-p, 0)$: We have $\lambda = \frac{y}{x+p}$, so

$$\begin{aligned} x(S) = \lambda^2 - x + p &= \frac{\frac{1-p^2r^4}{r^6}}{\frac{(1+pr^2)^2}{r^4}} - \frac{1}{r^2} + p \\ &= p - \frac{2p}{1+pr^2} \end{aligned}$$

Now let $S = (x, y)$. If $x \equiv 0\,(p^2)$, $x = p^2 t, t \in \mathbb{Z}_p$ we want to show that $x = p^2 r^2, r \in \mathbb{Z}_p$, so that S lies in the coset $P(r) + (0, 0)$. Note that

$$\begin{aligned} y^2 &= x^3 - p^2 x \\ &= x(x+p)(x-p) \\ x &= \frac{y^2}{(x+p)(x-p)} \\ &= \frac{y^2}{p^2(1+tp)(1-tp)} \end{aligned}$$

and $1 \pm tp$ are squares in $\mathbb{Q}_p$, so indeed x is a square and we can set $r = \sqrt{\frac{x}{p^2}}$.

If $x \equiv p\,(p^2), x = p + p^2 t$ we want to solve

$$p - \frac{2p}{1+pr^2} = x = p + p^2 t$$

or

$$\frac{-2}{1+pr^2} = pt$$

to show that S lies in the coset $P(r) + (-p, 0)$.

$$\begin{aligned} 1 + pr^2 &= \frac{-2}{pt} \\ r^2 &= \frac{-2-pt}{p^2 t} \end{aligned}$$

. Now

$$\begin{aligned} x = \frac{y^2}{(x+p)(x-p)} &= \frac{y^2}{(p^2t+2p)(p^2t)} = \frac{y^2}{p^2t(2+pt)p} \\ \implies x &= \frac{y^2}{-r^2 p} \\ \implies r^2 &= \frac{y^2}{-px} = \frac{y^2}{p^2(-1-pt)} \end{aligned}$$

If $x \equiv -p\,(p^2), x = -p + p^2 t$ and we solve

$$-p + \frac{2p}{1-pr^2} = x = -p + p^2 t$$

or

$$\begin{aligned} \frac{2}{1-pr^2} &= pt \\ \implies r^2 &= \frac{pt-2}{p^2 t} \end{aligned}$$

Now

$$\begin{aligned} x = \frac{y^2}{(x+p)(x-p)} &= \frac{y^2}{(p^2t-2p)(p^2t)} = \frac{y^2}{p^2t(pt-2)p} \\ \implies x &= \frac{y^2}{r^2 p} \\ r^2 &= \frac{y^2}{xp} = \frac{y^2}{p^2(1+pt)} \end{aligned}$$

which is a square, so again we can solve for r.

Theorem 3.5. *The Tamagawa Number of E_P at 2 is 2.*

Proof: By checking all possibilities, we know that

$$\tilde{E}(\mathbb{F}_2) = \{\mathcal{O}, (0,0), (1,0)\},$$

with $(1,0)$ being the singular point. Let $\pi : E(\mathbb{Q}_2)_0 \to \tilde{E}(\mathbb{F}_2)_{ns}$ be the projection map. or any $P = (x,y) \in E(\mathbb{Q}_2)$, if $\pi(P) = (1,0)$ then $\pi(P * (p,0)) \neq (p,0)$. If x is a unit, let $(x,y) * (p,0) = (x',y')$. We want to show that x' is not a unit. Suppose it is, and let λ be the gradient of the line through $(x,y),(p,0),(x',y')$, so that $\lambda = \frac{y}{x-p}$. Then $x + p + x' = \lambda^2$, so $\lambda \not\equiv 0\,(2)$, so λ is a unit. We also have

$$\begin{aligned} y^2 &= x^3 - p^2 x \\ \implies \lambda^2(x-p)^2 &= x(x+p)(x-p) \\ \implies u^2 &= \frac{x(x+p)}{x-p} \end{aligned}$$

implying $\frac{x+p}{x-p}$ is a unit, which is a contradiction, since $\nu_2(\frac{x+p}{x-p}) =$