BSD and the Gross-Zagier Formula

Dylan Yott

July 23, 2014

1 Birch and Swinnerton-Dyer Conjecture

Consider $E : y^2 = x^3 + ax + b/\mathbb{Q}$, an elliptic curve over $\mathbb{Q}$. By the Mordell-Weil theorem, the group $E(\mathbb{Q})$ is finitely generated, so by the structure theorem of finitely generated abelian groups we have:

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

Where $r > 0$ is called the rank, and $E(\mathbb{Q}))_{tors}$ are the elements of finite order. In order to better understand these groups, we reduce mod p (whenever possible).

Let $p > 3$ and consider $E : y^2 = x^3 + ax + b/\mathbb{F}_p$, an elliptic curve over $\mathbb{F}_p$, which looks a little different when $p = 2, 3$. By a theorem of Hasse and Weil, we have:

$$|\#(E(\mathbb{F}_p)) - (p+1)| \leq 2\sqrt{p}$$

If we define $N_p = \#E(\mathbb{F}_p)$ then it is natrual to consider the quantity $\frac{N_p}{p}$. Numerical date collected by Birch and Swinnerton-Dyer suggested the following very interesting result:

$$\prod_{p \leq x} \frac{N_p}{p} \approx Clog(x)^r$$

where r is the rank of $E/\mathbb{Q}$. When they approached the experts with their results, they were told that they should rephrase their results in terms of L-functions, so they did.

Set $a_p = p + 1 - N_p$ and consider the following:

$$L_p(E, s) = \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

Then by formally evaluating at $s = 1$ we have:

$$L_p(E, 1) = \frac{p}{N_p}$$

Define $L(E, s) = \prod_p L_p(E, s)$ so that formally we have:

$$L(E, 1) = \prod_p \frac{p}{N_p}$$

The idea behind the Birch and Swinnerton-Dyer conjecture is as follows. Suppose $r > 0$. Then there should be lots of points over $\mathbb{Q}$, which should give lots of points mod p, forcing $L(E, 1) = 0$, and perhaps if the rank is larger we might believe that the denominators N_p are so large that it forces $L'(E, 1) = 0, L''(E, 1) = 0$, etc.

We have the following:

Conjecture 1.1. $rank(E(\mathbb{Q})) = ord|_{s=1}L(E, s)$

To explain the partial progress on BSD, which can be summarized as analytic rank 0 or 1 implies Mordell-Weil rank 0 or 1, we introduce the Gross-Zagier formula.

2 Modular Curves

Let $\mathbb{H} = \{z \in \mathbb{C} \mid Im(z) > 0\}$, and recall this space carries an action of $SL(2, \mathbb{Z})$ by linear fractional transformations. Now consider:

$$\Gamma_0(N) = \{A \in SL(2, \mathbb{Z}) \mid A \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod N\} \tag{1}$$

It is well known that $\Gamma_0(N)/\mathbb{H} := Y_0(N)$ is a Riemann surface with finitely many cusps, and whose compactification is an algebraic curve that can be defined over $\mathbb{Q}$. Away from the cusps, $X_0(N)$ parametrizes isogenies of elliptic curves ($\phi : E \to E'$) with $ker(\phi) \equiv \mathbb{Z}/(n)$. The covering $\pi : X_0(N) \to X_0(1)$ corresponds to $(\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}) \to \mathbb{C}/(\frac{1}{N}\mathbb{Z} + \tau\mathbb{Z}))) \to \mathbb{C}/((\mathbb{Z} + \tau Z))$

Now fix an imaginary quadratic field $K = Q(\sqrt{-d})$, and choose N with the property that the primes dividing N split in K. Such an N is said to satisfy the Heegner hypothesis. Then clearly we can find an ideal $\mathfrak{n}$ with $\mathcal{O}_K/\mathfrak{n} \equiv \mathbb{Z}/(N)$. Then for any $\mathfrak{a} \subset \mathcal{O}_K$, we have the covering $(\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{n}^{-1}\mathfrak{a}) \in X_0(N)(\mathbb{C})$. Dilating $\mathfrak{a}$ by anything in $K^\times$ gives the same elliptic curve, thus giving a well-defined map on ideal classes. We have:

$$\gamma_\mathfrak{n} : Cl(K) \to X_0(N)(\mathbb{C}) \tag{2}$$

These points on $X_0(N)$ are called Heegner points, and the theory of complex multiplication on elliptic curves tells us that they're actually defined over the Hilbert class field of K, which is the maximal unramified abelian extension of K and can be gotten by adjoining the j-invariant of an elliptic curve with CM by $\mathcal{O}_K$. These points also enjoy a nice property with respect to the Artin map called "Galois-equivariance".

$$Art_K(\mathfrak{p}) \cdot [\gamma_\mathfrak{n}([\mathfrak{a}])] = \gamma_\mathfrak{n}([\mathfrak{p}\mathfrak{a}]) \tag{3}$$

$$\tag{4}$$

Now, entering the stage, let E be an elliptic curve with conductor N. Then by the Modularity theorem, there exists a unique modular form $f_E = a_E(n)q^n$ of weight 2 and level N satisfying:

$$\#E(\mathbb{F}_p) = p + 1 - a_E(p) \tag{5}$$

For such an f_E, we the following, which will be important later in stating the Gross-Zagier formula:

$$||f_E||^2 = \int_{Y_0(N)} |f(z)|^2 dxdy \tag{6}$$

Another consequence of the modularity theorem is a dominant map $\phi_E : X_0(N) \to E$. We can consider $\phi_E(\gamma_{\mathfrak{n}}([\mathfrak{a}])) \in E(H_K)$. Rather, we consider the following point (which turns out to not to depend on $\mathfrak{n}$, so we drop it from our notation):

$$P_K = \sum_{[\mathfrak{a}]\in Cl(K)} \phi_E(\gamma_{\mathfrak{n}}([\mathfrak{a}])) \tag{7}$$

A priori we know $P_K \in E(H_K)$, but in fact by Galois equivariance any element of $Gal(H_K/K) \cong Cl(K)$ simply permutes the ideal classes in the sum, so in fact $P_K \in E(K)$. Our goal is to describe the height of the point in terms of an L-function.

3 Heights

Let k/Q be finite and v a place of k. For $w = [x, y, z] \in \mathbb{P}^2(k)$, define the height as follows:

$$h_k(x) = \frac{1}{[k:Q]} log \left(\prod_v max(|x|_v, |y|_v, |z|_v) \right) \tag{8}$$

Note that this is well-defined and nonnegative by the product formula, and $h_k(x) = h'_k(x)$ whenever $k' \subset k$. Thus we can define $h(x) \in \mathbb{P}^2(\overline{k})$ to be the direct limit over k. For $E \subset \mathbb{P}^2$, define the canonical height of a point $P \in E(\overline{k})$:

$$h_E(P) = \lim_{n\to\infty} \frac{h(n \cdot P)}{n^2} \tag{9}$$

Neron and Tate were able to show this height function is well-defined, a quadratic form, and $h_E(P) = 0$ iff P is a torsion point. With the notion of height in place, we now should define the relevant L-functions so we can state our theorem.

4 L-functions

Let $E/\mathbb{Q}$ be an elliptic curve with conductor N. Intuitively, the conductor measures the reduction behavior of E modulo different primes, as in the primes dividing the conductor are precisely the primes at which E has bad reduction, and the multiplicity of p in N measures the type of reduction. Now we recall the definition of the L-function of E:

$$L(s, E/\mathbb{Q}) = \prod_{p\nmid N} \frac{1}{1 - a_E(p)p^-s + p^{1-2s}} \prod_{p|N} \frac{1}{1 - a_E(p)p^{-s}} \tag{10}$$

If we define:

$$\Lambda(s, E/\mathbb{Q}) = (2\pi)^{-s} N^{\frac{s}{2}} \Gamma(s) L(s, E/\mathbb{Q}) \tag{11}$$

Then it turns out that modularity implies:

$$\Lambda(s, E/\mathbb{Q}) = \pm\Lambda(2 - s, E/\mathbb{Q}) \tag{12}$$

We call the sign in this expression $\epsilon(E/\mathbb{Q})$ the root number of E/Q. Also recall that the Dedekind zeta function, ζ_K admits the following factorization:

$$\zeta_K(s) = \zeta_{\mathbb{Q}}(s) L(s, \chi_d) \tag{13}$$

Where χ_d is the quadratic Dirichlet character of period $|d|$. Consider the following twisted L-function, $L(s, E^d/\mathbb{Q})$, which is also the L-function of the twist of E, given by $y \mapsto y\sqrt{d}$.

$$L(s, E^d/\mathbb{Q}) = \prod_{p \nmid N} \frac{1}{1 - a_E(p)\chi_d(p)p^{-s} + \chi_d(p)^2 p^{1-2s}} \prod_{p \mid N} \frac{1}{1 - a_E(p)p^{-s}} \tag{14}$$

The root number $\epsilon(E^d/\mathbb{Q}) = \epsilon(E, /\mathbb{Q})\chi_d(-N)$. Now set :

$$L(s, E/K) = L(s, E/\mathbb{Q}) L(s, E^d/\mathbb{Q}) \tag{15}$$

Now we wish to compute $\epsilon(E/K)$:

$$\epsilon(E/K) = \epsilon(E/\mathbb{Q})^2 \chi_d(-N) \tag{16}$$

$$= -1 \tag{17}$$

Since $d < 0$ and all the primes dividing N split in K. This forces:

$$L(1, E/K) = 0 \tag{18}$$

The goal of the Gross-Zagier formula is to express $L'(1, E/K)$ in terms of these previously defined height functions.

5 The Gross-Zagier Formula and Applications

Theorem 5.1. *With all the previous notation, we have the following:*

$$L'(1, E/K) = \frac{32\pi^2 ||f_E||^2}{|\mathcal{O}_K^\times|^2 \sqrt{|d|} deg\phi_E} h_E(P_K) \tag{19}$$

In particular, $L'(1, E/K) = 0$ iff P_K is torsion.

A more interesting corollary is the following:

Proposition 5.2. *Let $E/\mathbb{Q}$ be an elliptic curve with $\epsilon(E/\mathbb{Q}) = -1$ and $L'(1, E/\mathbb{Q}) \neq 0$. Then E/Q has points of infinite order.*

Proof. By a theorem of Waldspruger, we can find a K satisfying the Heegner hypothesis and with $L(1, E^d/\mathbb{Q}) \neq 0$. Then:

$$\begin{aligned} L'(1, E/K) &= L(1, E/\mathbb{Q})L'(1, E^d/\mathbb{Q}) + L'(1, E/\mathbb{Q})L(1, E^d/\mathbb{Q}) &(20)\\ &= L'(1, E/\mathbb{Q})L(1, E^d/\mathbb{Q}) &(21)\\ &\neq 0 &(22)\end{aligned}$$

Now, we use the Manin-Drinfeld theorem which says that the difference of any two cusps if a modular curve is torsion, that is, the following point is torsion:

$$\begin{aligned} \phi_E(0) &= -\int_0^{i\infty} \omega_f &(23)\\ &= \int_z^{i\infty} \omega_f + \int_0^{z} \omega_f &(24)\\ &= \int_z^{i\infty} \omega_f + \int_{w_N z}^{i\infty} w_N\omega_f &(25)\\ &= \int_z^{i\infty} \omega_f + \int_{i\infty}^{w_N z} w_N\omega_f &(26)\\ &= \int_z^{i\infty} \omega_f - \int_{w_N z}^{i\infty} w_N\omega_f &(27)\end{aligned}$$

Recall the the involution $w_N(z) = \frac{-1}{Nz}$ acts by $f(\frac{-1}{Nz}) = -\epsilon z^2 f(z)$, and $d(\frac{-1}{Nz}) = N^{-1}z^{-2}dz$, so that we have the following point is torsion (and in fact independent of $z \in X_0(N)(\mathbb{C})$).

$$\begin{aligned} \phi_E(0) &= \int_z^{i\infty} \omega_f + \epsilon\int_{w_N z}^{i\infty} \omega_f &(28)\\ &= \phi_E(z) + \epsilon\phi_E(w_N z) &(29)\end{aligned}$$

Setting $z = \gamma_{\bar{\mathfrak{n}}}(\bar{\mathfrak{a}})$, we have the following:

$$\begin{aligned} Torsion &= \phi_E(\gamma_{\bar{\mathfrak{n}}}(\bar{\mathfrak{a}})) + \epsilon\phi_E(w_N \cdot \gamma_{\bar{\mathfrak{n}}}(\bar{\mathfrak{a}})) &(30)\\ &= \overline{\phi_E(\gamma_{\mathfrak{n}}(\mathfrak{a}))} + \epsilon\phi_E(\gamma_{\mathfrak{n}}(\overline{\mathfrak{a}\mathfrak{n}^{-1}})) &(31)\\ &= \overline{P_{[a]}} + \epsilon P_{\mathfrak{a}^{-1}\mathfrak{n}} &(32)\\ &= \overline{P_{[a]}} + \epsilon Art_K(\mathfrak{a}^{-2}\mathfrak{n}) \cdot P_{[a]} &(33)\end{aligned}$$

Now, suppose $\tau \in Gal(H_K/\mathbb{Q})$ acts nontrivially on K. Then for an ideal class $[\mathfrak{a}]$, there is a restriction $\sigma \in Gal(H/K)$ so that $\tau P_{[\mathfrak{a}]} + \epsilon\sigma P_{[\mathfrak{a}]}$ is torsion. Summing over the translates in $Gal(H_K/K)$ gives the following torsion point (since its a sum of torsion points):

$$\sum_{\rho \in Gal(H_K/K)} \rho\tau P_{[\mathfrak{a}]} + \epsilon\rho\sigma P_{[\mathfrak{a}]} = \sum_{\rho \in Gal(H_K/K)} \tau P_{Art_K^{-1}(\rho)[\mathfrak{a}]} + \epsilon P_{Art_K^{-1}(\sigma\rho)[\mathfrak{a}]} \tag{34}$$

$$= \overline{P_K} + \epsilon P_K \tag{35}$$

However, since h_E is a quadratic form, we can apply the parallelogram law:

$$h_E(\overline{P_K} - \epsilon P_K) + h_E(\overline{P_K} + \epsilon P_K) = 2h_E(P_K) + 2h_E(\overline{P_K}) \tag{36}$$

$$= 4h_E(P_K) \tag{37}$$

$$> 0 \tag{38}$$

Where the last line follows since $L'(1, E/K) \neq 0$. Since the second point is torsion, its height is 0, so we must have:

$$h_E(\overline{P_K} - \epsilon P_K) > 0 \tag{39}$$

Thus $\overline{P_K} - \epsilon P_K$ is nontorsion, and is visibly defined over $\mathbb{Q}$ iff $\epsilon = -1$. $\square$