A Gross-Zagier Style Conjecture and the Birch and Swinnerton-Dyer Conjecture

William Stein

July 3, 2009

Contents

1 Introduction

In this paper we describe a conjecture that has a similar style to the Gross-Zagier formula, and implies the Birch and Swinnerton-Dyer conjecture. We then discuss some relevant computations related to the conjecture for some curves of rank > 1.

2 A Gross-Zagier Style Conjecture

Let E be an elliptic curve defined over $\mathbb{Q}$ with analytic rank at least 1 and let N be its conductor. Let K be one of the infinitely many quadratic imaginary fields with discriminant $D < -4$ coprime to N such that each prime dividing N splits in K, and such that

$$\mathrm{ord}_{s=1} L(E^D, s) \leq 1.$$

Fix any odd prime ℓ such that $\overline{\rho}_{E,\ell}$ is surjective. Below we only consider primes $p \nmid ND$ that are inert in K. Set $N_p = \#E(\mathbb{F}_p)$, and let $\tilde{a}_p = \ell^{\mathrm{ord}_\ell(p+1-N_p)}$ be the ℓ-part of $a_p = p+1-N_p$. Let

$$b_p = \#(E(\mathbb{F}_p)/\tilde{a}_p E(\mathbb{F}_p)),$$

Note that $b_p = \gcd(p+1, \tilde{a}_p)$, by [**?**, Lemma 5.1]. For any squarefree positive integer n, let

$$b_n = \gcd(\{b_p : p \mid n\}).$$

Let $P_n = J_n I_n y_n \in E(K_n)$ be the Kolyvagin point associated to n, where K_n is the ring class field of K of conductor n. The elements $J_n, I_n \in \mathbb{Z}[\mathrm{Gal}(K_n/K)]$ are constructed so that

$$[P_n] \in (E(K_n)/b_n E(K_n))^{\mathrm{Gal}(K_n/K)}.$$

See [**?**] for more details.

Let $r_{\mathrm{an}}(E/\mathbb{Q}) = \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s)$ and let $t < r_{\mathrm{an}}(E/\mathbb{Q})$ be any nonnegative integer with

$$t \equiv r_{\mathrm{an}}(E/\mathbb{Q}) - 1 \pmod 2.$$

For any prime $p \nmid n$ with $\ell \mid b_p \mid b_n$, reducing modulo any choice of prime $\wp$ over $p\mathcal{O}_K$ yields a well defined point

$$\overline{P}_n \in E(\mathbb{F}_p)/\tilde{a}_p E(\mathbb{F}_p).$$

The congruence condition on t and our assumption that ℓ is odd implies that $\overline{P}_n \in E(\mathbb{F}_p)$ and not just in $E(\mathbb{F}_{p^2})$. Let $Y_p^t \subset E(\mathbb{F}_p)/\tilde{a}_p E(\mathbb{F}_p)$ be the subgroup generated by all points $\overline{P}_n$ as we vary over all n divisible by exactly t primes such that $b_p \mid b_n$. The Chebotarev density theorem implies that there are infinity many such integers n.

Let $\pi_p : E(\mathbb{Q}) \to E(\mathbb{F}_p)/\tilde{a}_p E(\mathbb{F}_p)$ be the natural quotient map, and let

$$W_p^t = \pi_p^{-1}(Y_p^t) \subset E(\mathbb{Q}).$$

If G is a subgroup of $E(\mathbb{Q})$ and n is a positive integer, let

$$\langle G, G\rangle_n = \inf\{|\det\langle g_i, g_j\rangle| : \text{ independent points } g_1, \dots g_n \in G\},$$

where $g_1, \dots, g_n$ run through all choices of indepedent elements of $G/_{\mathrm{tor}}$. If G has rank $< n$, then $\langle G, G\rangle_n = 0$ since it is the infimum of the empty set. Also not that one can prove using reduction theory for quadratic forms that there are only finitely many subgroups of G of bounded height, so we

can replace the infimum by a minimum. Also, if G has rank $n > 0$, then $\langle G, G\rangle_n = \mathrm{Reg}(G)$ is the regulator of G.

Chose *any* maximal chain of subgroups $W^t_{p_1} \supsetneq W^t_{p_2} \supsetneq W^t_{p_3} \dots$ associated to primes $\mathcal{C} = \{p_1, p_2, \dots\}$, and let

$$W^t_{\mathcal{C}} = \bigcap_{p_i \in \mathcal{C}} W^t_{p_i}.$$

Note that $\mathcal{C}$ could be either finite or infinite. The intersection $W^t_{\mathcal{C}}$ may depend on $\mathcal{C}$ and not just t, but we expect that for each t, there are only finitely many possibilities for W^t and only one possibility for $[E(\mathbb{Q}) : W^t]$. Also, since Y_p is a subgroup of the cyclic group $E(\mathbb{F}_p)/\tilde{a}_p E(\mathbb{F}_p)$, if $W^t_{\mathcal{C}}$ has finite index in $E(\mathbb{Q})$, then the quotient $E(\mathbb{Q})/W^t_{\mathcal{C}}$ is cyclic.

Finally, let

$$v = t + 1 + r_{\mathrm{an}}(E^D/\mathbb{Q}),$$

and note that $v \le r_{\mathrm{an}}(E/K)$ and $v \equiv r_{\mathrm{an}}(E/K) \pmod 2$.

Conjecture 2.1. *Fix a prime ℓ, an integer t and set of primes $\mathcal{C}$ as above. Then we have the following generalization of the Gross-Zagier formula:*

$$\frac{L^{(v)}(E/K, 1)}{v!} = \frac{b \cdot \|\omega\|^2}{c^2\sqrt{|D|}} \cdot \langle W^t_{\mathcal{C}}, W^t_{\mathcal{C}}\rangle_{t+1} \cdot \mathrm{Reg}(E^D/\mathbb{Q}),$$

where b is a positive integer not divisible by ℓ.

Let B be divisible by 2 and the primes where $\overline{\rho}_{E,\ell}$ is not surjective.

Conjecture 2.2. *Let t be an integer as above. For prime $\ell \nmid B$, make a choice of $W(\ell) = W^t_{\mathcal{C}}$ as above. Let $W = \cap_{\ell \nmid B} W(\ell)$. Then*

$$\frac{L^{(v)}(E/K, 1)}{v!} = \frac{b \cdot \|\omega\|^2}{c^2\sqrt{|D|}} \cdot \langle W, W\rangle_{t+1} \cdot \mathrm{Reg}(E^D/\mathbb{Q}),$$

where b is an integer divisible only by prime divisors of B.

The classical Gross-Zagier formula is like the above formula, but $v = 1$, we have $\mathrm{Reg}(E^D/\mathbb{Q}) = 1$, and $\langle W, W\rangle_{t+1}$ is the height of the Heegner point $P_1 \in E(K)$.

All the definitions above make sense with no assumption on ℓ, but we are not confident making the analogue of Conjecture 2.2 without further data.

3 The Birch and Swinnerton-Dyer Conjecture

Theorem 3.1. *Conjecture 2.1 implies the BSD conjecture. More precisely, if Conjecture 2.1 is true, then*

$$\mathrm{rank}(E(\mathbb{Q})) = \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s)$$

and $Ш(E/\mathbb{Q})[\ell^\infty]$ *is finite.*

Proof. First take $t = r_{\mathrm{an}}(E/\mathbb{Q}) - 1$. If $Y_p^t = 0$ for all p, then using the Chebotarev density theorem (see ggz paper), we can find a sequence of primes p_i so that if $\mathcal{C} = \{p_1, p_2, \ldots\}$, then $W_{\mathcal{C}}^t = 0$. However, in Conjecture 2.1 we have $v = r_{\mathrm{an}}(E/K)$, so $L^{(v)}(E/K, 1) \neq 0$, hence $\langle W_{\mathcal{C}}^t, W_{\mathcal{C}}^t \rangle_t \neq 0$ so $W_{\mathcal{C}}^t$ is infinite. Consequently, some $Y_p^t \neq 0$, hence some class $[P_n] \neq 0$ for some n divisible by t primes. Thus Kolyvagin's "Conjecture A" is true with $f \leq r_{\mathrm{an}}(E/\mathbb{Q}) - 1$. It follows by [**?**, Theorem 4.2] that for all $m \gg 0$ we have

$$\mathrm{Sel}^{(\ell^m)}(E/\mathbb{Q}) = (\mathbb{Z}/\ell^m\mathbb{Z})^{f+1} \oplus S \tag{3.1}$$

where S is a finite group independent of m (note that conjecturally, S is the ℓ part of $Ш(E/\mathbb{Q})$). Thus $\mathrm{rank}(E/\mathbb{Q}) \leq f + 1$.

By Conjecture 2.1 above there are $t + 1$ independent points in $W_{\mathcal{C}}^t \subset E(\mathbb{Q})$, so $t + 1 \leq \mathrm{rank}(E/\mathbb{Q})$ and $t + 1 \leq f + 1$. Thus $f = r_{\mathrm{an}}(E/\mathbb{Q}) - 1$, and the BSD conjecture that $\mathrm{rank}(E/\mathbb{Q}) = r_{\mathrm{an}}(E/\mathbb{Q})$ is true. Finiteness of $Ш(E/\mathbb{Q})[\ell^\infty]$ then follows from (3.1). □

4 Explicit Computations

For the rest of this section, we let $t = r_{\mathrm{an}}(E/\mathbb{Q}) - 1$, and set $Y_p = Y_p^t$.

Theorem 4.1. *Assume Conjecture 2.1, the BSD formula at ℓ for E over K, and Kolyvagin's Conjecture D_ℓ. Then for any good prime p, the group Y_p is the image of $I \cdot E(\mathbb{Q})$ in $E(\mathbb{F}_p)/\tilde{a}_p E(\mathbb{F}_p)$, where*

$$I = c \prod c_q \prod \sqrt{\#Ш(E/K)}.$$

[[worry – there is a "sufficiently large" in Kolyvagin? If so, make this a conjecture, then give a theorem for sufficiently large as evidence.]]

[[worry – the above only gives W_p, not Y_p]]

Proof. This is Proposition 7.3 of [**?**]. (It might be that assuming Kolyvagin's Conjecture D_ℓ is redundant.) □

Assuming the conclusion of Theorem 4.1, we can *in practice* compute the group Y_p for any elliptic curve E. We can thus conditionally verify Conjecture 2.1. Just verifying the conjecture is not worth doing, since under the above hypothesis, Conjecture 2.1 is implied by the BSD formula, since $\pi_P^{-1}(Y_p)$ has small enough index that it must contain a Gross-Zagier subgroup (see [**?**, Prop. 2.4] and [**?**, Lemma. 7.4]). There is, however, extra information contained in *which* subgroup $\pi_p^{-1}(Y_p)$ we find for a given p, since that does depend in a possiby subtle way on p.

A deeper structure on Y_p is that it has labeled generators $\overline{P}_n$, indexed by positive integers n. So far, it appears to be a highly nontrivial calculation to explicitly compute a specific $\overline{P}_n$ in any particular case.

In the rest of this section, we compute as much as we reasonably can about the objects above in some specific examples.

For the computations below, we assume BSD and Kolyvagin's conjecture so we can use Theorem 4.1 to compute Y_p.

Example 4.2. Let E be the rank 2 elliptic curve 389a, and let $\ell = 3$. We have $v = 0$, since $c = c_{389} = 1$ and $\#Ш_{\text{an}} = 1.000\ldots$. The primes $p < 100$ such that $E(\mathbb{F}_p)/\tilde{a}_p E(\mathbb{F}_P) \neq 0$ are $P = \{5, 17, 29, 41, 53, 59, 83\}$, and in each case $E(\mathbb{F}_p)/\tilde{a}_p E(\mathbb{F}_P)$ is cyclic of order 3. We have

$$E(\mathbb{Q}) = \mathbb{Z}P_1 \oplus \mathbb{Z}P_2$$

where $P_1 = (-1, 1)$ and $P_2 = (0, -1)$.

5 Future Directions and Projects

1. Assuming the hypothesis of Theorem 4.1, compute groups W for various choices of $W_{p_1} \supsetneq W_{p_2} \supsetneq \cdots$ when $I \neq 1$.

2. Formulate Conjecture 2.1 on $J_0(N)$ over the Hilbert class field of K, and deduce Conjecture 2.1 from this more general conjecture.

3. Formulate Conjecture 2.1 at *all* primes ℓ hence get an exact formula for $\langle W, W\rangle_{t+1}$ as almost in Conjecture 2.2.

4. Find an algorithm to compute Y_p or W_p. This would be especially interesting when Theorem 4.1 does not apply. Give a conjectural description of Y_p in *all* cases.