MATHEMATICS OF COMPUTATION
Volume 00, Number 0, Pages 000–000
S 0025-5718(XX)0000-0

COMPUTATIONAL VERIFICATION OF THE FULL BIRCH AND SWINNERTON-DYER CONJECTURE FOR CERTAIN ELLIPTIC CURVES

WORK IN PROGRESS – DON'T TRUST ANYTHING

Contents

[[Todo: get bibliography to work]]

1. Introduction

[[Todo: Write this last.]]

2. Background

[[Todo: since everyone reading the paper knows what sha is already, and we likely want to safe space, should we omit the diagram and just define sha verbally?

OK – get rid of it...]]

For an elliptic curve E defined over a number field K the following diagram defines the Selmer and the Shafarevich-Tate groups as $Sel(E/K)_p = \ker f, Ш(E/K) = \ker g$:

$$\begin{tikzcd}
0 \arrow[r] & (E(K)/pE(K)) \arrow[r] & H^1(G(\bar{K}/K), E[p]) \arrow[r] \arrow[d, "Res"'] \arrow[dr, "f"] & H^1(G(\bar{K}/K), E)[p] \arrow[d, "g_p"] \\
& & H^1(G(\bar{K_\lambda}/K_\lambda), E[p]) & \prod_v H^1(G(\bar{K_v}/K_v), E)[p]
\end{tikzcd}$$

Recall that $H^1(K,E) = \varinjlim H^1(L/K,E)$, where the direct limit is taken over all finite Galois extensions L/K; since each one of these groups is torsion, (killed by $[L:K]$,) so is $H^1(K,E)$. Therefore, $Ш(E/K)$ is a torsion group, a fact we will later to use to conclude that $Ш(E/K) = 0$ for curves having $Ш(E/K)[p] = 0$ for all primes p. In what follows, we will obtain results of the form $Ш(E/K)[p] = 0$ for almost all p, where $[K : \mathbf{Q}] = 2$. The canonical map $Ш(E/\mathbf{Q}) \to Ш(E/K)$ has kernel contained in $H^1(K/\mathbf{Q}, E)$, a finite abelian 2-group, so $Ш(E/K)[p] = 0 \Rightarrow Ш(E/\mathbf{Q})[p] = 0$ as long as $p \neq 2$. The difficulty in studying the Shafarevich-Tate group is the major obstacle to progress on the Birch and Swinnerton-Dyer conjecture:

Conjecture 2.1 (Birch-Swinnerton-Dyer). *Let E be an elliptic curve defined over $\mathbf{Q}$. Then the order of vanishing at $s = 1$ of $L(E/\mathbf{Q}, s)$ equals the rank of $E(\mathbf{Q})$. More precisely, letting $r = rk_{\mathbf{Z}} E(\mathbf{Q})$, and phrasing the conjecture in terms of $\#Ш(E/\mathbf{Q})$,*

$$\#Ш(E/\mathbf{Q}) = \frac{L^r(E/\mathbf{Q}, 1)|E(\mathbf{Q})_{tors}|^2}{r! R(E/\mathbf{Q}) \prod_v c_v(E)}$$

$R(E/\mathbf{Q})$ denotes the elliptic regulator, the determinant of the canonical height pairing matrix on a set of free generators. The $c_v = [E(\mathbf{Q}_v) : E_0(\mathbf{Q}_v)]$ for finite places are the Tamagawa numbers, measuring bad reduction at v (in particular, they are 1 when E has good reduction at v), and $c_\infty = \int_{E(\mathbf{R})} |\omega|$, where ω is the invariant differential $\frac{dx}{2y + a_1 x + a_3}$ attached to a global minimal Weierstrass equation.

Note that a theorem of Cassels (see [**?**]) asserts that, assuming the Shafarevich-Tate group is finite, the full Birch and Swinnerton-Dyer conjecture is invariant under isogeny. For elliptic curves of analytic rank at most 1, Kolyvagin showed that $Ш(E/\mathbf{Q})$ is finite; for these curves it is enough to check the full BSD conjecture for one curve in the isogeny class.

3. Derivatives of L-functions

3.1. **Gross-Zagier.** One of the factors in the BSD formula is the derivative of the L-function. For $K = \mathbf{Q}(\sqrt{-D})$ a quadratic imaginary extension, let E^D be the quadratic twist associated with D, so $L(E/K,s) = L(E/\mathbf{Q},s)L(E^D/\mathbf{Q},s)$. [[**Todo: necessary?:**]]If the newform of E is f, then the newform of E^D is $f \otimes \left(\frac{\cdot}{D}\right)$. On the level of Weierstrass equations, if E has equation $y^2 = x^3 + ax + b$, then E^D has equation $y^2 = x^3 + D^2ax + D^3b$.

We say that K satisfies the Heegner hypothesis for the elliptic curve $E/\mathbf{Q}$ of conductor N if all prime factors of N split in K. This allows the construction of a Heegner point y_K on E/K.

The following limit formula was proved by Gross and Zagier ([GZ86]) [[**Todo: we need gross-zagier for $(D,N) = 1$. do we dig up another reference for this, or just assert it? include the theorem below, but dig up a reference for the general case. Maybe in a paper of Zhang of Columbia University.**]]

Theorem 3.1 (Gross-Zagier)**.** *If $(D, 2N) = 1$ then*

$$\hat{h}(y_K) = \frac{u^2\sqrt{D}}{c\int_{E(\mathbb{C})} \omega \wedge i\overline{\omega}} L'(E/K,1) = \alpha L'(E/K,1),$$

(where ω is the invariant differential associated with the elliptic curve and u is half the number of units of $\mathcal{O}_K$).

The following decomposition theorem relates the behavior of the L-function for E/K and $E/\mathbf{Q}$:

Proposition 3.2.

$$E(K) \otimes \mathbf{Z}\left[\frac{1}{2}\right] = E(\mathbf{Q}) \otimes \mathbf{Z}\left[\frac{1}{2}\right] \oplus E^D(\mathbf{Q}) \otimes \mathbf{Z}\left[\frac{1}{2}\right].$$

Proof. Denote complex conjugation by τ. We will decompose $E(K)$ into its eigenspaces under the action of τ. Note that tensoring with $\mathbf{Z}\left[\frac{1}{2}\right]$ kills 2-torsion. For $P \in E(K)$ we have the following decomposition into +1 and -1 eigenspaces of τ:

$$P = \frac{1+\tau}{2}P + \frac{1-\tau}{2}P.$$

But if $P = (x,y) \in E(K)$ satisfies $\tau P = P$, then $P \in E(\mathbf{Q})$; if $\tau P = -P = (x,-y)$, then $x \in \mathbf{Q}$ and $y \in \sqrt{D}\mathbf{Q}$. In particular, $(Dx, D\sqrt{D}y) \in E^D(\mathbf{Q})$, and conversely we can obtain any such point in the -1 eigenspace of $E(K)$ from a point of $E^D(\mathbf{Q})$. We may rewrite the decomposition into eigenspaces as the statement of the proposition. □

[[**Todo: Add result about the index of $E(\mathbf{Q})$ or $E^D(\mathbf{Q})$ in $E(K)$, and make the above into a more precise result for whenever E has no 2-torsion.**]]

Assume that $L'(E^D/\mathbf{Q},1) \neq 0$. For elliptic curves of rank 0 or 1 (the only ones for which we will check the full BSD conjecture) this implies that $E(K)$ has rank 1 and exactly one of the groups $E(\mathbf{Q}), E^D(\mathbf{Q})$ has rank 1. By the Gross-Zagier formula, the Heegner point y_K will have infinite order.

The parity of the root number (the sign of the functional equation of the L-function) is the same as the parity of the rank of $E/\mathbf{Q}$.

(1) If the root number is -1 then a generator of $E(K) \otimes \mathbf{Z}\left[\frac{1}{2}\right]$ comes from a generator of $E(\mathbf{Q}) \otimes \mathbf{Z}\left[\frac{1}{2}\right]$ and
$$L'(E/K, 1) = L'(E/\mathbf{Q}, 1)L(E^D/\mathbf{Q}, 1).$$
(2) If the root number is $+1$ then a generator of $E(K) \otimes \mathbf{Z}\left[\frac{1}{2}\right]$ comes from a generator of $E^D(\mathbf{Q}) \otimes \mathbf{Z}\left[\frac{1}{2}\right]$ and
$$L'(E/K, 1) = L(E/\mathbf{Q}, 1)L'(E^D/\mathbf{Q}, 1).$$

Note that this method is faster than computing the rank directly.

3.2. **The Index of the Heegner point.** The Birch and Swinnerton-Dyer conjecture may be rephrased [**?**] using the Gross-Zagier formula as

Conjecture 3.3 (Birch-Swinnerton-Dyer)**.** *For E an elliptic curve of rank 1 over K, a quadratic extension of $\mathbf{Q}$, we have*
$$|\text{Ш}(E/K)| = \left(\frac{[E(K) : \mathbf{Z}y_K]}{c\prod c_p}\right)^2.$$
Here the c_p are the Tamagawa numbers, and c is the Manin constant.

To compute $\text{Ш}(E/\mathbf{Q})$, we will use a refinement of Gross's argument in []. For this we need to compute $[E(K) : \mathbf{Z}y_K]$ efficiently.

Note that $[E(K) : \mathbf{Z}y_K]^2 = h(y_K)/h(z)$, where z is a generator of $E(K)$. We saw that we may compute z up to a power of 2, which implies that we may compute $h(z) = 2h_{\mathbf{Q}}(z)$ up to a power of 2.

All that is left is a computation of L-functions and of $\alpha = \frac{u^2\sqrt{|D|}}{c\int_{E(\mathbb{C})}\omega\wedge i\overline{\omega}}$. We may compute

$$\begin{aligned}\int_{E(\mathbb{C})} \omega \wedge i\overline{\omega} &= \int_{E(\mathbb{C})} \frac{dx}{y} \wedge i\frac{\overline{dx}}{y} = i\int_{\mathbb{C}/\Lambda} \wp'(z)\frac{dz}{\wp'(z)} \wedge \overline{\wp'(z)\frac{dz}{\wp'(z)}} \\ &= i\int_{\mathbb{C}/\Lambda} dz \wedge d\bar{z} = \int (dx + idy) \wedge (idx + dy) = 2\int dx \wedge dy = 2a,\end{aligned}$$

where a is the volume of the lattice $\mathbb{C}/\Lambda$.

3.3. **Precision.** In the course of our computations of $[E(K) : \mathbf{Z}y_K] = \sqrt{h(y_K)/h(z)}$ we need to compute the heights with sufficient precision to obtain the square of $[E(K) : \mathbf{Z}y_K]$ after rounding.

Assume that the rank of E is 0, which is the case for most of the curves in our databases.

Then $[E(K) : \mathbf{Z}y_K]^2 = h(y_K)/h(z) = \alpha L(E/\mathbf{Q}, 1)L'(E^D/\mathbf{Q}, 1)/h(z)$.

(1) To find α all we need to do is find the area of the period lattice, which can be done with fast convergence ([**?**], section 3.7).
(2) To find a generator z of $E/\mathbf{Q}$ we use Cremona's mwrank ([**?**]).
(3) The computation of the height of a generator of $E/\mathbf{Q}$ is described in detail in [**?**] (section 3.4). Moreover, the truncation error is exponentially small; there is an explicit bound on truncation that ensures an error of at most $10^{-k}/2$. **[[Todo: what is k? number of terms?]]**

(4) Using [?] section 2.13 we get that
$$L(E/\mathbf{Q},1) = 2\sum \frac{a_n}{n} e^{-2\pi n/\sqrt{N}},$$
(where a_n are the Fourier coefficients of the normalized newform associated with E). We have the trivial bound $|a_n| \leq n$ and so the truncation error is $2\sum e^{-2\pi n/\sqrt{N}} = 2/(1-e^{-2\pi/\sqrt{N}})e^{-2\pi k/\sqrt{N}}$. [[**Todo: Explain the trivial bound, which is likely true... Use that $|a_p| < 2\sqrt{p}$ and recursion.**]]

(5) If F is an elliptic curve of rank 1 and conductor N, then a similar formula in the same section yields that
$$L'(F/\mathbf{Q},1) = 2\sum \frac{a_n}{n} G_1(2\pi n/\sqrt{N}),$$
where $G_1(x) = \int_1^\infty e^{-xy}dy/y \leq e^{-x}/x$. Therefore we may get the same truncation bound as before. We apply this to the curve $F = E^D$

4. Kolyvagin's Method and Consequences

4.1. **Kolyvagin's approach to $Ш_{\mathbf{tors}}$.** Let E be an elliptic curve and K be a quadratic extension staisfying the Heegner hypothesis such that $L'(E/K,1) \neq 0$. Then y_K has infinite order. Kolyvagin ([Kol90]) shows that in this case the rank of $E(K)$ is 1 and $Ш(E/K)$ is finite.

Following Gross's account of Kolyvagin's work ([Gro91]), we get the following bounds on $|Ш(E/K)|$.

Assume that E does not have complex multiplication.[[**Todo: we don't want this to sound like we're assuming CM in what follows; this is only for the description of gross's work. is the description of K's argument below necessary? YES, add something about how we will strengthen his argument to say something in the CM case, though he did not.**]] Let $I_K = [E(K) : \mathbf{Z}y_K]$. There exists an integer $t_{E/K}$ divisible only by primes p (shown to be finite by Serre in [Ser72]) such that the representation $G(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(E[p])$ is not surjective; then $|Ш(E/K)|\ |t_{E/K}I_K^2$. [[**Todo: looks weird – change all cardinialities to use # notation. Use $|$ and $\nmid$ for divides and doesn't divide.**]]

The main assumption on the p where Kolyvagin *does* prove triviality of p-torsion of Ш (i.e., the surjectivity of the mod p representation) is used in two places in the argument.[[**Todo: make clear that this is gross's argument, not kolyvagin's**]] [[**Todo: these 2 exact sequences below are awkwardly long**]]

(1) The construction of the cohomology classes requires that restriction Res : $H^1(K,E[p]) \to H^1(K_n,E[p])^{G(K_n/K)}$ is an isomorphism, where K_n is the ring class field of conductor n over K. The mod p representation $G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_p)$ is surjective so $E(K_n)[p] = 0$, hence the inflation-restriction-transgression sequence implies that $H^1(K,E[p]) \to H^1(K_n,E[p])^{G(K_n/K)}$ is an isomorphism.

(2) Surjectivity is used in the definition of a nondegenerate pairing
$$H^1(K,E[p]) \otimes G(K(E[p])) \to E[p].$$
For simplicity of notation write $L = K(E[p])$. Again, the inflation restriction sequence yields
$$H^1(L/K,E(L)[p]) \to H^1(K,E[p]) \to H^1(L,E[p])^{G(L/K)} \to H^2(L/K,E(L)[p]).$$

Since $G(L)$ acts trivially on $E[p]$, it is enough to prove that $H^i(L/K, E[p]) = 0$. The surjectivity of the mod p representation implies that $G = G(L/K) = G(\mathbf{Q}(E[p])/\mathbf{Q}) \equiv GL_2(\mathbf{F}_p)$. If Z is the group of scalars the Hochschild-Serre spectral sequence $H^i(G/Z, H^j(Z, E[p])) \Longrightarrow H^{i+j}(L/K, E[p])$ will give the result since $|Z| = p-1$ and $E[p]$ is a p-group. [[**Todo: do we want to describe gross's argument like this, or just state the result needed? ok as is, I think.**]]

4.2. **Computational Difficulties.** [[**Todo: rephrase this**]] The main computational problem of this method is that there is no universal bound on p so that the mod p representation is surjective for all elliptic curves and primes larger than the bound.

There are a few results towards this bound:

(1) For E semi-stable the representation is surjective if $p \geq 11$ ([Gro91]).
(2) For general E, the representation is surjective when $p \geq 1+\frac{4\sqrt{6}N}{3}\prod_{l|N}\left(1+\frac{1}{l}\right)$ ([**?**]).[[**Todo: cite something besides grigor's paper**]]

Kolyvagin's method yields triviality of the p-primary component of $\text{Ш}(E/\mathbf{Q})$ for all primes that do not divide I_K and for which the mod p representation is surjective. For these primes, information about Ш may be obtained by using descents, which are very hard in general.

The equivalent statement of the BSD conjecture (3.3) implies that I_K will always be divisible by the Tamagawa numbers c_p. Therefore we may hope to reduce work by weakening the surjectivity hypothesis and by dealing with the primes that divide I_K but not $\prod c_p$. [[**Todo: awkward**]]

5. Weakening the Hypotheses of Kolyvagin's Method

In Gross's treatment of Kolyvagin's work, Gross uses the surjectivity of the mod p representation only to prove that $H^i(K(E[p])/K, E[p]) = 0$ and $H^i(K_n/K, E(K_n)[p]) = 0$. Our goal, therefore, is to determine weaker, and easily computable, conditions under which these cohomology groups are trivial.

5.1. **Irreducibility of the mod p representation.** In a recent thesis, Cha ([**?**]) has in certain cases provided weaker conditions under which Kolyvagin's results hold. Let K be any finite extension of $\mathbf{Q}$ and let p be an odd prime. Cha assumes that

(1) There is an unramified prime divisor v of p in $K/\mathbf{Q}$ such that E has either good or multiplicative reduction at v.
(2) $E(K)[p] = 0$.

He then proves the following two theorems:

(1) $H^1(K(E[p^i])/K, E[p^i]) = 0$ for all $i \geq 1$ unless $p = 3$ and $G(K(E[p])/K) \cong G_{except}$, where G_{except} is the subgroup of $GL_2(\mathbf{F}_p)$ given by
$$G_{except} = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} | a \in \mathbf{F}_p^*, b \in \mathbf{F}_p \right\}.$$
(2) When K is an imaginary quadratic extension of $\mathbf{Q}$ satisfying the Heegner hypothesis, such that $E(K)$ has rank 1, let $y_K \in E(K)$ denote the usual Heegner point. Let $m = \mathrm{ord}_p[E(K) : \mathbf{Z}y_K]$ be the largest integer such that $y_K \in p^m E(K)$ ($E(K)[p] = 0$, by assumption); also assume p does not

divide the discriminant of K and E has good or multiplicative reduction at p. Then if the Galois representation

$$\rho_p : G(\bar{\mathbf{Q}}/\mathbf{Q}) \to Aut(E[p])$$

is irreducible,

$$\mathrm{ord}_p |Ш(E/K)| \leq 2m.$$

Kolyvagin proved the following effective version of his theorem (see [Kol90]):

Theorem 5.1 (Kolyvagin)**.** *Let R be the ring of endomorphisms of E, with F its field of fractions. Suppose the Heegner point y_K has infinite order. Then if p is an odd prime unramified in F such that $G(F(E[p])/F) = Aut_R(E[p])$,*

$$\mathrm{ord}_p |Ш(E/K)| \leq 2 \,\mathrm{ord}_p [E(K) : \mathbf{Z} y_K].$$

Assuming E does not have complex multiplication, the hypotheses of both these theorems imply $E(K)[p] = 0$, so, in particular, $Ш(E/K)$ has no p-torsion if $p \nmid [E(K) : \mathbf{Z} y_K]$ (for a proof that irreducibility of the mod-p representation over $\mathbf{Q}$ implies $E(K)[p] = 0$, see Lemma 5.9).

[[**Todo: add sentence: what "these" are.**]] These are generally dealt with by p-descent, however, and Cha's assumption on the reduction of E at a given prime makes the result ineffective for potentially large prime divisors of the conductor of E (for which E has additive reduction). The assumption on irreducibility of the Galois representation is, from a computational perspective, a great improvement on Kolyvagin's original assumption, but we can further improve this hypothesis to one about torsion over K.

5.2. Reducing the hypotheses to statements about torsion.

5.2.1. *The mod p representation.*

Lemma 5.2. *The determinant of the mod p representation attached to E is the cyclotomic character, and is therefore surjective.*

Proof. The Weil pairing induces an isomorphism of $G(\bar{\mathbf{Q}}/\mathbf{Q})$-modules $E[p] \wedge E[p] \cong \mu_p$. Let us fix a basis $\{e_1, e_2\}$ of $E[p]$, with respect to which $\rho_p(\sigma)$ has the form $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then

$$\sigma(e_1 \wedge e_2) = (ae_1 + ce_2) \wedge (be_1 + de_2) = \det(\rho_p(\sigma)) e_1 \wedge e_2.$$

It follows that composition with the determinant gives the cyclotomic character (i.e., the action of $G(\bar{\mathbf{Q}}/\mathbf{Q})$ on μ_p), which is clearly surjective.

□

Ultimately, we will choose the quadratic field K to be linearly disjoint from $\mathbf{Q}(E[p])$, so $G(K(E[p]/K) \cong G(\mathbf{Q}(E[p])/\mathbf{Q})$. Thus, it will suffice to show vanishing of $H^i(\mathbf{Q}(E[p])/\mathbf{Q}, E[p])$.

Let $G = G(\mathbf{Q}(E[p])/\mathbf{Q})$ be the image of the mod p representation. If $p \nmid |G|$, then $H^i(G, E[p]) = 0$ since $E[p]$ is a p-group. Therefore we may assume $p \mid \#G$. By Proposition 15 of [Ser72], G either contains $SL_2(\mathbf{F}_p)$ or is contained in a Borel subgroup of $GL_2(\mathbf{F}_p)$. [[**Todo: should we define borel subgroups of GL? definitely, but only in the "extra" part.**]] If G contains $SL_2(\mathbf{F}_p)$ then Lemma 5.2 implies that $\det : G \to \mathbf{F}_p^*$ is surjective, so $G = GL_2(\mathbf{F}_p)$. [[**Todo: is now a more appropriate time to note what andrei has shifted to proposition 5.5?**]] [[**Todo: should we throw out this lemma, since it's already proven**

in gross's paper? it's the surjective representation case, which we already know. YES, but just move it to "extra".]]

Lemma 5.3. *If $G = GL_2(\mathbf{F}_p)$ then $H^i(G, E[p]) = 0$.*

Proof. Let Z be the subgroup of scalars. Clearly $E[p]^Z = 0$. Consider the Hochshild-Serre spectral sequence

$$H^i(G/Z, H^j(Z, E[p])) \Longrightarrow H^{i+j}(G, E[p]);$$

If $j > 0$ then the group $H^j(Z, E[p]) = 0$ because $|Z| = p - 1$ and $E[p]$ is a p-group. If $j = 0$ then $H^j(Z, E[p]) = E[p]^Z = 0$. Therefore $H^i(G, E[p]) = 0$. □

Lemma 5.4. *Assume that G is contained in a Borel subgroup of $GL_2(\mathbf{F}_p)$. Moreover, assume that (with respect to some basis of $E[p]$), G acts as $\left(\begin{smallmatrix} \chi & * \\ 0 & \psi \end{smallmatrix}\right)$ such that χ and ψ are nontrivial characters. Then $H^i(G, E[p]) = 0$.*

Proof. Let W be the (unique) p-Sylow subgroup of $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$.

We may assume $W \subset G$, for otherwise G has order prime to p, and the cohomology clearly vanishes.

We begin by explicitly computing $H^j(W, E[p])$ using the fact that W is cyclic (generated by $w = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, for instance). Recall that for cyclic groups we can compute cohomology using the particularly simple projective resolution

$$... \to \mathbf{Z}[W] \to \mathbf{Z}[W] \to \mathbf{Z} \to 0$$

where the boundary maps alternate between $w - 1$ and $\mathrm{Norm} = \sum_{i=0}^{p-1} w^i$ (i.e., the maps are given by multiplication in the group ring $\mathbf{Z}[W]$). Then we immediately see that

$$H^j(W, E[p]) = \left\{ \begin{array}{ll} \ker(1-w)/\mathrm{im}(\mathrm{Norm}(w)) = \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle & \text{if } j \text{ is even;} \\ \ker(\mathrm{Norm}(w))/\mathrm{im}(1-w) = \mathbf{F}_p^2 / \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle & \text{if } j \text{ is odd} \end{array} \right\}.$$

Since χ and ψ are nontrivial by assumption, the G/W-invariants for both of these groups are trivial. Thus, $H^j(W, E[p])^{G/W} = 0$ for $j \geq 0$. Let us then consider the Hochschild-Serre spectral sequence

$$H^i(G/W, H^j(W, \mathbf{F}_p^2)) \Rightarrow H^{i+j}(G, \mathbf{F}_p^2).$$

For $i > 0$, since $|G/W|$ is prime to p, and $H^j(W, \mathbf{F}_p^2)$ is a p-group ($\forall j$), the group $H^i(G/W, H^j(W, \mathbf{F}_p^2))$ is trivial. But when $i = 0$ we have just computed that $H^i(G/W, H^j(W, \mathbf{F}_p^2)) = H^j(W, \mathbf{F}_p^2)^{G/W} = 0$, so the entire spectral sequence is trivial, and we conclude that $H^n(G, E[p]) = 0$ for all $n \geq 0$. □

5.2.2. *Vanishing of Cohomology Groups I.* The next propositions show how to reduce the hypothesis that $H^i(\mathbf{Q}(E[p])/\mathbf{Q}) = 0$ to a statement about torsion and rational isogeny. In terms of the mod p representation, the fact that E has no $\mathbf{Q}$-rational p-isogeny corresponds to the irreducubility of the representation.

Proposition 5.5. *Suppose E has no $\mathbf{Q}$-rational p-isogeny. Then $H^i(\mathbf{Q}(E[p])/\mathbf{Q}, E[p]) = 0$ for all $i > 0$.*

Proof. The assumption implies that the mod p representation is irreducible.

As we already noted, the problem reduces to the case when either G is contained in a Borel subgroup or $G = GL_2(\mathbf{F}_p)$. The latter case follows from Lemma 5.3. The former case contradicts the hypothesis since $E[p]$ is reducible under the action of a Borel subgroup. □

For the above result, we used the irreducibility of the representation to deal with the case when G was not contained in a Borel subgroup. The following proposition completes the proof of the general case:

Proposition 5.6. *Suppose that for all elliptic curves E' p-isogenous to E over $\mathbf{Q}$ we have $E'(\mathbf{Q})[p] = 0$. Then $H^i(\mathbf{Q}(E[p]/\mathbf{Q}, E[p]) = 0$ for all $i > 0$.*

Proof. The proof of the previous proposition works here except for the case when G is contained in a Borel subgroup. For some basis of $E[p]$, G acts as $\left(\begin{smallmatrix} \chi & * \\ 0 & \psi \end{smallmatrix}\right)$ for characters χ and ψ. Lemma 5.4 proves the proposition if the characters are not trivial.

Assume that χ is trivial. Then all matrices of the above form fix $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$. Therefore there is a point of $E[p]$ fixed by the action of G, which contradicts the assumption that $E(\mathbf{Q})[p] = 0$.

Assume that ψ is trivial. Matrices of the above form preserve the line generated by $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$, so this line forms a $G(\bar{\mathbf{Q}}/\mathbf{Q})$-stable subspace of $E[p]$. In particular, there exists an isogeny over $\mathbf{Q}$ to a curve E' having this line as kernel. The image of the complementary line generated by $\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$ is a 1-dimensional subspace of $E'[p]$, and if $\psi = 1$, $G(\bar{\mathbf{Q}}/\mathbf{Q})$ clearly acts trivially on this subspace (we have an isomorphism of Galois modules $E/\left\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \right\rangle \cong E'$). Thus, $E'(\mathbf{Q})[p]$ is nontrivial, contradicting our assumption.

□

5.2.3. *Vanishing of Cohomology Groups II.* We will verify that $H^i(K_n/K, E(K_n)[p]) = 0$ under a simple condition on p-torsion over K.

Proposition 5.7. *Let E be an elliptic curve with $E(K)[p] = 0$, where $p > 3$ or, if $p = 3$, $K \neq \mathbf{Q}(\mu_3)$. Let L be a finite abelian extension of K. Then $H^i(L/K, E(L)[p]) = 0$ for all $i \geq 1$.*

Proof. The proof is similar to the previous use of Sylow groups and the Hochschild-Serre spectral sequence. [[**Todo: do we want to replace the spectral sequence with a more down-to-earth inf-res argument, or keep the exposition uniform? – I'd say to use inf-res here. Include the spectral sequence version in the extra version.**]] Write the abelian group $G(L/K)$ as a direct sum $P \oplus P'$, where P is its Sylow p-subgroup, so $(p, \#P') = 1$. We claim that the subgroup of $E(L)[p]$ invariant under P' is trivial. Let $G = G(L/K)/H$, where H is the subgroup of $G(L/K)$ that acts trivially on $E(L)[p]$. If $(\#G, p) = 1$, $P \subseteq H$, so P' surjects onto G. As there is no nontrivial element of $E(L)[p]$ invariant under all of $G(L/K)$ (by the assumption on $E(K)[p]$), the same then holds for P'.

If $p | \#G$, we cannot have $E(L)[p] = \mathbf{F}_p$: the latter group has automorphism group isomorphic to $\mathbf{F}_p^*$, of order $p-1$, but if $p | \#G$, G would give rise to at least p distinct automorphisms. Thus, $E(L)[p]$ is the full p-torsion subgroup of E, and we can identify G with a subgroup of $GL_2(\mathbf{F}_p)$ acting on $E(L)[p] = (\mathbf{F}_p)^2$.

We can choose a basis of $(\mathbf{F}_p)^2$ so that G contains the subgroup $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$ where $x \in \mathbf{F}_p$. Being abelian, G must be contained in the normalizer of this subgroup, so $G \subseteq \{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) : a \in \mathbf{F}_p^*, b \in \mathbf{F}_p\}$, and we claim that G contains an element with $a \neq 1$. Since $E[p] = E(L)[p]$, the representation $G(\bar{\mathbf{Q}}/K) \to \mathrm{Aut}(E[p])$ factors through $G(L/K)$ (recall that the image of the representation is $G(K(E[p])/K)$). The determinant of the mod-p representation of $G(\bar{\mathbf{Q}}/\mathbf{Q})$ is surjective (onto $\mathbf{F}_p^*$), and $[K : \mathbf{Q}] = 2$, so the character $G(\bar{K}/K) \to \mathbf{F}_p^*$ has image of index at most 2 in F_p^*. That is, it contains at least $\frac{p-1}{2}$ elements, the squares in $\mathbf{F}_p^*$. Thus, for $p > 3$, G contains an element with non-trivial determinant having the form $\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right)$ with $a \neq 1$. Now, $\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right)^p = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ since we're working mod p, and it follows that $G(L/K)$ contains an element that acts as a nontrivial scalar. In particular, since the group of scalars of $GL_2(\mathbf{F}_p)$ has $p-1$ elements, this nontrivial scalar must be an element of P'. Therefore $E(L)[p]^{P'} = 0$.

The result will now follow from the Hochschild-Serre spectral sequence

$$H^i(P', H^j(P, E(L)[p]^{P'})) \Longrightarrow H^{i+j}(L/K, E(L)[p]).$$

Then we must have $H^n(L/K, E(L)[p]) = 0$ for $n > 0$.

If $p = 3$, $E(L)[3] = E[3] \Rightarrow \mu_3 \subset L \Rightarrow K = \mathbf{Q}(\mu_3)$. The last implication holds because $G(L/\mathbf{Q})$ is abelian since $G(K_n/K)$ and $G(K/\mathbf{Q})$ are, so it has a unique index 2 subgroup; both K and $\mathbf{Q}(\mu_3)$ correspond to index 2 subgroups by elementary Galois theory. This contradicts our assumption on K. □

Corollary 5.8. [[**Todo: state hypothesis.**]]

$$H^i(K_n/K, E(K_n)[p]) = 0.$$

The relation between the two section is given by the following lemma: [[**Todo: this sentence is awkward; should we say something about the converse to the following statement NOT holding?**]]

Lemma 5.9. *Let $E/\mathbf{Q}$ be an elliptic curve, K a quadratic extension of $\mathbf{Q}$, and $p > 3$ an odd prime such that $E(K)[p] \neq 0$. Then the mod-p representation over $\mathbf{Q}$ is reducible. In particular, E has a $\mathbf{Q}$-rational p-isogeny.*

Proof. Let P be a nontrivial element of $E(K)[p]$, and let τ be a lift of complex conjugation in $G(K/\mathbf{Q})$ to $G(\bar{\mathbf{Q}}/\mathbf{Q})$. If τP is a multiple of P, then the one-dimensional subspace of $E[p]$ generated by P is $G(\bar{\mathbf{Q}}/\mathbf{Q})$-stable, so the representation over $\mathbf{Q}$ is reducible. Else, P and τP generate all of $E[p]$. By definition, $\tau P \in E(K)$, so $E(K)[p] = E[p]$, and because of the Weil pairing, $\mu_p \subset K$. For $p > 3$, this is a contradiction. □

[[**Todo: summarize the relation between the lemma and $E[p]$ being irreducible.**]]

In summary, we can now apply Kolyvagin's [[**Todo: Gross's?**]] arguments (as given in [Gro91]) to show that $Ш(E/\mathbf{Q})[p] = 0$ for all odd primes p such that all curves in the $\mathbf{Q}$-isogeny class of E have no K-rational p-torsion and $p \nmid I_K$

5.2.4. *Existence of K.*

Here we collect the results that imply the existence of quadratic imaginary extensions $K/\mathbf{Q}$ such that K satisfies the Heegner hypothesis and $\operatorname{ord}_{s=1} L(E/K) = 1$. Then the Heegner point y_K has infinite order, so we may apply the work of Kolyvagin to conclude that $Ш(E/K)$ is finite and $E(K)$ has rank 1. There are two cases to consider:

(1) If $\operatorname{ord}_{s=1} L(E/\mathbf{Q}) = 0$, then the papers [**?**] and [**?**] both imply the existence of infinitely many distinct K (that is, with different fundamental discriminants) satisfying our two hypotheses.
(2) If $\operatorname{ord}_{s=1} L(E/\mathbf{Q}) = 1$, then a result of Waldspurger ([**?**]) does the trick[[**Todo: too colloquial**]], as does the above result of Bump-Friedberg-Hoffstein.

See also [**?**] for a clear overview of how all of these results– along with the work of Gross-Zagier and Kolyvagin– fit together to settle the weak BSD conjecture for elliptic curves of analytic rank 0 or 1.

In our computations, however, we do not merely take any K satisfying the Heegner hypothesis and the analytic rank hypothesis. We instead choose K to be linearly disjoint from the fields $\mathbf{Q}(E[p])$ for all primes p, and we have observed [[**Todo: reformat this section; at this point in the paper we haven't actually made this observation yet**]] that a simple way to ensure this is to require the discriminant of K ($:= D$) to be divisible by at least 2 distinct odd primes. A conjecture of Goldfeld says that the density of discriminants D such that $K = \mathbf{Q}(\sqrt{D})$ satisfies our hypotheses is roughly $\frac{1}{2}$ (see [**?**]). Thus far the best proven result is due to Ono and Skinner, who showed ([**?**]) that, in the case $\mathrm{ord}_{s=1} L(E/\mathbf{Q}) = 0$, the number of such discriminants has density at least on the order of magnitude of $\frac{1}{\log X}$. Unfortunately, this is precisely the density of the prime numbers, so a density argument will not help us here (Ono and Skinner's result also does not distinguish between discriminants that give rise to the same imaginary quadratic extension). Note that Ono later improved this theorem (by a small power of $\log X$) under the assumption that $E/\mathbf{Q}[2] = 0$ (see [**?**]).

In the worst case, the only K that exist and satisfy both of our hypotheses have only a single odd prime divisor p of their discriminants. But then for $\ell \neq p$, K is linearly disjoint from $\mathbf{Q}(E[\ell])$, so we can run our algorithm as before, only adding p to the list of "bad primes" on which we have to perform descents. We have used the fact that the only ramified primes in $\mathbf{Q}(E[\ell])/\mathbf{Q}$ are, by the criterion of Néron-Ogg-Shafarevich (see [Sil92]), primes dividing the conductor N of E and ℓ itself.

This bad prime p might be large, however, making the p-descent cumbersome. In that case, it would be better in practice to produce a second field K' satisfying our hypotheses (recall that infinitely many exist). Unless $K' = K$, K' is linearly disjoint from $\mathbf{Q}(E[p])$ since p will not ramify in K'. There is a good chance that we might be able to show $Ш(E/K)[p] = 0$, but it is possible that a curve in E's isogeny class has p-torsion or that y_K is a multiple of p in $E(K)$. There are universal bounds on the possible p-torsion for quadratic fields, so the problematic primes resulting from torsion will still be 'small,' but the ever-mysterious index of the Heegner point may keep us from getting information at large primes (in particular, the contributions from nontrivial elements of the Shafarevich-Tate group, or large Tamagawa numbers). In practice, the bad primes are usually small, but see [[**Todo: later section for tamagawa discussion**]].

6. Elliptic Curves with Complex Multiplication

Unlike Gross's result, which relies on Serre's theorem for elliptic curves without complex multiplication, the results of section 5.2 do not make any assumptions on $\mathrm{End}(E)$. In the case of curves with complex multiplication, however, Rubin has obtained much stronger results (see [Rub91]).

Perrin-Riou proves [**?**] the following corollaries to the p-adic Gross-Zagier type formula: [[**Todo: necessary? or just state Rubin's results? move to extra.**]]

Proposition 6.1. (1) *If f is the normalized newform attached to an elliptic curve with complex multiplication then L_p has analytic rank 1 if and only if L has analytic rank 1.*

(2) *If the rank of L_p is 1 then the p-part of the Birch and Swinnerton-Dyer conjecture is true up to a unit of $\mathbf{Z}_p$.*

This follows from the Gross-Zagier type formula and a similar formula for the algebraic p-adic L-series obtained in [**?**].

Rubin proves the following theorem ([Rub91])

[[**Todo: in item** 1 **of the theorem, should it be** $L(E/\mathbf{Q}, 1) \neq 0$**; i.e., isn't this the rank** 0 **case? no, it's** K **– emphasize this!!!**]]

Theorem 6.2. *Let E have complex multiplication by K. (Since the Birch and Swinnerton-Dyer conjecture is isogeny-invariant we may assume that $End(E) = \mathcal{O}_K$.)*

(1) *If $L(E/K, 1) \neq 0$ then for all primes $\mathfrak{p}$ not dividing $|\mathcal{O}_K^\times|$ we have*
$$|\text{Ш}[\mathfrak{p}^\infty]| = \mathbb{N}(\mathfrak{p})^{m(\mathfrak{p})},$$
where $m(\mathfrak{p}) = \mathrm{ord}_{\mathfrak{p}}\left(|E(K)|\frac{L(\bar{\psi},1)}{\Omega}\right)$, where ψ is the Hecke character associated to E.

(2) *If the analytic rank of E over K is 1 then Perrin-Riou's work together with the conjecture of Mazur and Swinnerton-Dyer implies that $\text{Ш}(E/\mathbf{Q})[p]$ is as expected from the BSD conjecture whenever $p > 2$ splits in K.*

[[**Todo: insert brief discussion of how rubin's results help, for example:**]]

If we choose K such that $\mathcal{O}_K^* = \{\pm 1\}$, case (1) of Rubin's result proves, modulo the 2-component of Ш, the full BSD conjecture for CM curves with analytic rank 0. Part (2) of the theorem cannot be so systematically applied because of the condition that p split in K, but at an *ad hoc* level it may help us resolve certain troublesome cases that arise in our computations.

7. Kato's Theorem

[[**Todo: write this section**]]

8. Algorithm to Bound Ш

Algorithm 8.1. Let E be an elliptic curve over $\mathbf{Q}$ of analytic rank at most 1. The following algorithm computes $|\text{Ш}(E/\mathbf{Q})[p]|$ for *all* primes p.

(1) [Choose K] Choose two quadratic imaginary fields K that satisfy the Heegner hypothesis, such that E/K has analytic rank 1.
(2) [Find p-torsion] Decide for which primes p there is a curve E' that is $\mathbf{Q}$-isogenous to E such that $E'(\mathbf{Q})[p] \neq 0$. Let B be the product of these primes and 2.
(3) [Root number] Compute the root number of E.
(4) [Compute Mordell-Weil]
    (a) If the root number is -1, compute $E(\mathbf{Q})$ and let z be a generator modulo torsion.
    (b) If the root number is $+1$, compute $E^D(\mathbf{Q})$, and let z be a generator modulo torsion.
(5) [Height of Heegner point] Compute the [[**Todo: is silverman's** $\hat{h}$ **standard for canonical height?**]] height $h_K(y_K)$.

(6) [Index of Heegner point] Compute [[**Todo: only true up to $E(K)_{tors}$; do we want to rexpress in terms of $I'_K = [E(K)/E(K)_{tors} : \mathbf{Z}y_K]$?**]]

$$I_K = \sqrt{h_K(y_K)/h_K(z)} = [E(K) : \mathbf{Z}y_K].$$

(7) [Annihilate Ш] Then $Ш(E/\mathbf{Q})[p] = 0$ for all primes $p \nmid B \cdot I_K$.

(8) [p-descent] For each prime $p \mid B \cdot I_K$, do a p-descent and compute $Ш(E/\mathbf{Q})[p]$. [[**Todo: given the tamagawa problem, this note is false; but we should comment at some point that in many cases p-descent will be possible b/c rational p-isogenies exist (currently done in section 9.2), but in many cases not!**]] (Note that this is likely not too difficult because there is a p-torsion point over K on a curve F that is $\mathbf{Q}$-isogenous to E. Ideas: If an isogeny from E to F has degree divisible by p, then E has a rational p-isogeny, which makes p-descent easier. If an isogeny from E to F has degree coprime to p, then $Ш(F/\mathbf{Q})[p] \cong Ш(E/\mathbf{Q})[p]$, and F has a K-rational p-torsion point, so p-descent on F should be relatively easy.) To reduce the number of p for which one must do a p-descent, use several K.

Proof. Step 1 guarantees that $G(K(E[p])/K) \cong G(\mathbf{Q}(E[p])/\mathbf{Q})$. The results cited in section 5.2.4 ensure that we can always find such K. Step 2 will determine the primes for which the weakened hypothesis fails and so the primes for which we must do descent.

Since the root number and the rank have the same parity, the fact that the rank is at most 1 implies that the root number determines the rank of the curve over $\mathbf{Q}$. Therefore, by computing the Mordell-Weil group of E or E^D over $\mathbf{Q}$ (but only one of them) we can find a [[**Todo: almost**]] generator of $E(K)$. Step 6 computes the last set of primes at which we need descent.

Finally, the last step takes care of the exceptional primes. □

[[**Todo: omit the following comment? but note that in certain cases we can use Rubin or Kato to get stronger results. NO. How about it two additional steps to the algorithm, one taking into account CM possibility, the other taking into account Kato. Then reference CM and Kato sections in the proof of the algorithm.**]] For elliptic curves with complex multiplication by K, if E has rank 0 we may just do descent for the primes dividing $|\mathcal{O}_K^\times|$. If E has rank 1, then we need to take care of the primes that do not split in K. We may also apply Kolyvagin's method with our weakened (computationally viable) hypotheses to eliminate some of these primes. Then we may do descent on those.

9. Other Algorithms

9.1. **Computing the Mordell-Weil group.** While in general an unsolved problem, finding a complete set of (free) Mordell-Weil generators when the rank of the curve is already known is a fairly simple, if sometimes time-consuming, problem. Basically, one searches for points by naive height until a point of infinite order is found (the easiest way to check whether a point on $E(\mathbf{Q})$ has infinite order is to compute its multiples up to 12; if none of these is zero, the point cannot have finite order by Mazur's theorem on torsion subgroups of elliptic curves over $\mathbf{Q}$). The first point of infinite order found (call it P) may not be a generator, however: it may only generate a finite-index subgroup of $E(\mathbf{Q})$. But if it is a nontrivial multiple of a generator, the canonical height of the generator is at most $\frac{1}{4}\hat{h}(P)$ (the canonical height). By a result of Silverman [[**Todo: should we cite silverman, or the better result of siksek? we should definitely cite siksek, i.e., both.**]], the naive height of the generator may then be bounded, and an exhaustive computation will then turn it up if it exists. For more details on both the theory and implementation of this method, see [Cre97] or the updated version available on Cremona's webpage (http://www.maths.nott.ac.uk/personal/jec/book/fulltext/index.html). [[**Todo: move to bibliography.**]]

9.2. **p-descents.**

Traditionally, performing a p-descent on $E/\mathbf{Q}$ means computing the quotient group $E(\mathbf{Q})/pE(\mathbf{Q})$ by first computing the p-Selmer group and then somehow trying to get a handle on $Ш(E/\mathbf{Q})[p]$. Our task is much simpler since we already know the rank of any curve we are working with (by Kolyvagin's theorem). In particular, $\dim_{\mathbf{F}_p} E(\mathbf{Q})/pE(\mathbf{Q}) = \mathrm{rk}_{\mathbf{Z}} E(\mathbf{Q}) + \dim_{\mathbf{F}_p} E(\mathbf{Q})[p]$; we know all of these quantities, so we can compute $Ш(E/\mathbf{Q})[p]$ (our ultimate goal) by simply finding the order of the p-Selmer group and applying the fundamental exact sequence

$$0 \to E(\mathbf{Q})/pE(\mathbf{Q}) \to Sel^p(E/\mathbf{Q}) \to Ш(E/\mathbf{Q})[p] \to 0.$$

$Sel^p(E/\mathbf{Q})$ is effectively computable, so this poses no problem for the validity of our algorithm. In all cases this calculation can be reduced to "standard" computations over number fields. In particular, for S a set of "bad primes" (traditionally p and places of bad reduction for $E/\mathbf{Q}$), we have to determine the p-part of the S-class group and a basis of the S-units modulo p^{th}-powers. For a full discussion and improvements to the basic approach, see [**?**]. The method is practical when $p = 2$ or $p = 3$ (given that we are working over $\mathbf{Q}$), but for larger primes current limitations in computational number theory may make the theoretically possible calculations infeasible. Fortunately, many of our examples are exceptional cases having K-rational p-torsion. This implies they have rational p-isogenies (for a proof, see lemma 5.9), and Schaefer and Stoll, for instance, perform a successful 13-descent on a curve using the fact that it has a rational 13-isogeny.

[[**Todo: the following 2 sections were never really written; do we want as much as sections 9.1 and 9.2 for these (for consistency), or is that just a waste of space? One paragraph each. If referee complains remove.**]]

9.3. **Finding Isogenies.** Cremona ([**?**], section 3.8) describes an algorithm to compute all isogenous curves for any given elliptic curve over $\mathbf{Q}$.

[[**Todo: what is this table doing at the top of the page?**]]

9.4. **Root Number.** Cremona's reference?

10. Results of Computations

10.1. **Introduction.** This project begins with the following lofty goal:

Goal 10.1. Prove the full Birch and Swinnerton-Dyer for every elliptic curve over $\mathbf{Q}$ of conductor at most 1000.

The BSD conjecture asserts that $\mathrm{ord}_{s=1} L(E,s) = \dim E(\mathbf{Q}) \otimes \mathbf{Q}$ and

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega_E \cdot \prod c_p \cdot \mathrm{Reg}_E \cdot \#Ш(E)}{\#E(\mathbf{Q})_{\mathrm{tor}}^2}$$

The rank part is a theorem of Kolyvagin, when $\mathrm{ord}_{s=1} L(E,s) \leq 1$.

TABLE 10.1. The 4 optimal curves with nontrivial $Ш(E)_?$ and $N_E \leq 1000$

Curve	Equation	$Ш(E)_?$
571A	[0,-1,1,-929,-105954]	4
681B	[1,1,0,-1154,-15345]	9
960D	[0,-1,0,-900,-10098]	4
960N	[0,1,0,-20,-42]	4

By Tate's theorem about isogeny invariance of the BSD conjecture, to achieve the goal it suffices to prove the conjecture for each optimal elliptic curve quotient of $X_0(N)$ for $N \leq 1000$. The rank part of the conjecture (when $\mathrm{ord}_{s=1} L(E,s) > 1$) has been verified by Cremona for curves with $N \leq 25000$, and all of the quantities in the conjecture, except for $\#Ш(E/\mathbf{Q})$ have been computed for curves of conductor ≤ 25000. Inspecting that data shows that Goal 10.1 amounts to proving that $Ш(E)$ is *trivial* for all but four optimal elliptic curves with conductor at most 1000. The four exceptions are given in Table 10.1.

We can prove that $Ш(E)$ is at least as big as expected for $571A$ using the method of Cremona-Mazur or a 3-descent, and expect to be able to show that $Ш(E)$ is at most of order 9 using the thoerem stated at the beginning of McCallum's article on Kolyvagin's work, and possibly also Kato's theorem. We can hopefully show the 2-primary part of $Ш(E)$ is exactly as predicted for the other three curves by computing $\mathrm{Sel}^{(4)}(E/\mathbf{Q})$ for each of them (note that the two curves of conductor 960 have rational 2-torsion, which might simplify this computation).

Another critical obstruction to Goal 10.1 is that nobody has proved that $Ш(E)$ is finite for *any* elliptic curve of rank greater than 1. Up to isogeny, there are 18 such curves with conductor at most 1000:

389A, 433A, 446D, 563A, 571B, 643A, 655A, 664A, 681C,
707A, 709A, 718B, 794A, 817A, 916C, 944E, 997B, 997C

For these curves we have no hope, using present techniques, to show that $Ш(E)$ is trivial, let alone finite. We make the following new goal:

Goal 10.2. Prove the full Birch and Swinnerton-Dyer for every elliptic curve over $\mathbf{Q}$ of conductor at most 1000 and rank zero or one. (The rank condition excludes the 18 curves of rank two.)

10.2. **The Plan.** There are 2463 optimal curves of conductor at most 1000. Of these, 18 have rank 2, which leaves 2445 curves. Our plan for computationally verifying the full BSD conjecture for these curves is as follows:

(1) Prove a refinement of Kolyvagin's theorem, which bounds $Ш(E)$ for elliptic curves of (analytic) rank at most one. (Stefan will talk about this). Also read about Kato's theorem, which applies to E of rank 0.
(2) Create an algorithm based on a refined Kolyvagin theorem and Kato's theorem that with the following input and output (Andrei's talk is about this):
    Input: An elliptic curve over $\mathbf{Q}$.
    Output: A square-free integer B such that if a p is a prime and $p \nmid B$, then $p \nmid \#Ш(E)$.

Note that if E has (analytic) rank greater than one, then this algorithm outputs $B = 0$. When E has analytic rank at most one, it would be desirable that B only be divisible by primes such that it is reasonably easy to compute $\dim_{\mathbf{F}_p} \mathrm{Sel}^{(p)}(E/\mathbf{Q})$, e.g., when there is a rational p-isogeny; our current algorithm sometimes fails in this regard.

(3) Implement the algorithm from step 2 in MAGMA, then run it on the curves of conductor at most 1000. One step of the algorithm is to find generators for the Mordell-Weil groups of certain elliptic curves of rank one. MAGMA does not include a command that finds such generators with certainty, so we record the curve along with the generators MAGMA claims are correct.
(4) Prove correct the generators that MAGMA claims are correct, probably using a new program of Cremona for saturating Mordell-Weil groups.
(5) Compute $\dim_{\mathbf{F}_2} \mathrm{Sel}^{(2)}(E/\mathbf{Q})$ for all E, in order to prove that $\text{Ш}(E)[2] = 0$ for most E, by using the exact sequence
$$0 \to E(\mathbf{Q})/2E(\mathbf{Q}) \to \mathrm{Sel}^{(2)}(E/\mathbf{Q}) \to \text{Ш}(E)[2] \to 0.$$
(6) Analyze the output from the previous steps to see how often a difficult bound on $\text{Ш}(E/\mathbf{Q})$ arises.
(7) Prove a new theorem that allows us to show triviality of $\text{Ш}(E)$ for the curves with a difficult B. It appears that the one case in which $p \mid B$ but there is no rational p-isogeny and $\text{Ш}(E/\mathbf{Q})[p] = 0$ is when p divides some Tamagawa number and E has rank 1 (when E has rank 0, a theorem of Kato applies).
(8) Prove correctness of the order of $\text{Ш}(E)$ for the four examples with nontrivial $\text{Ш}(E)$ (see discussion above).
(9) Recode everything using only open source programs (e.g., C++, PARI), and rerun it to see that we get the same results.
(10) Publish with complete source code that other people can read and run.

10.3. **Status.** We have completed steps 1–3, and run the program on all curves of conductor up to 25000, but stop the program for a given curve after a certain amount of time (so the data is incomplete). We have so far done nothing about step 4. Regarding step 5, we have computed $\dim \mathrm{Sel}^{(2)}(E/\mathbf{Q})$ using MAGMA for most curves of conductor up to 25000, and expect this computation to finish in a few days. We have not done steps 7–10 yet. See Section 10.4 for step 6.

Remark 10.3. Tony Scholl mentioned to me last week that even if E has rank 1 over $\mathbf{Q}$, over the cyclotomic $\mathbf{Z}_p$ extension $\mathbf{Q}_\infty$ of $\mathbf{Q}$ it has bounded rank, and Kato gives information about E over $\mathbf{Q}_\infty$, i.e., about the p-adic L-function of E.

10.4. **Analysis.** This is a snapshot of the situation as of August 18, at 2pm. I ran the first computation with each job limited to 2 minutes of real time, so a heavily loaded processor would stop prematurely. I then reran the jobs that failed, but now limiting to 30 minutes, and after 18 hours all levels up to 360 had rerun (these really do take a long time). Recall that we are considering all 2463 optimal curves of level up to 1000.

- There are 18 curves of rank greater than one.

```
was$ awk '$5>=2' 00001-00999-shabound  |wc -l
18
was$ awk '$5>=2' 00001-00999-shabound
```

```
389   A   1   0   2   2   0.38  [0,0] [0,0] [0,1,1,-2,0]
433   A   1   0   2   2   0.45  [0,0] [0,0] [1,0,0,0,1]
446   D   1   0   2   2   0.59  [0,0] [0,0] [1,-1,0,-4,4]
563   A   1   0   2   2   0.48  [0,0] [0,0] [1,1,1,-15,16]
571   B   1   0   2   2   0.43  [0,0] [0,0] [0,1,1,-4,2]
643   A   1   0   2   2   0.44  [0,0] [0,0] [1,0,0,-4,3]
655   A   1   0   2   2   0.47  [0,0] [0,0] [0,0,1,-13,18]
664   A   1   0   2   2   0.61  [0,0] [0,0] [0,0,0,-7,10]
681   C   1   0   2   2   0.46  [0,0] [0,0] [0,-1,1,0,2]
707   A   1   0   2   2   0.53  [0,0] [0,0] [0,1,1,-12,12]
709   A   1   0   2   2   0.45  [0,0] [0,0] [0,-1,1,-2,0]
718   B   1   0   2   2   0.43  [0,0] [0,0] [1,0,1,-5,0]
794   A   1   0   2   2   0.54  [0,0] [0,0] [1,0,1,-3,2]
817   A   1   0   2   2   0.39  [0,0] [0,0] [0,1,1,1,6]
916   C   1   0   2   2   0.54  [0,0] [0,0] [0,0,0,-4,1]
944   E   1   0   2   2   0.54  [0,0] [0,0] [0,0,0,-19,34]
997   B   1   0   2   2   0.47  [0,0] [0,0] [0,-1,1,-5,-3]
997   C   1   0   2   2   0.44  [0,0] [0,0] [0,-1,1,-24,54]
```

- There are 318 curves for which the computation still doesn't complete in the alloted time. For these curves, we set $B = 0$ and do not include them in the lists below.

```
was$ grep timeout 00001-00999-shabound |wc -l
318
```

- There are 1363 curves for which $B = 1$ (note that B incorporates the 2-descent computation).

```
was$ awk '$4==1' 00001-00999-shabound |wc -l
1363
```

- There are curves for which B is divisible by 2 and nonzero.

```
was$ awk '$4%2==0 && $4 != 0' 00001-00999-shabound |wc -l
10
was$ awk '$4%2==0 && $4 != 0' 00001-00999-shabound
278   B   1   6   0   -1   233.0 [6,6] [-15,-15]
571   A   1   2   0   2    1.19  [14,2] [-7,-8]
786   C   1   2   1   -1   73.2  [46,94] [-23,-47]
804   B   1   6   1   -1   1.31  [6,6] [-95,-95]
873   C   1   2   1   -1   43.8  [2,22] [-8,-11]
886   C   1   2   0   -1   23.9  [14,2] [-7,-15]
906   A   1   2   1   -1   3.84  [46,142] [-23,-71]
954   E   1   6   1   -1   2.35  [282,42] [-47,-95]
960   D   1   2   0   3    2.64  [142,2] [-71,-119]
960   N   1   2   0   3    2.58  [142,2] [-71,-119]
```

The 6th column is the dimension of the 2-selmer group, and the -1 means the computation failed, hence we can't rule it. The 3 that don't have -1 really do have nontrivial Ш of order 2. There are 14 curves where computation of the 2-selmer group failed for some reason:

```
was$ awk '$6==-1' 00001-00999-shabound |wc -l
14
```

```
was$ awk '$6==-1' 00001-00999-shabound
278   B    1    6    0    -1   233.0 [6,6] [-15,-15]
645   C    1    0    0    -1   0     [0,0] [0,0] timeout
658   A    1    0    0    -1   0     [0,0] [0,0] timeout
742   F    1    0    0    -1   0     [0,0] [0,0]  timeout
774   C    1    0    0    -1   0     [0,0] [0,0] timeout
777   B    1    0    0    -1   0     [0,0] [0,0] timeout
786   C    1    2    1    -1   73.2  [46,94] [-23,-47]
804   B    1    6    1    -1   1.31  [6,6] [-95,-95]
873   C    1    2    1    -1   43.8  [2,22] [-8,-11]
886   C    1    2    0    -1   23.9  [14,2] [-7,-15]
906   A    1    2    1    -1   3.84  [46,142] [-23,-71]
942   B    1    0    0    -1   0     [0,0] [0,0] timeout
954   E    1    6    1    -1   2.35  [282,42] [-47,-95]
978   C    1    0    0    -1   0     [0,0] [0,0]  timeout
```

- There are 94 curves for which $B \geq 11$.

```
was$ awk '$4> 10' 00001-00999-shabound |wc -l
93
```

- There are 39 curves for which $B \geq 19$.

```
was$ awk '$4>=19' 00001-00999-shabound  |wc -l
39
was$ awk '$4>=19' 00001-00999-shabound
348   D  1  21 1  1    1.35  [966,2982] [-23,-71]
350   F  1  33 1  1    1.96  [2046,66] [-31,-111]
462   E  1  21 1  2    3.75  [42,42] [-215,-215]      warning
470   F  1  21 1  1    0.99  [1302,42] [-31,-39]
494   D  1  39 1  1    2.11  [8034,9906] [-103,-127]
550   I  1  21 1  1    8.89  [3318,42] [-79,-391]     warning
574   I  1  21 1  1    3.67  [1302,42] [-31,-87]
600   E  1  21 1  1    1.69  [2982,42] [-71,-119]
618   F  1  77 1  1    1.72  [10934,154] [-71,-95]    warning
650   K  1  21 1  1    3.72  [8358,42] [-199,-231]    warning
670   D  1  19 1  1    1.79  [1178,38] [-31,-111]
674   C  1  31 1  1    1.75  [434,62] [-7,-39]
682   B  1  57 1  1    10.8  [30894,114] [-271,-415]  warning
702   K  1  21 1  1    3.2   [966,8022] [-23,-191]    warning
702   M  1  57 1  1    18.9  [29982,114] [-263,-623]  warning
706   B  1  23 1  1    0.84  [46,46] [-15,-15]
715   B  1  21 1  1    1.02  [42,42] [-51,-51]
730   J  1  21 1  1    1.47  [2982,3318] [-71,-79]
735   F  1  21 1  1    10.3  [10542,42] [-251,-404]   warning
762   E  1  33 1  1    1.65  [66,66] [-95,-95]        warning
786   J  1  21 1  1    1.13  [966,1974] [-23,-47]
786   L  1  35 1  1    1.55  [1610,4970] [-23,-71]    warning
804   D  1  21 1  1    1.51  [42,42] [-95,-95]
806   D  1  33 1  1    29.9  [17358,66] [-263,-703]   warning
854   D  1  21 1  1    2.95  [1974,7014] [-47,-167]
858   F  1  55 1  1    40.0  [110,110] [-959,-959]    warning
```

```
861   C  1  35 1  1    1.58  [70,70] [-20,-20]
870   F  1  35 1  2    9.21  [16730,30170] [-239,-431]warning
886   D  1  19 1  1    3.57  [266,38] [-7,-15]
894   E  1  23 1  1    1.71  [46,46] [-95,-95]
894   G  1  77 1  1    1.64  [154,154] [-95,-95]      warning
906   H  1  55 1  1    2.48  [7810,110] [-71,-143]    warning
910   H  1  51 1  1    5.64  [20298,31722] [-199,-311]
910   K  1  35 1  2    2.48  [70,70] [-159,-159]
918   H  1  33 1  1    4.97  [3102,17358] [-47,-263]  warning
975   I  1  21 1  1    2.22  [42,42] [-116,-116]      warning
986   E  1  35 1  1    3.31  [7210,70] [-103,-111]
988   B  1  39 1  1    81.5  [6162,8034] [-79,-103]
996   B  1  39 1  1    2.35  [5538,78] [-71,-143]
```

Note that in every case the rank (column 5) is 1.

- The largest B is 77.

```
was$ sort -n -r -k 4 00001-00999-shabound |more
894   G  1  77 1  1    1.64  [154,154] [-95,-95] warning
618   F  1  77 1  1    1.72  [10934,154] [-71,-95] warning
```

- The largest prime divisor of a B is 31.

```
was$ awk '$4%17==0 && $4 != 0' 00001-00999-shabound |wc -l
5
was$ awk '$4%19==0 && $4 != 0' 00001-00999-shabound |wc -l
4
was$ awk '$4%23==0 && $4 != 0' 00001-00999-shabound |wc -l
2
was$ awk '$4%29==0 && $4 != 0' 00001-00999-shabound |wc -l
0
was$ awk '$4%31==0 && $4 != 0' 00001-00999-shabound |wc -l
1
was$ awk '$4%37==0 && $4 != 0' 00001-00999-shabound |wc -l
0
was$ awk '$4%43==0 && $4 != 0' 00001-00999-shabound |wc -l
0
was$ awk '$4%47==0 && $4 != 0' 00001-00999-shabound |wc -l
0
was$ awk '$4%53==0 && $4 != 0' 00001-00999-shabound |wc -l
0
was$ awk '$4%59==0 && $4 != 0' 00001-00999-shabound |wc -l
0
was$ awk '$4%61==0 && $4 != 0' 00001-00999-shabound |wc -l
0
was$ awk '$4%67==0 && $4 != 0' 00001-00999-shabound |wc -l
0
was$ awk '$4%71==0 && $4 != 0' 00001-00999-shabound |wc -l
0
was$ awk '$4%73==0 && $4 != 0' 00001-00999-shabound |wc -l
0
was$ awk '$4%31==0 && $4 != 0' 00001-00999-shabound
```

```
674   C  1  31 1  1    1.75  [434,62] [-7,-39]
```

10.5. **A Potentially Serious Obstruction.** We next list the most difficult curves, from our point of view. These are the curves with E of rank 1 such that B is divisible by a prime $p \geq 5$ for which no element of the $\mathbf{Q}$-isogeny class of E has a K-rational point of order p, i.e., such that divisor p of B also divides $[E(K)_{/\,\mathrm{tors}} : \mathbf{Z}y_K]$ for the two K we chose. We consider $p \geq 5$, because it is standard to do a p-descent in general for $p = 2, 3$, and we consider only rank 1, since when the rank is 0 Kato's theorem gives extremely strong results independent of the index.

There are 176 such curves in our data, for levels ≤ 1000, and for which our computation of Heegner points succeeded, and these are displayed below. The notation of the table is (E, n), where n is the greatest common divisor of the odd parts of the two indexes $[E(K)_{/\,\mathrm{tors}} : \mathbf{Z}y_K]$. Again, we emphasize that every curve below has rank 1.

141A1	7	522J1	13	702L1	15	861B1	17
190A1	11	530C1	5	702M1	57	861C1	35
214A1	7	542B1	7	705B1	15	861D1	5
238A1	7	550I1	21	705E1	5	870F1	35
258C1	5	550J1	11	706B1	23	874D1	5
262A1	11	551C1	7	706D1	5	876B1	15
274A1	7	558F1	5	710B1	17	880G1	5
280B1	15	558G1	7	710C1	7	886D1	19
285A1	5	560E1	5	715B1	21	886E1	5
286B1	13	561B1	5	726E1	5	890F1	13
302C1	5	574G1	11	726G1	15	894E1	23
303A1	7	582C1	5	730I1	7	894F1	5
309A1	5	585I1	7	730J1	63	894G1	77
318D1	11	594D1	5	735F1	21	897D1	15
322D1	5	598D1	17	738E1	5	897E1	5
326B1	5	600E1	21	738F1	11	901E1	15
346B1	7	605A1	15	742E1	5	906H1	55
348D1	21	605C1	5	742G1	5	910F1	55
350F1	33	608E1	5	762D1	5	910G1	5
354F1	7	615B1	7	762E1	33	910H1	51
357D1	7	618D1	5	777E1	5	910K1	35
362B1	7	618E1	5	777G1	5	912H1	5
364A1	15	618F1	77	786H1	7	918H1	33
366G1	5	620B1	15	786J1	21	920A1	15
381A1	5	622A1	7	786L1	35	924B1	15
408D1	5	629D1	5	794C1	5	924E1	15
414D1	5	642C1	13	798C1	5	930D1	7
418B1	13	650K1	21	798D1	5	930H1	15
430B1	5	658E1	11	798G1	15	933B1	11
430D1	75	665A1	5	804D1	21	938B1	5
434D1	5	666D1	5	806C1	5	939C1	5
446B1	7	666E1	13	806D1	33	942C1	5
458B1	5	670A1	11	814B1	5	954H1	7
462E1	21	670C1	5	816I1	11	954I1	5
470C1	7	670D1	19	817B1	5	954J1	17
470F1	21	672B1	15	822D1	5	974H1	15
474B1	5	674C1	31	830C1	5	975I1	21
490G1	5	678C1	7	831A1	5	975J1	5
494D1	39	681E1	5	834F1	7	978F1	11
497A1	5	682B1	57	842B1	13	978G1	7
498B1	5	690E1	5	850D1	7	986E1	35
506D1	5	696C1	5	850L1	7	987E1	15
506F1	13	700D1	15	854D1	21	988B1	39
522I1	5	702K1	21	858F1	55	996B1	39

If we assume the BSD conjecture, then the formulas at the beginning of McCallum's article suggest that in each case one of the following occurs:

(1) We did not choose enough K's.

(2) If p is a prime that divides the gcd of indexes, then p divides some Tamagawa number c_ℓ of E.

In the latter case all of the points P_n of McCallum's article are "divisible by p, in the sense described in that article, and Kolyvagin's method doesn't seem to yield the precise bound we require.

We now consider the first examples in more detail. The curve E called 141A and given by $y^2 + y = x^3 + x^2 - 12x + 2$ has rank 1, conductor $141 = 3 \cdot 47$, has $c_3 = 7$, and using all the results I know toward BSD we only see that Ш(E) is finite of order a power of 7. The curve E is isolated in its isogeny class. The modular degree of E is divisible by 7. The Jacobian $J_0(47)$ is of rank 0 and is simple of dimension 4, and we find that $E[7]$ sits in the old subvariety of $J_0(3 \cdot 47)$. Thus my hope is that proving something about the Shafarevich-Tate group of simple rank 0 abelian variety $J_0(47)$ will imply something about Ш$(E)[7]$. Also we have $L(J_0(47), 1)/\Omega = 16/23$, so BSD predicts that the Selmer group of $J_0(47)$ at 7 is trivial (since we know $c_{47} = 23...$).

Question 10.4 (Gross)**.** In your data, do all the Tamagawa numbers divide the index of the Heegner point?

I don't have things setup so I can trivially check whether all these indexes also come from Tamagawa numbers. However, I just tried three more examples:

- 190A1: We have $190 = 2 \cdot 5 \cdot 19$ and $c_2 = 11$. There is a 4-dimensional abelian variety over rank 0 and level 95 with Ш[11] trivial that contains $E[11]$.
- 214A1: We have $214 = 2 \cdot 107$ and $c_2 = 7$. There is a rank 0 simple abelian variety over level 107 and dimension 7 that contains $E[7]$.
- 674C1: We have $214 = 2 \cdot 337$ and $c_2 = 31$. For this one, there is a rank 0 simple abelian variety of level 337 and dimension 15 that contains $E[31]$ and according to BSD has trivial Ш[31].

Is there a connection with Gross's recent work on level raising, Heegner points, and Selmer group? First, he has the hypothesis $p \not\equiv 1 \pmod{\ell}$. For the 141A example, $p = 3$ and $\ell = 7$, which is OK. For the 190A, 214A, and 674A examples, $p = 2$ and $\ell \geq 5$ is odd, so in each case that hypothesis is satisfied.

10.6. Some Other Questions (for Dick Gross).

(1) $\int \omega \wedge \overline{(i\omega)} < 0$? *I think it's right, but maybe not...*
(2) Density $\alpha x/\log(x)$. What is α? *I don't know.*
(3) Connection between level changing idea (Section 10.5) and your (Gross's) research from one year ago. *My was sort of the other direction, but it seems similar.*
(4) CM curves: Unramified in F. Rank 0, OK; Rank 1, only get p that split. *Yes. Ben Howard adds that in principal one could use the Mazur-Rubin machinery in the case of Kolyvagin's Euler system to prove this in rank 1, but nobody has done this. In Ben Howard's thesis he pushes through this approach, but avoids Tamagawa numbers (for simplicity), and does some Iwasawa theory (for complexity).*
(5) In the Gross-Zagier formula, is it necessary that $(D, 2N) = 1$? *No. We only wrote it up that way so that D would be square free. Ben Howard adds*

that published work of Zhang should already deal with the case that D is even.

References

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[Gro91] B. H. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.

[GZ86] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. MR **87j:**11057

[Kol90] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483. MR **92g:**11109

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[Rub91] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), no. 1, 25–68. MR **92f:**11151

[Ser72] J-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.

[Sil92] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.