N.B. Some sections here are written up formally; others are just notes.

1 Introducing Ш

For an elliptic curve E defined over a number field K, let $Ш(E/K) = \ker(H^1(K,E) \to \prod_v H^1(K_v, E))$ be the Shafarevich-Tate group of E/K. 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 1.1. *Let E be an elliptic curve defined over $\mathbf{Q}$. Then the order of vanishing at $s = 1$ of $L(EQ, s)$equals the rank of $E(\mathbf{Q})$. More precisely, letting $r = rk_{\mathbf{Z}} E(\mathbf{Q})$, and phrasing the conjecture in terms of $\#Ш(E/\mathbf{Q})$,*

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

$R(E/\mathbf{Q})$ denotes the elliptic regulator, the determinant of the height pairing matrix on a set of free generators. The m_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 $m_\infty = \int_{E(\mathbf{R})} |\omega|$, where ω is the invariant differential $\frac{dx}{2y+a_1x+a_3}$ 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. Thus, if we can check the conjecture for a single curve in a given isogeny class, we will have verified it for all $\mathbf{Q}$-isogenous curves (as we will see, Kolyvagin has proven that $Ш(E/\mathbf{Q})$ is finite for curves of analytic rank at most 1).

2 Known Results for CM Elliptic Curves

NEED MORE SPECIFICALLY WHAT RUBIN GIVES– The result of Rubin in [**?**] implies, for elliptic curves with CM by the ring of integers in a quadratic imaginary field K, the full BSD conjecture up to primes dividing the number of units in the ring of integers (at worst requiring p-descent checks for $p = 2or3$). But does this hold for CM by any order, or just the ring of integers???

We will now summarize and give references for the main theoretical results that give information about Ш and the rank of elliptic curves over $\mathbf{Q}$. Progress was first made in the case of elliptic curves with complex multiplication: J. Coates and A. Wiles showed in [?] that for such an elliptic curve $E/\mathbf{Q}$, $L(E/\mathbf{Q}, 1) \neq 0 \Rightarrow E(\mathbf{Q})$ is finite. Improving on their techniques, K. Rubin proved two major results in his paper [?] about elliptic curves over $\mathbf{Q}$ with complex multiplication. Rubin's Theorem A implies that whenever $L(E/\mathbf{Q}, 1) \neq 0$, Ш$(E/\mathbf{Q})$ is finite. Theorem A also includes a local result, providing evidence for the full Birch and Swinnerton-Dyer conjecture, describing for which primes p Ш$(E/\mathbf{Q})[p]$ can be non-trivial. Note that before Rubin's result, not a single Shafarevich-Tate group was known to be finite; his local result makes Ш$(E/\mathbf{Q})$ effectively computable in some cases. Under the same hypotheses, Theorem B of Rubin's paper states that $\mathrm{rk}_{\mathbf{Z}}(E/\mathbf{Q}) \geq 2 \Rightarrow \mathrm{ord}_{s=1} L(E/\mathbf{Q}, s) \geq 2$. The previous year B. Gross and D. Zagier proved ([?]) their limit formula

$$L'(E/K, 1) = \frac{\iint_{E(\mathbf{C})} \omega \wedge \overline{i\omega}}{\sqrt{D}} \hat{h}(y_K),$$

where y_K denotes the usual Heegner point. Combining Rubin's result with the work of Coates-Wiles and the theorem, of Gross-Zagier, one obtains the

Theorem 2.1. *Let $E/\mathbf{Q}$ be an elliptic curve with complex multiplication by an order in a quadratic imaginary field. Then*

$$ord_{s=1} L(E/\mathbf{Q}, s) \leq 1 \Rightarrow rk_{\mathbf{Z}}(E/\mathbf{Q}) = ord_{s=1} L(E/\mathbf{Q}, s).$$

As we will see in the next section, Kolyvagin has extended this result to all elliptic curves over $\mathbf{Q}$.

3 Kolyvagin and Consequences

Let $K = \mathbf{Q}(\sqrt{D})$ be a quadratic extension of discriminant D. We say that K satisfies the Heegner hypothesis for an 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. Kolyvagin shows ([?]) that if y_K has infinite order (i.e., $L'(E/K, 1) \neq 0$), then $E(K)$ has rank 1. Moreover, he proves Ш(E/K) is finite, with the following bounds (we follow Gross's notation and organization of Kolyvagin's results in [?]). 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 [?]) such that the representation $G(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(E[p])$ is not surjective; then $\#$Ш$(E/K) | t_{E/K} I_K^2$. The existence of an imaginary quadratic extension K satsifying the Heegner hypothesis and such that $L'(E/K, 1) \neq 0$ is assumed in Kolyvagin's paper; this result was simultaneously proven (using different methods) in [**?**] and [**?**].

REST OF THIS SECTION MOSTLY USELESS:(Under the same hypothesis, he obtains the corresponding result for $E/\mathbf{Q}$ and $E_D/\mathbf{Q}$: $2c_3C_D$ kills $Ш(E/\mathbf{Q})$ and $Ш(E_D/\mathbf{Q})$, and both groups have order dividing $c_4 2^a C_D^2$, where a is the 2-rank of both groups. Moreover, he gives a condition for determining whether $E/\mathbf{Q}$ or its twist $E_D/\mathbf{Q}$ contains the point of infinite order. If E has modular parametrization $\gamma : X_0(N) \to E$, then $\gamma \circ w_N = \varepsilon\gamma + \gamma(0)$, where w_N is the principal (Fricke) involution on the modular curve (alternatively, ε is the eigenvalue on the normalized newform associated to E of the involution w_N). Kolyvagin deduces that $\varepsilon = 1 \Rightarrow E(\mathbf{Q})$ contains the point of infinite order, and $\varepsilon = -1 \Rightarrow E_D(\mathbf{Q})$ contains the point of infinite order. (Note that our calculations for $E/\mathbf{Q}$ will give us some info free of charge about $E_D/\mathbf{Q}$) $\varepsilon = 1$ makes our calculations easier, because while we'll be using low-level $E/\mathbf{Q}$, we don't know how high the conductor of $E_D/\mathbf{Q}$ might be.

In [**?**] Kolyvagin shows that 23 elliptic curves over $\mathbf{Q}$ have trivial Shafarevich-Tate group, and he verifies the full Birch and Swinnerton-Dyer conjecture for 5 of them, reducing the verification in other cases to a computation we will check. Note, however, that all of these curves have rank 0: they are quadratic twists of the rank 1 curve $E : y^2 = 4x^3 - 4x + 1$ having $\varepsilon = 1$. In particular, he shows for the 23 curves $E_D : -Dy^2 = 4x^3 - 4x + 1$ with $D \in \{7, 11, 47, 71, 83, 84, 127, 159, 164, 219, 231, 263, 271, 287, 292, 303, 308, 359, 371, 404, 443, 447, 471\}$, $Ш(E_D/\mathbf{Q}) = 0$. These are the twists with $D < 500$ (the extent of the tables of computations Kolyvagin had available), D prime to the conductor of E (37), and as usual ruling out $D = 3, 4$, for which $C_D = 1$. This suffices to conclude that $Ш(E_D/\mathbf{Q}) = 0$ because in Theorem B of his paper, Kolyvagin shows that for whichever of $E/\mathbf{Q}$ and $E_D/\mathbf{Q}$ that does not contain the point of infinite order, $Ш$ is killed by C_D (as opposed to c_3C_D, which works for both curves).

By explicitly working with the curve E, Kolyvagin reduces the full BSD conjecture in this case to showing $r_2(D) = 0$, where $r_2(D) = \#\{q\,\text{an odd prime} : q|D, (\frac{q}{37}) = 1, \text{and}\, a_q\, \text{is even}\}$. $(\frac{q}{37})$ denotes the Legendre symbol, and a_q is the Hecke eigenvalue. NOTE Cremona's tables won't be good for handling these, because conductors may get very high. His outputs of a_q also only go up to 100, and some of our D's have prime divisors > 100.)

4 Weakening the Hypotheses for Triviality of $Ш(E/K)[p]$

S. Donnelly has explained a way to weaken the hypotheses of Gross's Proposition 2.1, replacing $G(\mathbf{Q}(E[p])/\mathbf{Q}) = GL_2(\mathbf{F}_p)$ with the statement that E admits no p-

isogenies. Gross only uses the hypothesis on $G(\mathbf{Q}(E[p])/\mathbf{Q})$ at two points in the paper: section 4, where he constructs Kolyvagin's cohomology classes and shows that restriction gives an isomorphism $H^1(K, E[p]) \cong H^1(K_n, E[p])^{\mathcal{G}_n}$, where K_n denotes the ring class field of conductor n over K and $\mathcal{G}_n = G(K_n/K)$; and section 9, where he requires $H^n(K(E[p])/K, E[p]) = 0$ for all $n > 0$, for then by the Hochshild-Serre spectral sequence he obtains the isomorphism $H^1(K, E[p]) \cong H^1(K(E[p]), E[p])^{G(K(E[p])/K)}$.

The following lemma (exercise 6 in [**?**]) will be useful in the next two propositions.

Lemma 4.1. *The determinant of the mod ℓ representation attached to E is the cyclotomic character.*

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

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

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

□

Lemma 4.2. *Let p be an odd prime and E an elliptic curve over $\mathbf{Q}$. If E has no $\mathbf{Q}$-rational p-isogeny, then E has no K-rational p-isogeny for any quadratic field K.*

Proof. The existence of a p-isogeny over $\mathbf{Q}$ is equivalent to the reducibility of the representation

$$\rho_p : G(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(E[p]) \cong GL_2(\mathbf{F}_p).$$

[[THIS PROOF IS NOT CORRECT, since complex conjugation doesn't just change the order of the subgroup to $2p$ — could be p^2.]]

Let the image of this representation be G, and consider the corresponding representation

$$\rho_p : G(\bar{\mathbf{Q}}/\mathbf{K}) \twoheadrightarrow H \subset \mathrm{Aut}(E[p]) \cong GL_2(\mathbf{F}_p).$$

Then $[G : H] \leq 2$ (letting $\alpha \in G(\bar{\mathbf{Q}}/\mathbf{Q})$ be a lift of complex conjugation in $G(K/\mathbf{Q})$, $\rho_p(\alpha)$ must generate G/H, but clearly $\rho_p(\alpha)^2 \in H$). In particular, if $E[p]$ has a subgroup P of order p invariant under H, the action of α on P can generate a subgroup of order either p or $2p$. The latter is impossible, since $2p \nmid p^2$, and it follows that the action of all of G leaves P invariant. Thus, if the representation over K is reducible, so is the representation over $\mathbf{Q}$, and we conclude that if E has no p-isogenies over $\mathbf{Q}$, it cannot have any over K. □

The next proposition shows the weakened hypothesis is sufficient in section 9 of Gross's paper.

Proposition 4.3. *Suppose E has no $\mathbf{Q}$-rational p-isogeny, and let $[K : \mathbf{Q}] = 2$. Then $H^i(K(E[p])/K, E[p]) = 0$ for all $i > 0$.*

Proof. First observe that $G(K(E[p])/K) = H$ is precisely the image of the Galois representation $\rho_p : G(\bar{\mathbf{Q}}/K) \to \mathrm{Aut}(E[p]) \cong GL_2(\mathbf{F}_p)$. Let G and H be as in the preceding lemma. By the lemma, H is the image of an irreducible representation. There are two cases to consider: if $p \nmid \#H$, the cohomology clearly vanishes because multiplication by $\#G$ kills the cohomology but is an isomorphism on the p-group $E[p]$. Otherwise, let $p|\#H$. By Proposition 15 of [**?**], H either contains $SL_2(\mathbf{F}_p)$ or is contained in a Borel subgroup of $GL_2(\mathbf{F}_p)$. $E[p]$ is reducible under the action of a Borel subgroup, so by hypothesis $SL_2(\mathbf{F}_p) \subset H$. Thus, H contains a nontrivial scalar (minus the identity); in fact, Lemma 4.1 implies that $\det : G \to \mathbf{F}_p^*$ is surjective, so $G = GL_2(\mathbf{F}_p)$ and contains all of the nontrivial scalars. As H is a subgroup of index at most 2, H must contain at least half of the scalars (in particular, it must contain the squares in $\mathbf{F}_p^*$. Applying the inflation-restriction exact sequence to the subgroup of G generated by the scalars implies that $H^i(G, E[p]) = 0$ for all $i > 0$, because this subgroup has order prime to p ($p - 1$, in fact), and it leaves no subgroup of $E[p]$ invariant. □

For the above result, we assumed that the representation of $G(\bar{\mathbf{Q}}/\mathbf{Q})$ was irreducible, but we in fact improve our hypotheses further with the following proposition:

Proposition 4.4. *In the notation of the above proposition, suppose that the image H of the representation is contained in a Borel subgroup (we used our irreducibility hypothesis to avoid this situation before). Then unless E has a K-rational p-torsion point, $H^i(K(E[p]/K, E[p]) = 0$ for all $i > 0$.*

Proof. Choosing a basis, suppose that the action of H on $E[p] = \mathbf{F}_p^2$ is given by $\begin{pmatrix} \chi & * \\ 0 & \psi \end{pmatrix}$ for characters χ and ψ. If χ is trivial, all matrices of the above form fix $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. In particular, there is a point of $E[p]$ fixed by the action of H, a contradiction since we have assumed that $E(K)[p] = 0$. Now suppose that ψ is trivial. Then by assumption (the reducibility of the representation), there is a 1-dimensional $G(\bar{\mathbf{Q}}/K)$-invariant subspace of $E[p]$, which in our basis is the span of a vector $\begin{pmatrix} a \\ b \end{pmatrix}$. This means that $\begin{pmatrix} a \\ b \end{pmatrix}$ is an eigenvector for all matrices of the form

$\begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$, and since the action of these matrices preserves the second coordinate of a column vector, we see that $\begin{pmatrix} a \\ b \end{pmatrix}$ must in fact be fixed by the action of $G(\bar{\mathbf{Q}}/K)$. We have therefore produced a nontrivial element of $E(K)[p]$, so the assumption $\psi = 1$ contradicts our hypothesis.

Let W be the (unique) p-Sylow subgroup of $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ consisting of matrices of the form $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. We may assume $W \subset H$, for otherwise H has order prime to p, and the cohomology clearly vanishes. Applying the inflation-restriction exact sequence, we find

$$0 \to H^1(H/W, E[p]^W) \to H^1(H, E[p]) \to H^1(W, E[p])^{H/W}$$

H/W has order prime to p, so the first group in the sequence is trivial. We explicitly compute the third cohomology group using the fact that W is cyclic (generated by $w = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, for instance). Recal 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 $\text{Norm} = \sum_{i=0}^{p-1} w^i$ (i.e., the maps are given by multiplication in the group ring $\mathbf{Z}[W]$). Then we immediately see that

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

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

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

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

The next proposition extends the result of section 4 of Gross's paper. Note that if E has no p-isogeny (defined over $\mathbf{Q}$) for $p > 2$, then it has no p-torsion over K.

Proposition 4.5. *Let E be an elliptic curve with $E(K)[p] = 0$, where $p > 3$ or, if $p = 3$, $K \neq \mathbf{Q}(\mu_3)$. Then $H^i(K_n/K, E(K_n)[p]) = 0$ for all $i \geq 1$.*

Proof. We may write the abelian group $G(K_n/K)$ as a direct sum $P \oplus P'$, where P is its Sylow p-subgroup and $(p, \#P') = 1$. We claim that the subgroup of $E(K_n)[p]$ invariant under P' is trivial. Let $G = G(K_n/K)/H$, where H is the subgroup of $G(K_n/K)$ that acts trivially on $E(K_n)[p]$. If $(\#G, p) = 1$, $P \subseteq H$, so P' surjects onto G. As there is no nontrivial element of $E(K_n)[p]$ invariant under all of $G(K_n/K)$ (by the assumption on $E(K)[p]$, the same then holds for P'.

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

We can choose a basis of $(\mathbf{Z}/p\mathbf{Z})^2$ so that G contains the subgroup $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, where $x \in \mathbf{Z}/p\mathbf{Z}$. Being abelian, G must be contained in the normalizer of this subgroup, so $G \subseteq \{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} | a, b \in \mathbf{Z}/p\mathbf{Z}\}$, and we claim that G contains an element with $a \neq 1$. Since $E[p] \subset E(K_n)[p]$, the representation $G(\bar{\mathbf{Q}}/K) \to \mathrm{Aut}(E[p])$ factors through $G(K_n/K)$ (recall that the image of the representation is $G(K(E[p]/K))$. We argued before that this image contained the scalars corresponding to squares in $\mathbf{F}_p^*$, so P' contains at least $\frac{p-1}{2}$ (which is > 1 for $p > 3$) elements that leave no subgroup of $E(K_n)[p]$ invariant. Now, the result will follow from an application of the inflation-restriction exact sequence:

$$0 \to H^1(P, E(K_n)[p]^{P'}) \to H^1(K_n/K, E(K_n)[p]) \to H^1(P', E(K_n)[p])$$

The first group vanishes since $E(K_n)[p]^{P'} = 0$, and the third group vanishes since the order of P' is prime to p, and thus to the order of $E(K_n)[p]$. We conclude that the middle group is trivial, as desired. We can therefore extend the sequence to the second cohomology groups, deduce the same triviality result, and by induction conclude that $H^m(K_n/K, E(K_n)[p]) = 0$ for all $m \geq 1$.

If $p = 3$, $E(K_n)[3] = E[3] \Rightarrow \mu_3 \subset K_n \Rightarrow K = \mathbf{Q}(\mu_3)$. The last implication holds because $G(K_n/\mathbf{Q})$ 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, so we must have $E(K_n)[3] = 0$, in which case the cohomology is clearly trivial. □

To summarize, we can now apply Kolyvagin's arguments (as given in [**?**]) to find $Ш(E/\mathbf{Q})[p] = 0$ for all odd primes p such that E has no K-rational p-torsion and $p \nmid I_K$. If $E(K)[p] \neq 0$ the subsequent situation is particularly easy to deal with because p-descent is much more easily implemented with a known rational p-torsion point.

5 The Decomposition of $E(K)$ under Complex Conjugation

To compute the index $I_K = \#E(K)/\mathbf{Z}y_K$ needed to verify the full Birch and Swinnerton-Dyer conjecture, we compare the canonical height of the Heegner point y_K with the height of a generator of $E(K)$, which we know to have algebraic rank 1 by Kolyvagin's theorem. To assist in finding the (infinite order) generator of $E(K)$, we use the

Proposition 5.1. *For a quadratic imaginary field $K = \mathbf{Q}(\sqrt{D})$, $E(K)$ decomposes, up to 2-torsion, as a direct sum $E(\mathbf{Q}) \oplus E_D(\mathbf{Q})$, where E_D is the quadratic twist of E. (Recall that from a Weierstrass equation of $E/\mathbf{Q}$, we obtain a Weierstrass equation of $E_D/\mathbf{Q}$ as follows:*

$$\begin{array}{c} E : y^2 = x^3 + ax + b \\ E_D : y^2 = x^3 + D^2ax + D^3b \end{array})$$

Proof. Denote complex conjugation by τ. We will decompose $E(K)$ into its eigenspaces under the action of τ. First, we kill $E(K)[2]$ (by tensoring with $\mathbf{Z}[\frac{1}{2}]$, for instance), so that, using the fact that $\tau^2 = 1$, we can define the projections from $E(K)$ to its $+1$ and -1 eigenspaces under τ: for $P \in E(K)$,

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

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 $E_D(\mathbf{Q})$. Thus, having eliminated the 2-torsion, the decomposition of $E(K)$ into its τ-eigenspaces just reads

$$E(K) = E(\mathbf{Q}) \oplus E_D(\mathbf{Q}).$$

□

6 Application of Gross-Zagier to our calculations

In light of Donnelly's observation, we can apply Kolyvagin's result that $Ш(E/K)[p] = 0$ for all odd primes p not dividing the Heegner point y_K (i.e., p does not divide C_D) and such that E/K has no p-isogenies. By the inflation-restriction sequence, $Ш(E/\mathbf{Q})[p] =$ for all of these primes as well, since $Ш(E/\mathbf{Q})[p] =$ maps to $Ш(E/K)[p]$ with kernel contained in $H^1(K/\mathbf{Q}, E(K)$, a finite 2-group. Thus, it will be essential to compute the constant $I_K = [E(K) : \mathbf{Z}y_K]$. Actually, we only want this index for $E(K)/E(K)_{tors}$, but if $E(K)$ contains nontrivial p-torsion, we must include p in our list of "bad primes" anyway, so it doesn't matter if p is counted again as a prime factor of I_K. First we will have to find a generator P of the free part of $E(K)$ and compute its canonical height $\hat{h}(P)$. We use the root number to determine whether the free generator of $E(K)$ comes from $E(\mathbf{Q})$ or $E^D(\mathbf{Q})$. We can use another form of the Gross-Zagier formula to compute $\hat{h}(y_K)$:

$$\hat{h}(y_K) = \frac{u^2\sqrt{D}}{\|\omega_E\|} L'(E_D/\mathbf{Q}, 1) L(E/\mathbf{Q}, 1),$$

where u is half the number of units in $K = \mathbf{Q}(\sqrt{-D})$, and $\|\omega_E\|$ is the determinant of the period lattice associated to a Nèron differential of $E/\mathbf{Q}$ (note that for $D \neq 3, 4$, $u = 1$).

With these preliminaries, we can compute the index $I_K = \sqrt{\hat{h}(y_K)/\hat{h}(P)}$. Note that we are free to choose $K = \mathbf{Q}(\sqrt{-D})$ as long as $D \neq 3, 4$ and all the prime factors of N (the conductor of E) split in K. To find D given N amounts to solving a finite number of congruences, so we should be able to implement this.