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

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

GRIGOR GRIGOROV, ANDREI JORZA, STEFAN PATRIKIS, WILLIAM A. STEIN, AND CORINA TARNIŢĂ-PĂTRAŞCU

Abstract. We describe theorems and computational methods for verifying the Birch and Swinnerton-Dyer conjecture for specific elliptic curves over $\mathbb{Q}$. We apply our techniques to show that if E is a non-CM elliptic curve over $\mathbb{Q}$ of conductor ≤ 1000 and rank ≤ 1, then the full Birch and Swinnerton-Dyer conjecture is true for E up to odd primes that divide either a Tamagawa number of E or the degree of some rational cyclic isogeny with domain E.

Contents

THIS MATERIAL IS BASED UPON WORK SUPPORTED BY THE NATIONAL SCIENCE FOUNDATION UNDER GRANT NO. 0555776.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$. The L-function $L(E,s)$ of E is a holomorphic function on $\mathbb{C}$ that encodes deep arithmetic information about E. This paper is about a connection between the behavior of $L(E,s)$ at $s=1$ and the arithmetic of E.

We use theorems and computation to attack the following conjecture for many specific elliptic curves of conductor ≤ 1000:

Conjecture 1.1 (Birch and Swinnerton-Dyer)**.** *The order of vanishing* $\mathrm{ord}_{s=1} L(E,s)$ *equals the rank r of E, the group $\text{Ш}(E)$ is finite, and*

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

For more about Conjecture 1.1, see [Lan91, Wil00] and the papers they reference. See also Section 1.2 below for the notation used in the conjecture. Henceforth we call it the BSD conjecture.

Definition 1.2 (Analytic Ш)**.** If E has rank r, let

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

denote the order of $\text{Ш}(E)$ predicted by Conjecture 1.1. We call this the *analytic order* of $\text{Ш}(E)$.

Conjecture 1.3 ($\mathrm{BSD}(E,p)$)**.** *Let (E,p) denote a pair consisting of an elliptic curve E over $\mathbb{Q}$ and a prime p. We also call the assertion that* $\mathrm{ord}_{s=1} L(E,s)$ *equals the rank r, that $\text{Ш}(E)[p^\infty]$ is finite, and*

$$\mathrm{ord}_p(\#\text{Ш}(E)[p^\infty]) = \mathrm{ord}_p(\#\text{Ш}(E)_{\mathrm{an}})$$

the BSD conjecture at p, *and denote it* $\mathrm{BSD}(E,p)$.

The BSD conjecture is invariant under isogeny.

Theorem 1.4 (Cassels)**.** *If E and F are $\mathbb{Q}$-isogeneous and p is a prime, then* $\mathrm{BSD}(E,p)$ *is true if and only if* $\mathrm{BSD}(F,p)$ *is true.*

Proof. See [Cas65, Mil86, Jor05]. □

One way to give evidence for the conjecture is to compute $\#\text{Ш}(E)_{\mathrm{an}}$ and note that it is a perfect square, in accord with the following theorem:

Theorem 1.5 (Cassels)**.** *If E is an elliptic curve over $\mathbb{Q}$ and p is a prime such that $\text{Ш}(E)[p^\infty]$ is finite, then $\#\text{Ш}(E)[p^\infty]$ is a perfect square.*

Proof. See [Cas62, PS99]. □

We use the notation of [Crea] to refer to specific elliptic curves over $\mathbb{Q}$.

Conjecture 1.6 (Birch and Swinnerton-Dyer ≤ 1000)**.** *For* all *optimal curves of conductor ≤ 1000 we have $\text{Ш}(E) = 0$, except for the following four rank 0 elliptic curves, where $\text{Ш}(E)$ has the indicated order:*

Curve	571A	681B	960D	960N
$\#\text{Ш}(E)_{\mathrm{an}}$	4	9	4	4

Theorem 1.7 (Cremona)**.** *Conjecture 1.1 is true for all elliptic curves of conductor* ≤ 1000 *if and only if Conjecture 1.6 is true.*

Proof. In the book [Cre97], Cremona computed $\#Ш(E)_{\mathrm{an}}$ for every curve of conductor ≤ 1000. By Theorem 1.4 it suffices to consider only the optimal ones, and the four listed are the only ones with nontrivial $\#Ш(E)_{\mathrm{an}}$. □

In view of Theorem 1.7, the main goal of this paper is to obtain results in support of Conjecture 1.6. The results of Section 4.2 below together imply the theorem we claimed in the abstract:

Theorem 1.8. *Suppose that E is a non-CM elliptic curve of rank ≤ 1, conductor ≤ 1000 and that p is a prime. If p is odd, assume further that the mod p representation $\overline{\rho}_{E,p}$ is irreducible and p does not divide any Tamagawa number of E. Then* $\mathrm{BSD}(E, p)$ *is true.*

Proof. Combine Theorem 3.27, Theorem 3.31, and Theorem 4.4. □

For example, if E is the elliptic curve 37A, then according to [Cre97], all $\overline{\rho}_{E,p}$ are irreducible and the Tamagawa numbers of E are 1. Thus Theorem 1.8 asserts that the full BSD conjecture for E is true.

There are 18 optimal curves of conductor ≤ 1000 of rank 2 (and none of rank > 2). For these E of rank 2, nobody has proved that $Ш(E)$ is finite in even a single case. We exclude CM elliptic curves from most of our computations. The methods for dealing with the BSD conjecture for CM elliptic curves are different than for general curves, and will be the subject of another paper. The same is true for $\mathrm{BSD}(E, p)$ when $\overline{\rho}_{E,p}$ is reducible.

1.1. **Acknowledgement.** We thank Michael Stoll for suggesting this project at an American Institute of Mathematics meeting and for initial feedback and ideas, and Stephen Donnelly and Michael Stoll for key ideas about Section 5. We thank John Cremona for many discussions and his immensely useful computer software. Finally we thank Benedict Gross and Noam Elkies for helpful feedback and encouragement throughout the project.

We thank the Harvard College Research Program for funding Pătraşcu's work on this paper, and the Herchel Smith Harvard Undergraduate Research Fellowship for supporting Patrikis. Jorza and Stein were supported by the National Science Foundation under Grant No. 0400386.

1.2. **Notation and Background.** If G is an abelian group, let G_{tor} denote the torsion subgroup and $G_{/\,\mathrm{tor}}$ denote the quotient G/G_{tor}. For an integer m, let $G[m]$ be the kernel of multiplication by m on G. For a commutative ring R, we let R^* denote the group of units in R.

1.2.1. *Galois Cohomology of Elliptic Curves.* For a number field K, let $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Let E be an elliptic curve defined over a number field K, and consider the first Galois cohomology group $\mathrm{H}^1(K, E) = \mathrm{H}^1(G_K, E(\overline{K}))$, and the local Galois cohomology groups $\mathrm{H}^1(K_v, E) = \mathrm{H}^1(\mathrm{Gal}(\overline{K}_v/K_v), E(\overline{K}_v))$, for each place v of K.

Definition 1.9 (Shafarevich-Tate group)**.** The *Shafarevich-Tate group*

$$Ш(E/K) = \mathrm{Ker}\Big(\mathrm{H}^1(K, E) \to \bigoplus_v \mathrm{H}^1(K_v, E)\Big),$$

of E measures the failure of global cohomology classes to be determined by their localizations at all places.

If E is an elliptic curve over a field F and the field F is clear from context, we write $\text{Ш}(E) = \text{Ш}(E/F)$. For example, if E is an elliptic curve over $\mathbb{Q}$, then $\text{Ш}(E)$ means $\text{Ш}(E/\mathbb{Q})$.

Definition 1.10 (Selmer group)**.** For each positive integer m, the *m-Selmer group* is

$$\mathrm{Sel}^{(m)}(E/K) = \mathrm{Ker}\Big(\mathrm{H}^1(K, E[m]) \to \bigoplus_v \mathrm{H}^1(K_v, E)\Big).$$

The Selmer group relates the Mordell-Weil and Shafarevich-Tate groups of E via the exact sequence

$$0 \to E(K)/mE(K) \to \mathrm{Sel}^{(m)}(E/K) \to \text{Ш}(E/K)[m] \to 0,$$

where $\text{Ш}(E/K)[m]$ denotes the m-torsion subgroup of $\text{Ш}(E/K)$. Note that $\text{Ш}(E/K)$ is a torsion group since $\mathrm{H}^1(K, E)$ is torsion.

1.2.2. *Elliptic Curves over* $\mathbb{Q}$. See [Sil92, pp. 360–361] for the definition of $L(E, s)$ and [Wil95, BCDT01] for why $L(E, s)$ is entire.

Let E be an elliptic curve over $\mathbb{Q}$. We use the notation of [Crea] to refer to certain elliptic curves. Thus, e.g., 37B3 refers to the third elliptic curve in the second isogeny class of elliptic curves of conductor 37, i.e., the curve $y^2+y = x^3+x^2-3x+1$. The ordering of isogeny classes and curves in isogeny classes is as specified in [Cre97]. If the last number is omitted, it is assumed to be 1, so 37B refers to the first curve in the second isogeny class of curves of conductor 37.

Let Reg_E be the absolute value of the discriminant of the canonical height pairing on $E(\mathbb{Q})_{/\,\mathrm{tor}}$. Let $c_p = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$ be the Tamagawa number of E at p, where $E_0(\mathbb{Q}_p)$ is the subgroup of points that reduce to a nonsingular point modulo p. Let $\Omega_E = \int_{E(\mathbb{R})} |\omega|$, where

$$\omega = \frac{dx}{2y + a_1x + a_3}$$

is the invariant differential attached to a minimal Weierstrass model for E.

For any prime p, let $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$ denote the mod p representation and $\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(T_pE)$ the representation on the p-adic Tate module T_pE of E.

It follows from [BCDT01] that every elliptic curve E over $\mathbb{Q}$ is a factor of the modular curve $X_0(N)$, where N is the conductor of E.

Definition 1.11 (Optimal)**.** An elliptic curve E over $\mathbb{Q}$ is *optimal* if for every elliptic curve F and surjective morphisms $X_0(N) \to F \to E$, we have $E \cong F$. (Optimal curves are also called "strong Weil curves" in the literature.)

We say E is a *complex multiplication* (CM) curve, if $\mathrm{End}(E/\overline{\mathbb{Q}}) \neq \mathbb{Z}$.

2. Elliptic Curve Algorithms

2.1. **Images of Galois Representations.** Let E be an elliptic curve over $\mathbb{Q}$. Many theorems that provide explicit bounds on $\#\text{Ш}(E)[p^\infty]$ have as a hypothesis that $\overline{\rho}_{E,p}$ or $\rho_{E,p}$ be either surjective or irreducible. In this section we explain how to prove that $\overline{\rho}_{E,p}$ or $\rho_{E,p}$ is surjective or irreducible, in particular cases.

2.1.1. *Irreducibility.* Regarding irreducibility, note that $\overline{\rho}_{E,p}$ is irreducible if and only if there is no isogeny $E \to F$ over $\mathbb{Q}$ of degree p. The degrees of all such isogenies for curves of conductor ≤ 1000 are recorded in [Cre97], which were computed using Cremona's program `allisog`. This program uses results of Mazur [Maz78] along with computations involving modular curves of genus 0.

2.1.2. *Surjectivity.* We discuss surjectivity of $\rho_{E,p}$ in the rest of this section.

Theorem 2.1 (Mazur)**.** *If E is semistable and $p \geq 11$, then $\overline{\rho}_{E,p}$ is surjective.*

Proof. See [Maz78, Thm. 4]. □

Example 2.2. Mazur's theorem implies that the representations $\overline{\rho}_{E,p}$ attached to the semistable elliptic curve $E = X_0(11)$ are surjective for $p \geq 11$. Note that $\overline{\rho}_{E,5}$ is reducible.

Theorem 2.3 (Cojocaru, Kani, and Serre)**.** *If E is a non-CM elliptic curve of conductor N, and*

$$p \geq 1 + \frac{4\sqrt{6}}{3} \cdot N \cdot \prod_{\textit{prime } \ell \mid N} \left(1 + \frac{1}{\ell}\right)^{1/2},$$

then $\overline{\rho}_{E,p}$ is surjective.

Proof. See Theorem 2 of [CK], whose proof relies on the results of [Ser72]. □

Example 2.4. When $N = 11$, the bound of Theorem 2.3 is ~ 38.52. When $N = 997$, the bound is ~ 3258.8. For $N = 40000$, the bound is ~ 143109.35.

Proposition 2.5. *Let E be a non-CM elliptic curve over $\mathbb{Q}$ of conductor N and let $p \geq 5$ be a prime. For each prime $\ell \nmid p \cdot N$ with $a_\ell \not\equiv 0 \pmod{p}$, let*

$$s(\ell) = \left(\frac{a_\ell^2 - 4\ell}{p}\right) \in \{0, -1, +1\},$$

where the symbol $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol. If -1 and $+1$ both occur as values of $s(\ell)$, then $\overline{\rho}_{E,p}$ is surjective. If $s(\ell) \in \{0, 1\}$ for all ℓ, then $\mathrm{Im}(\overline{\rho}_{E,p})$ is contained in a Borel subgroup (i.e., reducible), and if $s(\ell) \in \{0, -1\}$ for all ℓ, then $\mathrm{Im}(\overline{\rho}_{E,p})$ is a nonsplit torus.

Proof. This is an application of [Ser72, §4], where we use the quadratic formula to convert the condition that certain polynomials modulo p be reducible or irreducible into a quadratic residue symbol. □

For computational applications we apply Proposition 2.5 as follows. We choose a bound B and compute values $s(\ell)$; if both -1 and $+1$ occur as values of $s(\ell)$, we stop computing $s(\ell)$ and conclude that $\overline{\rho}_{E,p}$ is surjective. If for $\ell \leq B$ we find that $s(\ell) \in \{0, 1\}$, we suspect that $\mathrm{Im}(\overline{\rho}_{E,p})$ is Borel, and attempt to show this (see Section 2.1.1). If for $\ell \leq B$, we have $s(\ell) \in \{0, -1\}$, we suspect that $\mathrm{Im}(\overline{\rho}_{E,p})$ is contained in a nonsplit torus, and try to show this by computing and analyzing the p-division polynomial of E. If this approach is inconclusive, we can alway increase B and eventually the process terminates. In practice we often apply some theorem under the hypothesis that $\overline{\rho}_{E,p}$ is surjective, which is something that in practice we verify for a particular p using Proposition 2.5.

Example 2.4 suggests that the bound of Theorem 2.3 is probably far larger than necessary. Nonetheless, it is small enough that in a reasonable amount of time we can determine whether $\overline{\rho}_{E,p}$ is surjective, using the above process, for all p up to the bound. In this way we determine the exact image of Galois.

Remark 2.6. We can also determine surjectivity of the mod 2 and mod 3 representations directly using the 3-division polynomial of E. For $p \leq 3$ one can show that $\overline{\rho}_{E,p}$ is surjective if and only if the p-division polynomial (of degree n) has Galois group S_n.

Theorem 2.7 (Serre)**.** *If $p \geq 5$ is a prime of good reduction, then $\rho_{E,p}$ is surjective if and only if $\overline{\rho}_{E,p}$ is surjective.*

Proof. This is proved in greater generality as [Ser72, Thm. 4′, pg. 300]. □

Remark 2.8. This result does not extend to $p = 3$ (see [Ser98, Ex. 3, pg IV-28]). In fact, there are infinitely many elliptic curves with $\overline{\rho}_{E,p}$ surjective, but $\rho_{E,p}$ not surjective (see forthcoming work of Noam Elkies).

2.2. **Special Values of L-Functions.** Let E be an elliptic curve over $\mathbb{Q}$ of conductor N, and let $f = \sum a_n q^n$ be the corresponding cusp form.

The following lemma will be useful in determining how many terms of the L-series of E are needed to compute the L-series to a given precision. (We could give a strong bound, but for our application this will be enough, and is simplest to apply in practice.)

Lemma 2.9. *For any positive integer n, we have $|a_n| \leq n$.*

Proof. For p prime we know that $a_p = \alpha + \beta$, where α and β are the roots of $x^2 - a_p x + p = 0$. Note that $|\alpha| = |\beta| = \sqrt{p}$.

Since a_n is multiplicative, it is enough to show $|a_n| \leq n$ for prime powers p^r. Let $r > 1$. Then $a_{p^r} = a_p a_{p^{r-1}} - p a_{p^{r-2}}$, and by induction,

$$a_{p^r} = \frac{\alpha^{r+1} - \beta^{r+1}}{\alpha - \beta}.$$

Then

$$|a_{p^r}| \leq \frac{2p^{(r+1)/2}}{|\alpha - \beta|} = \frac{2p^{(r+1)/2}}{\left|\sqrt{4p - a_p^2}\right|}.$$

Note that the sign is changed since we only deal with absolute values. We need to show that this is $\leq p^r$. This happens if

$$\frac{2}{\sqrt{4p - a_p^2}} \leq p^{(r-1)/2}.$$

Since $a_p^2 < 4p$ the difference is at least 1 so it is enough to show that $2 \leq p^{(r-1)/2}$. This is true as long as $p > 3$. For $p = 2$ and $p = 3$ note that a_p is an integer with $|a_p| < 2\sqrt{p}$. For $p = 2$ this integer is at most 2 and so $4p - a_p^2 \geq 4$. Similarly for $p = 3$ this is at most 3 and so $4p - a_p^2 \geq 4$. Therefore it is enough to show that $1 \leq p^{(r-1)/2}$, which is true for all $r > 1$. □

Suppose E has even analytic rank. By [Cre97, §2.13] or [Coh93, Prop. 7.5.8], we have

$$L(E,1) = 2\sum_{n=1}^{\infty} \frac{a_n}{n} e^{-2\pi n/\sqrt{N}}, \tag{2.1}$$

where a_n are the Fourier coefficients of the normalized eigenform associated with E. Using the bound $|a_n| \leq n$ of Lemma 2.9, we see that if we truncate the series (2.1) at the kth term, the error is at most

$$\varepsilon = 2\sum_{n=k}^{\infty} e^{-2\pi n/\sqrt{N}} = \frac{2e^{-2\pi k/\sqrt{N}}}{1 - e^{-2\pi/\sqrt{N}}},$$

and the quantity on the right can easily be evaluated.

Next suppose E has odd analytic rank. In [Cre97, §2.13] or [Coh93, Prop. 7.5.9] we find that

$$L'(E,1) = 2\sum_{n=1}^{\infty} \frac{a_n}{n} G_1(2\pi n/\sqrt{N}).$$

We have

$$G_1(x) = \int_1^{\infty} e^{-xy}\frac{dy}{y} = \int_x^{\infty} e^{-y}\frac{dy}{y} \leq e^{-x},$$

and we obtain the same error bound as for $L(E,1)$. (In fact, $G_1(x) \leq e^{-x}/x$ but we will not need this stronger bound.)

2.3. **Mordell-Weil Groups.** If E is an elliptic curve over $\mathbb{Q}$ of analytic rank ≤ 1, there are algorithms to compute $E(\mathbb{Q})$ that are guaranteed to succeed. This is because $\#Ш(E)$ is finite, by [Kol91]. Independent implementations of these algorithms are available as part of `mwrank` [Creb] and MAGMA [BCP97]. We did most of our computations of $E(\mathbb{Q})$ using `mwrank`, but use MAGMA in a few cases, since it implements 3-descents, 4-descents and Heegner points methods (thanks to work of Tom Womack, Mark Watkins, and others).

2.4. **Other Algorithms.** We use many other elliptic curves algorithms, for example, for computing root numbers and the coefficients a_n of the modular form associated to E. For the most part, we used the PARI (see [ABC$^+$]) C-library via SAGE (see [Ste]). For descriptions of these general elliptic curves algorithms, see [Coh93, Cre97].

3. The Kolyvagin Bound

In this section we describe a bound due to Kolyvagin on $\#Ш(E)$, and compute it for many specific elliptic curves over $\mathbb{Q}$. In fact, the bound is on $\#Ш(E/K)$, where K is a quadratic imaginary field; this is not a problem, because the natural map $Ш(E/\mathbb{Q}) \to Ш(E/K)$ has kernel of order a power of 2, so the bound is also a bound on the odd part of $\#Ш(E)$.

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. For any quadratic imaginary field $K = \mathbb{Q}(\sqrt{-D})$, let E^D denote the twist of E by D. If E is defined by $y^2 = x^3 + ax + b$, then E^D is defined by $y^2 = x^3 + D^2ax + D^3b$, and

$$L(E/K,s) = L(E,s)\cdot L(E^D,s).$$

Definition 3.1 (Heegner Hypothesis)**.** We say that K satisfies the *Heegner hypothesis* for E if $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, and every prime factor of N splits as a product of two distinct primes in the ring of integers of K. (The condition $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$ is not necessary for some of the results below, but we include it for simplicity.)

If K satisfies the Heegner hypothesis for E, then there is a Heegner point $y_K \in E(K)$, which is the sum of images of certain complex multiplication (CM) points on $X_0(N)$ (see [GZ86, §I.3]). Properties of this point impact the arithmetic of E over K.

3.1. **Bounds on $\#\text{Ш}(E/K)$.** Suppose that K is an imaginary quadratic extension of $\mathbb{Q}$ that satisfies the Heegner hypothesis for E. Kolyvagin proved the following theorem in [Kol90]:

Theorem 3.2 (Kolyvagin)**.** *Let $R = \text{End}(E/\mathbb{C})$ and let $F = \text{Frac}(R)$, so if E is non-CM then $F = \mathbb{Q}$. If p is an odd prime unramified in F such that $\text{Gal}(F(E[p])/F) = \text{Aut}_R(E[p])$, i.e., $\text{Im}(\overline{\rho}_{E,p})$ is as large as possible, then*

$$\text{ord}_p(\#\text{Ш}(E/K)) \leq 2 \cdot \text{ord}_p([E(K) : \mathbb{Z}y_K]).$$

Note that if E does not have complex multiplication, the hypotheses of both these theorems imply that $p \nmid \#E(K)_{\text{tor}}$ (see Lemma 5.7).

Cha [Cha03, Cha05] extended Kolyvagin's method to provide better bounds on $\text{Ш}(E/K)$ in some cases. Let K be a number field, let D_K be the discriminant of K, and let N be the conductor of E.

Theorem 3.3 (Cha)**.** *If $p \nmid D_K$, $p^2 \nmid N$, and $\overline{\rho}_{E,p}$ is irreducible, then*

$$\text{ord}_p(\#\text{Ш}(E/K)) \leq 2 \cdot \text{ord}_p([E(K) : \mathbb{Z}y_K]).$$

As we will see in the proof of Theorem 4.3 below, there is one curve that satisfies the hypotheses of that theorem, but for which we cannot use Theorem 3.2 to prove $\text{BSD}(E, 5)$. The problem is that $\overline{\rho}_{E,5}$ is not surjective. We can use Cha's theorem though:

Lemma 3.4. *Let E be the elliptic curve* 608B*, which has rank* 0*. Then* $\text{BSD}(E, 5)$ *is true for E.*

Proof. Since E admits no 5-isogeny (see [Cre97]), $\overline{\rho}_{E,5}$ is irreducible. Also, $5^2 \nmid 608$, so for any Heegner K of discriminant coprime to 5 we can apply Theorem 3.3. Taking $K = \mathbb{Q}(\sqrt{-79})$, we find that the odd part of $[E(K) : \mathbb{Z}y_K]$ is 1, so $5 \nmid \#\text{Ш}(E/K)$. It follows that $5 \nmid \#\text{Ш}(E)$, so $\text{BSD}(E, 5)$ is true, according to Theorem 1.7. □

Cha's assumption on the reduction of E at p and that $p \nmid D_K$ is problematic when there is a prime $p \geq 5$ of additive reduction or one uses only one K. This situation does occur in several cases, which motivated us to prove the following theorem:

Theorem 3.5. *Suppose E is a non-CM elliptic curve over $\mathbb{Q}$. Suppose K is a quadratic imaginary field that satisfies the Heegner hypothesis and p is an odd prime such that $p \nmid \#E'(K)_{\text{tor}}$ for any curve E' that is $\mathbb{Q}$-isogenous to E. Then*

$$\text{ord}_p(\#\text{Ш}(E)) \leq 2\,\text{ord}_p([E(K) : \mathbb{Z}y_K]),$$

unless $\mathrm{disc}(K)$ *is divisible by exactly one prime* ℓ*, in which case the conclusion is only valid if* $p \neq \ell$*.*

Since the proof of Theorem 3.5 is somewhat long and technical, we defer the proof until Section 5.

Remark 3.6. If in Theorem 3.5, $\overline{\rho}_{E,p}$ is irreducible, then $p \nmid \#E'(K)_{\mathrm{tor}}$ for all E' isogenous to E. This is because the isogeny $E \to E'$ has degree coprime to p, so $E[p] \cong E'[p]$. Also, since $E[p]$ is irreducible, if $E'(K)$ were to contain a p-torsion point, it would have to contain all of them, a contradiction since $\boldsymbol{\mu}_p \not\subset K$ (recall that we exclude $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-4})$).

Theorem 3.7 (Bump-Friedberg-Hoffstein, Murty-Murty, Waldspurger)**.** *There are infinitely many quadratic imaginary extensions* $K/\mathbb{Q}$ *such that* K *satisfies the Heegner hypothesis and* $\mathrm{ord}_{s=1} L(E/K) = 1$*.*

Proof. If $\mathrm{ord}_{s=1}L(E,s) = 0$, then the papers [MM91] and [BFH90] both imply the existence of infinitely many K such that y_K has infinite order. If $\mathrm{ord}_{s=1}L(E,s) = 1$, then a result of Waldspurger ([Wal85]) applies, as does [BFH90]. □

Theorem 3.7 is not used in our computations, but ensures that our procedure for bounding $\#Ш(E)$, when E has analytic rank ≤ 1, is an algorithm, i.e., it always terminates with a nontrivial upper bound.

3.2. **The Gross-Zagier Formula.** We use the Gross-Zagier formula to compute the index $[E(K) : \mathbb{Z}y_K]$ without explicitly computing y_K.

The modularity theorem of [BCDT01] asserts that there exists a surjective morphism $\pi : X_0(N) \to E$. Choose π to have minimal degree among all such morphisms. Let $\pi^*(\omega)$ be the pullback of a minimal invariant differential ω on E. Then $\pi^*(\omega) = \alpha \cdot f$, for some constant α and some normalized cusp form f. By [Edi91, Prop. 2], we know that $\alpha \in \mathbb{Z}$.

Definition 3.8 (Manin Constant)**.** The *Manin constant* of E is $c = |\alpha|$.

Manin conjectured in [Man72, §5] that $c = 1$ for the optimal curve in the $\mathbb{Q}$-isogeny class of E.

Theorem 3.9 (Gross-Zagier)**.** *If* K *satisfies the Heegner hypothesis for* E*, then the Néron-Tate canonical height of* y_K *is*

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

Proof. Gross and Zagier proved the following formula in [GZ86] under the hypothesis that D is odd. For the general assertion see [Zha04, Thm. 6.1]. □

3.3. **Remarks on the Index.** Suppose that E is an elliptic curve over $\mathbb{Q}$ of conductor N and that E has analytic rank 1 over a quadratic imaginary field K that satisfies the Heegner hypothesis. In [McC91], McCallum rephrases the analogue of Conjecture 1.1 for E over K using the Gross-Zagier formula as follows:

Conjecture 3.10 (Birch and Swinnerton-Dyer)**.** *Suppose* K *is a quadratic imaginary field that satisfies the Heegner hypothesis, and that* E *has analytic rank* 1 *over* K*. Then*

$$\#Ш(E/K) = \left(\frac{[E(K) : \mathbb{Z}y_K]}{c^2 \cdot \prod_{p \mid N} c_p}\right)^2.$$

Here the c_p are the Tamagawa numbers of E over $\mathbb{Q}$, c is the Manin constant of E, and $\mathbb{Z}y_K$ is the cyclic group generated by y_K.

Remark 3.11. A serious issue is that Conjecture 3.10 implies that the index $I_K = [E(K) : \mathbb{Z}y_K]$ will be divisible by the Tamagawa numbers c_p. One sees using Tate curves that these Tamagawa numbers can be arbitrarily large. In many cases when E has analytic rank 0, we could instead apply Theorem 4.1 below, but when E has analytic rank 1 a new approach is required, e.g., computation of p-adic regulators and use of results of P. Schneider and others toward p-adic analogues of the BSD conjecture. This will be the subject of a future paper.

Remark 3.12. Conjecture 3.10 has interesting implications in certain special cases. For example, if E is the curve 91B, then $c_7 = c_{13} = 1$. Also $c = 1$, as Cremona has verified, and $\#E(\mathbb{Q})_{\mathrm{tor}} = 3$. Thus for any K, we have $3 \mid [E(K) : \mathbb{Z}y_K]$. If y_K has infinite order, then Conjecture 3.10 implies that $3^2 \mid \#\text{Ш}(E/K)$. For $K = \mathbb{Q}(\sqrt{-103})$, the point y_K is torsion, and in this case $E(K)$ has rank 3 and (conjecturally) $\text{Ш}(E/K)[3] = 0$. See Remark 3.23 for another example along these lines.

3.4. **Mordell-Weil Groups and Quadratic Imaginary Fields.**

Let E be an elliptic curve over $\mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{D})$ a quadratic imaginary field such that $E(K)$ has rank 1. In this section we explain how to understand $E(K)$ in terms of $E(\mathbb{Q})$ and $E^D(\mathbb{Q})$.

Proposition 3.13. *Let $R = \mathbb{Z}[1/2]$ and $K = \mathbb{Q}(\sqrt{D})$. For any squarefree integer $D \neq 1$, we have*

$$E(K) \otimes R = (E(\mathbb{Q}) \otimes R) \oplus (E^D(\mathbb{Q}) \otimes R).$$

Proof. Let τ be the complex conjugation automorphism on $E(K) \otimes R$. The characteristic polynomial of τ is $x^2 - 1$, which is squarefree, so $E(K) \otimes R$ is a direct sum of its $+1$ and -1 eigenspaces for τ. The natural map $E(\mathbb{Q}) \hookrightarrow E(K)$ identifies $E(\mathbb{Q}) \otimes R$ with the $+1$ eigenspace for τ since $E(K)^{G_\mathbb{Q}} = E(\mathbb{Q})$; likewise, $E^D(\mathbb{Q}) \hookrightarrow E(K)$ identifies $E^D(\mathbb{Q}) \otimes R$ with the -1 eigenspace for τ. □

The following slightly more refined proposition will be important for certain explicit Heegner point computations (directly after Equation 3.1).

Proposition 3.14. *Suppose $E(K)$ has rank 1. Then the image of either $E(\mathbb{Q})_{/\,\mathrm{tor}}$ or $E^D(\mathbb{Q})_{/\,\mathrm{tor}}$ has index at most 2 in $E(K)_{/\,\mathrm{tor}}$.*

Proof. Since $E(K)$ has rank 1, Proposition 3.13 implies that exactly one of $E(\mathbb{Q})$ and $E^D(\mathbb{Q})$ has rank 1 and the other has rank 0. We may assume that $E(\mathbb{Q})$ has rank 1 (otherwise, swap E and E^D). Let i be the natural inclusion $E(\mathbb{Q}) \hookrightarrow E(K)$, and let τ denote the automorphism of $E(K)$ induced by complex conjugation. Then $P \mapsto (1+\tau)P$ induces a map $E(K) \to E(K)^+ = E(\mathbb{Q})$ that, upon taking quotients by torsion, induces a map $\psi : E(K)_{/\,\mathrm{tor}} \to E(\mathbb{Q})_{/\,\mathrm{tor}}$. Let P_1 be a generator for $E(\mathbb{Q})_{/\,\mathrm{tor}}$ and P_2 a generator for $E(K)_{/\,\mathrm{tor}}$, and write $i(P_1) = nP_2$, for some nonzero integer n. Then

$$[2]P_1 = \psi(i(P_1)) = \psi(nP_2) = [n]\psi(P_2) = [nm]P_1 \pmod{E(\mathbb{Q})_{\mathrm{tor}}},$$

for some nonzero integer m. Thus $2 = nm$, so $n \leq 2$. □

If D satisfies the Heegner hypothesis, then by computing the residue symbol $\left(\frac{N}{D}\right)$ and understanding how the sign of the functional equation changes under twist, we see that

$$\mathrm{ord}_{s=1} L(E,s) \not\equiv \mathrm{ord}_{s=1} L(E^{(D)},s) \pmod 2.$$

Suppose K satisfies the Heegner hypothesis and $\mathrm{ord}_{s=1} L(E/K,s)=1$. Then work of Kolyvagin (see [Kol91, Kol88]) implies that $E(K)$ has rank 1.

The root number $\varepsilon_E = \pm 1$ of E is the sign of the functional equation of $L(E,s)$. If $\varepsilon_E=+1$, then the analytic rank $\mathrm{ord}_{s=1} L(E,s)$ is even, and if $\varepsilon_E=-1$, then it is odd.

Proposition 3.15. *Let E be an elliptic curve, let $D=D_K$ be a discriminant that satisfies the Heegner hypothesis such that $\mathrm{ord}_{s=1} L(E/K,s)=1$, and let $R=\mathbb{Z}[1/2]$. Then*

(1) *If $\varepsilon_E=+1$, then a generator of $E(K)\otimes R$ is the image of a generator of $E^D(\mathbb{Q})\otimes R$ and $L'(E/K,1)=L(E,1)\cdot L'(E^D,1)$.*
(2) *If $\varepsilon_E=-1$, then a generator of $E(K)\otimes R$ is the image of a generator of $E(\mathbb{Q})\otimes R$ and $L'(E/K,1)=L'(E,1)\cdot L(E^D,1)$.*

We will use the above proposition to relate computation of $E(K)\otimes R$ to computation of Mordell-Weil groups of elliptic curves defined over $\mathbb{Q}$.

3.5. **Computing the Index of the Heegner Point.** A key input to the theorems of Section 3.1 is computation of the index $[E(K):\mathbb{Z}y_K]$. We have

$$[E(K)_{/\mathrm{tor}}:\mathbb{Z}y_K]^2 = h(y_K)/h(z), \tag{3.1}$$

where z is a generator of $E(K)_{/\,\mathrm{tor}}$.

In the Gross-Zagier formula we have $h=h_K$, the Néron-Tate canonical height on $E(K)=E^D(K)$ relative to K. Let $h_{\mathbb{Q}}$ denote the height on $E(\mathbb{Q})$ or $E^D(\mathbb{Q})$. Note that if $P\in E(\mathbb{Q})$ or $E^D(\mathbb{Q})$, then

$$h_{\mathbb{Q}}(P) = \frac{1}{[K:\mathbb{Q}]}\cdot h_K(P) = \frac{h_K(P)}{2}. \tag{3.2}$$

Using Proposition 3.14 and algorithms for computing Mordell-Weil groups (see Section 2.3), we can compute z or $2z$, so we can compute $h(z)$ or $2h(z)$. In practice, even for curves of conductor up to 1000, it can take a huge amount of time to compute z. This section about practical methods to either compute the index or at least bound it.

It is not difficult to compute $h(y_K)$, without computing y_K itself, using the Gross-Zagier formula (Section 3.2). We compute $L'(E/K,1)$ by computing L-functions of elliptic curves defined over $\mathbb{Q}$ as explained in Proposition 3.15. It remains to compute

$$\alpha = \frac{\sqrt{|D|}}{c^2\int_{E(\mathbb{C})}\omega\wedge\overline{i\omega}}. \tag{3.3}$$

3.5.1. *The Manin Constant.* Manin conjectured that the Manin constant c for any optimal elliptic curve factor E of $X_0(N)$ is 1, and there are bounds on the possibilities for c (see, e.g., [Edi91, ARS05]). There is an algorithm to verify in any particular case that $c=1$, as explained in the proof of the following proposition.

Proposition 3.16 (Cremona). *If E is an optimal elliptic curve of conductor at most 80000, then the Manin constant of E is 1.*

Proof. For each level $N \leq 80000$ we do the following. Using the modular symbols algorithms of [Cre97], we enumerate the rational newforms $f_1, \ldots, f_d$, which correspond (via the modularity theorem) to the optimal elliptic curves $E_1, \ldots, E_d$ of conductor N, respectively. For each f_i we compute approximations to **xxx** decimal digits of the c_4 and c_6 invariants of the lattice Λ_{E_i} attached to the optimal curve in the isogeny class. We then guess integers c_4' and c_6' that are close to the computed approximations, and verify that the elliptic curve E_i' with invariants c_4', c_6' is an elliptic curve of conductor N. We also compute the full isogeny class of E_i' using the program `allisog`. Repeating this procedure for each newform f, we obtain d distinct isogeny classes of elliptic curves of conductor N, and by modularity these must be in bijection with the newforms f_i. However, at this point we have not *proved* that $E_i = E_i'$ or even that E_i' is an optimal quotient. However, we have provably found all elliptic curves over $\mathbb{Q}$ of conductor N.

We next compute the c_4 and c_6 invariants of all curves of conductor N, and observe that the first 12 digits of the c-invariants for these curves are sufficient to distinguish them. (12 digits is enough for every curve up to conductor 80000.) If we had guessed c_4' and c_6' incorrectly above, so that $E_i' \neq E_i$, there would be two curves of conductor N both of whose c-invariants have the same initial **xxx** decimal digits, which is impossible since 12 digits of precision are sufficient to distinguish any two. Thus $E_i' = E_i$, and the c_4', c_6' we computed are the correct invariants of the optimal quotient attached to f_i.

Finally, we observe that c_4' and c_6' are the invariants of a minimal Weierstrass equation, which implies that the Manin constant of E_i is 1. □

3.5.2. *The Integral.* We have the following lemma regarding the integral in (3.3):

Lemma 3.17. *We have $\int_{E(\mathbb{C})} \omega \wedge i\overline{\omega} = 2 \cdot \mathrm{Vol}(\mathbb{C}/\Lambda)$, where the volume $\mathrm{Vol}(\mathbb{C}/\Lambda)$ is the absolute value of the determinant of a matrix formed from a basis for the lattice in $\mathbb{C}$ obtained by integrating the Néron differential ω_E against all homology classes in $\mathrm{H}_1(E, \mathbb{Z})$.*

Proof. Fix the Weierstrass equation $y^2 = 4x^3 + g_4 x + g_6$ for E, so $x = \wp(z)$ and $y = \wp'(z)$. First note that

$$\omega = \frac{dx}{y} = \frac{d\wp(z)}{\wp'(z)} = \frac{\wp'(z)dz}{\wp'(z)} = dz.$$

Thus

$$\begin{aligned}
\int_{E(\mathbb{C})} \omega \wedge i\overline{\omega} &= i \int_{\mathbb{C}/\Lambda} dz \wedge \overline{dz} \\
&= i \int_{\mathbb{C}/\Lambda} (dx + idy) \wedge (dx - idy) \\
&= i(-2i) \int_{\mathbb{C}/\Lambda} dx \wedge dy = 2 \cdot \mathrm{Vol}(\mathbb{C}/\Lambda).
\end{aligned}$$

□

Note that $\mathrm{Vol}(\mathbb{C}/\Lambda)$ can be computed to high precision using the Gauss arithmetic-geometric mean, as described in [Cre97, §3.7].

3.5.3. *Mordell-Weil Groups and Heights.* For the curves that we run our computation on, we use [Creb] (via [Ste]), which computes a basis for $E^D(\mathbb{Q})$, and not just a basis for a subgroup of finite index.

Cremona describes the computation of heights of points on curves defined over $\mathbb{Q}$ in detail in [Cre97, §3.4]. There is an explicit bound on the error in the height computation, which shrinks exponentially in terms of the precision of approximating series, and can be made arbitrarily small. For the L-function computations, see Section 2.2.

3.5.4. *Indexes of Heegner Points on Rank* 1 *Curves.* Suppose E is an elliptic curve over $\mathbb{Q}$ of analytic rank 1, and we wish to compute indexes $i_K = [E(K)_{/\,\mathrm{tor}} : \mathbb{Z}y_K]$ for various K. Assume that $E(\mathbb{Q})$ is known, so we can compute $h(z)$ to high precision, where z generates $E(\mathbb{Q})/_{\mathrm{tor}}$. Then computing the indexes i_K is relatively easy. For each K, compute $h(y_K)$ as described above using the Gross-Zagier formula, so

$$h(y_K) = \alpha \cdot L'(E,1)\cdot L(E^D,1).$$

Then

$$i_K = \sqrt{\frac{h(y_K)}{h(z)}} = \sqrt{\frac{h(y_K)}{2h_{\mathbb{Q}}(z)}}.$$

We emphasize that computation of the Heegner point itself is not necessary. For the results of this index computation for E of conductor ≤ 1000, see Section 3.6.1.

Example 3.18. Let E be the elliptic curve 540B, which has rank 1, and conductor $540 = 2^2 \cdot 3^3 \cdot 5$. The first K that satisfies the Heegner hypothesis is $\mathbb{Q}(\sqrt{-71})$. The group $E(\mathbb{Q})$ is generated by $z = (0,1)$, and we have $h_{\mathbb{Q}}(z) \sim 0.656622630$. We have

$$\alpha \sim \frac{\sqrt{71}}{2\cdot 3.832955} \sim 1.09917,$$

so

$$h(y_K) \sim 1.09917 \cdot 1.9340458 \cdot 5.559761726 \sim 11.819.$$

Thus

$$i_K = \sqrt{\frac{11.819}{2\cdot 0.656622630}} \sim \sqrt{8.99999} \sim 3.$$

3.5.5. *Indexes of Heegner Points on Rank* 0 *Curves.* Assume that the analytic rank of E is 0. In practice, computing the indexes of Heegner points in this case is substantially more difficult than the rank 1 case. For a Heegner quadratic imaginary field $K = \mathbb{Q}(\sqrt{D})$, we have

$$i_K = [E(K)_{/\,\mathrm{tor}} : \mathbb{Z}y_K]^2 = \frac{h(y_K)}{h(z)} = \alpha \cdot \frac{L(E,1)\cdot L'(E^D,1)}{h(z)},$$

so one method to find i_K is to find a generator $z \in E^D(\mathbb{Q})$ exactly using descent algorithms, which will terminate since we know that $Ш(E^D)$ is finite, by Kolyvagin's theorem. However, since E^D has potentially large conductor and rank 1, in practice the Mordell-Weil group will sometimes be generated by a point of large height, hence be extremely time consuming to find. One can use 2-descent, 3-descent, 4-descent, and Heegner points methods (i.e., explicitly compute the coordinates of the Heegner point as decimals and try to recognize them using continued fractions.) In some cases these methods produce in a reasonable amount of time an element of

$E^D(\mathbb{Q})$ of infinite order, and one can then saturate the point using [Creb] to find a generator z.

Example 3.19. Let E be the curve 11A. The first field that satisfies the Heegner hypothesis is $K = \mathbb{Q}(\sqrt{-7})$. The conductor of $F = E^{-7}$ is 539, and we find a generator $z \in F(\mathbb{Q})$ for the Mordell-Weil group of this twist. This point has height $h_{\mathbb{Q}}(z) \sim 0.1111361471$. We have

$$\alpha \sim \frac{\sqrt{7}}{2 \cdot 1.8515436234} \sim 0.71447177.$$

The height over K of the Heegner point is thus

$$h(y_K) \sim 0.71447177 \cdot 0.25384186 \cdot 1.225566874 \sim 0.2222722925.$$

Thus by (3.2)

$$i_K = \frac{h(z)}{h(y_K)} = \frac{2h_{\mathbb{Q}}(z)}{h(y_K)} \sim 1.$$

There is a trick to bound the index i_K without computing *any* elements of $E(K)$. This is useful when the algorithms mentioned above for computing a generator of $E^D(\mathbb{Q})$ produce no information in a reasonable amount of time. First compute the height $h(y_K)$ using the Gross-Zagier formula. Next compute the Cremona-Prickett-Siksek [Pri04, Ch. 4] bound B for E^D, which is a number such that if $P \in E^D(\mathbb{Q})$, then the naive logarithmetic height of P is off from the canonical height of P by at most B. Using standard sieving methods implemented in [Creb], we compute all points on E of naive logarithmic height up to some number h_0. If we find any point of infinite order, we saturate, and hence compute $E^D(\mathbb{Q})$, then use the above methods. If we find no point of infinite order, we conclude that there is no point in $E^D(\mathbb{Q})$ of canonical height $\leq h_0 - B$. If $h_0 - B > 0$, we obtain an upper bound on i_K as follows. If z is a generator for $E^D(\mathbb{Q})$, then $h_{\mathbb{Q}}(z) > h_0 - B$, so using (3.2) we have

$$h_{\mathbb{Q}}(z) = \frac{1}{2} \cdot h_K(z) = \frac{h(y_K)}{2 \cdot i_K^2} > h_0 - B.$$

Solving for i_K gives

$$i_K < \sqrt{\frac{h(y_K)}{2(h_0 - B)}}, \tag{3.4}$$

so to bound i_K we consider many K (e.g., the first 30), and for each compute the quantity on the right side of (3.4) for a fixed choice of h_0. We then use a K that minimizes this quantity.

Remark 3.20. Another approach to finding some Heegner point, which we discussed with Noam Elkies, is to search for small points on $E(K)$ over various fields K, until finding a K that satisfies the Heegner hypothesis and is such that $E(K)$ has rank 1. For example, if E is given by $y^2 = x^3 + ax + b$, and x_0 is a small integer, write $y_0^2 \cdot D = x_0^3 + ax_0 + b$, where y_0 and D are integers, and D is square free. Then (x_0, y_0) is a point on the quadratic twist of E by D. We did not use this approach, since it was not necessary in order to prove Theorem 1.8.

Example 3.21. Let E be the elliptic curve 546E. Then $K = \mathbb{Q}(\sqrt{-311})$ satisfies the Heegner hypothesis, since the prime divisors of $546 = 2 \cdot 3 \cdot 7 \cdot 13$ split completely in K. We compute the height of the Heegner point y_K. Let F be the quadratic twist of E by -311. We have

$$\alpha \sim \frac{\sqrt{311}}{2 \cdot 0.0340964942689662168001} \sim 258.60711587$$

Thus

$$\begin{aligned} h(y_K) &\sim \alpha \cdot L(E,1) \cdot L'(F,1) \\ &\sim 258.60711587 \cdot 2.2783578 \cdot 12.41550 \sim 7315.20688, \end{aligned}$$

where in each case we compute the L-series using enough terms to obtain a value correct to $\pm 10^{-5}$. Thus 7320 is a conservative upper bound on $h(y_K)$. The Cremona-Prickett-Siksek bound for F is $B = 13.0825747$. We search for points on F of naive logarithmic height ≤ 18, and find no points. Thus (3.4) implies that

$$i_K < \sqrt{7320/(2 \cdot (18 - 13.0825747))} \sim 27.28171 < 28.$$

It follows that if $p \mid i_K$, then $p \leq 23$. Searching up to height 21 would (presumably) allow us to remove 23, but this might take much longer.

For the results of our computations for all E of conductor ≤ 1000, see Section 3.6.2.

3.6. **Results of Computations.**

3.6.1. *Curves of Rank* 1. First we consider curves of rank 1. Recall from Conjecture 1.6 that we expect Ш to be trivial for all optimal rank 1 curves of conductor at most 1000.

Proposition 3.22. *Suppose (E,p) is a pair with E an optimal elliptic curve of conductor up to* 1000 *of rank* 1*. Let I be the greatest common divisor of $[E(K)_{/\mathrm{tor}} : \mathbb{Z}y_K]$ for the first four quadratic imaginary fields $K = \mathbb{Q}(\sqrt{D})$ that satisfy the Heegner hypothesis. If $p \mid I$, then*

$$p \mid 2 \cdot \#E(\mathbb{Q})_{\mathrm{tor}} \cdot \prod_{q \mid N} c_{E,q},$$

except if (E,p) is $(540B,3)$ or $(756B,3)$.

Proof. For each rank 1 curve E of conductor up to 1000 we perform the following computation.

1. Let R_E be the regulator of E, correct to precision at least 10^{-10}, which we look up in the `allbsd` table of [Crea].
2. List the first four discriminants $D = D_0, D_1, D_2, D_3$ such that $K = \mathbb{Q}(\sqrt{D})$ satisfies the Heegner hypothesis. For each $D = D_i$ do the following computation:
   (a) Compute $L'(E,1)$ to some bounded precision ε, using $2\sqrt{N}+10$ terms. The bound ε is determined as explained in Section 2.2.
   (b) Compute $L(E^D,1)$ to some bounded precision ε' using $2\sqrt{N}+10$ terms.
   (c) Compute $\alpha = \sqrt{|D|}/(2\,\mathrm{Vol}(\mathbb{C}/\Lambda))$ to precision at least 10^{-10} using PARI.

(d) Using a simple implementation of classical interval arithmetic (in [Ste]) and the bounds above, we compute an interval in which the real number

$$\alpha \cdot L'(E,1) \cdot L'(E^D,1)/(\mathrm{Reg}_E/2)$$

must lie. If there is a unique integer in this interval, by Theorem 3.9 this must be the square of the index $[E(K) : \mathbb{Z}y_K]^2$. If there is no unique integer in this interval, we increase the precision of the computation of L' and L and repeat the above steps. In all cases in the range of our computation, we find a unique integer in the interval; as a double check on our calculations we verify that the integer is a perfect square.

□

Remark 3.23. For the curves 540B and 756B there is no 3-torsion, but there is a rational 3-isogeny. In each case we verified in addition that 3 divides the GCD of the indexes for at least the first 16 fields K that satisfy the Heegner hypothesis. Thus as in Remark 3.12, Conjecture 3.10 asserts that $9 \mid \#Ш(E/K)$ for the first sixteen K. This illustrates that not only Tamagawa numbers but also isogenies can be an obstruction to applying Kolyvagin's theorem to bound $\#Ш(E)$, even if the irreducibility hypothesis on $\overline{\rho}_{E,p}$ is removed.

Proposition 3.24. *Suppose E is a non-CM optimal curve of conductor ≤ 1000 and p is an odd prime such that $\overline{\rho}_{E,p}$ is irreducible but not surjective. If E has rank 0 then (E,p) is one of the following:* (245B,3), (338D,3), (352E,3), (608B,5), (675D,5), (675F,5), (704H,3), (722D,3), (726F,3), (800E,5), (800F,5), (864D,3), (864F,3), (864G,3), (864I,3). *If E has rank 1, then (E,p) is one of the following:* (245A,3), (338E,3), (352F,3), (608E,5), (675B,5), (675I,5), (704L,3), (722B,3), (726A,3), (800B,5), (800I,5), (864A,3), (864B,3), (864J,3), (864L,3). *There are no curves of rank ≥ 2 with the above property.*

Proof. Using Proposition 2.5 we make a list of pairs (E,p) such that $\overline{\rho}_{E,p}$ might not be surjective, and such that if (E,p) is not in this list, then $\overline{\rho}_{E,p}$ is surjective. Then using the program `allisog`, we compute for each curve E, a list of all degrees of isogenies emanating from E, and remove those pairs (E,p) for which p divides the degree of one of those isogenies. The curves listed above are the ones that remain. □

Remark 3.25. In Proposition 3.24, the non-surjective irreducible (E,p) come in pairs, one of rank 0 and one of rank 1 having the same conductor. Each pair of curves are related by a quadratic twist. This pattern is common, but does not always occur. For example, (1184F,3) and (1184H,3) are both of rank 0 and have non-surjective irreducible representation, and no curve of conductor 1184 and rank 1 has this property. Note that $1184 = 2^5 \cdot 37$ and 1184F and 1184H are quadratic twists of each other by -1.

Remark 3.26. Proposition 3.24 suggests that it is rare for $\overline{\rho}_{E,p}$ to be non-surjective yet irreducible. When this does occur, frequently $p^2 \mid N$, though not always. Continuing the computation to conductor 10000 we find that $p^2 \mid N$ about half the time in which $\overline{\rho}_{E,p}$ is non-surjective yet irreducible. This gives a sense of the extent to which Theorem 3.3 improves on Theorem 3.2.

Theorem 3.27. *Suppose (E, p) is a pair consisting of a rank 1 non-CM elliptic curve E of conductor ≤ 1000 and a prime p such that $\rho_{E,p}$ is irreducible and p does not divide any Tamagawa number of E. Then $\mathrm{BSD}(E, p)$ is true.*

Proof. By Theorem 3.31 we may assume that p is odd. The pairs that do not satisfy the Heegner point divisibility hypothesis in Proposition 3.22 are those in $S = \{(540B, 3), (756B, 3)\}$. However, both of these curves admit a rational 3-isogeny, so are excluded by the hypothesis of Theorem 3.27.

Let

$$\begin{aligned} T = \{&(245A, 3), (338E, 3), (352F, 3), (608E, 5), (675B, 5), (675I, 5),\\ &(704L, 3), (722B, 3), (726A, 3), (800B, 5), (800I, 5), (864A, 3),\\ &(864B, 3), (864J, 3), (864L, 3)\}. \end{aligned}$$

Then Proposition 3.24, Theorem 1.7, and Theorem 3.2 together imply $\mathrm{BSD}(E, p)$ for all pairs as in the hypothesis of Theorem 3.27, except the pairs in $S \cup T$. Note that for each $(E, p) \in T$, we have $p^2 \mid N$, so Theorem 3.3 does not apply either. We eliminate the pairs

$$(245A, 3), (338E, 3), (352F, 3), (608E, 5), (704L, 3), (864J, 3), (864L, 3)$$

from consideration because in each case $p \mid \prod c_\ell$.

For each $(E, p) \in T$ the representation $\overline{\rho}_{E,p}$ is irreducible and E does not have CM, so the hypothesis of Theorem 3.5 are satisfied. For the pairs

$$\{((245A, 3), (338E, 3), (352F, 3), (608E, 5), (704L, 3), (864J, 3), (864L, 3)\}$$

we have $p \mid [E(K) : \mathbb{Z}y_K]$ for the first six Heegner K, but that is not a problem since we eliminated these pairs from consideration. For the remaining pairs, in each case we find a K such that $p \nmid [E(K) : \mathbb{Z}y_K] \cdot \mathrm{disc}(K)$, so Theorem 3.5 implies that $p \nmid \#\text{Ш}(E)$, so $\mathrm{BSD}(E, p)$ is true. □

3.6.2. *Curves of Rank* 0.

Proposition 3.28. *Suppose (E, p) is a pair with E an optimal elliptic curve of conductor ≤ 1000 of rank 0. Let I be the greatest common divisor of $[E(K)_{/\,\mathrm{tor}} : \mathbb{Z}y_K]$ as K varies over quadratic imaginary fields that satisfy the Heegner hypothesis. If $p \mid I$ and $\overline{\rho}_{E,p}$ is irreducible, then*

$$p \mid 2 \cdot \#E(\mathbb{Q})_{\mathrm{tor}} \cdot \prod_{q \mid N} c_{E,q},$$

except possibly for the curves in the following table:

E	$p \mid I$?	D used
258E	3	-983
378G	3	-47
594F	3	-359
600G	3	-71
612D	3	-359
626B	3	-39
658A	3	-31
676E	5	-23
681B	3	-8
735B	3	-479
738B	3	-23
742F	3, 5	-199

E	$p \mid I$?	D used
777B	3	-215
780B	3,7	-191
819D	3,5	-404
850I	3	-151
858D	5, 7	-95
858K	7	-1031
900A	3	-71
906E	$p \leq 19$	-23
924A	5	-1679
978C	3	-431
980I	3	-671

In this table, the first column gives an elliptic curve, the second column gives the primes p (with $\overline{\rho}_{E,p}$ irreducible) that might divide the GCD *of indexes, and the third column gives the discriminant used to make this deduction.*

Proof. We use the methods described in Section 3.5.5, and precision bounds as in the proof of Proposition 3.22. In many cases we combined explicit computation of a Heegner point for one prime, with the bounding technique explained in Section 3.5.5, or only computed information using the bound.

For the curve 910E, we used four-descent via MAGMA to compute the point $(3257919871/16641, 133897822473008/2146689)$ on the -159 twist E^D, found using [Creb] that it generates $E^D(\mathbb{Q})$, and obtained an index that is a power of 2 and 3. Since 3 divides a Tamagawa number, we do not include 910E in our table. Likewise, for 930F and $D = -119$, we used MAGMA's four-descent commands to find a point of height ~ 85.3, and deduced that the only odd prime that divides the index is 11; since 11 is a Tamagawa number, we do not include 930F. Similar remarks apply for 966J with $D = -143$. We were unable to use 4-descent to find a generator for a twist of 906E1. (Fortunately, $906 = 2 \cdot 3 \cdot 151$, so Theorem 4.3 implies $\mathrm{BSD}(E, p)$ except for $p = 2, 3, 151$, and for our purposes we will only need that 151 does not divide the Heegner point index.) □

Remark 3.29. We could likely shrink the table in Proposition 3.28 further using MAGMA's four descent command. However, we will not need a smaller table for our ultimate application to the BSD conjecture (Theorem 4.4).

Theorem 3.30. *Suppose (E, p) is a pair with E a rank 0 non-CM curve of conductor ≤ 1000 and p a prime such that $\overline{\rho}_{E,p}$ is irreducible and p does not divide any Tamagawa number of E. Then* $\mathrm{BSD}(E, p)$ *is true except possibly if (E, p) appears in the table in the statement of Proposition 3.22, i.e., E appears in column* 1 *and p appears in the column directly to the right of p.*

Proof. The argument is similar to the proof of Theorem 3.27. By Theorem 3.31 we may assume that p is odd. Let S be the set of pairs (E, p) in the table in Proposition 3.22. Let

$$\begin{aligned} T = \{&(245B, 3), (338D, 3), (352E, 3), (608B, 5), (675D, 5), (675F, 5), \\ &(704H, 3), (722D, 3), (726F, 3), (800E, 5), (800F, 5), (864D, 3), \\ &(864F, 3), (864G, 3), (864I, 3)\}. \end{aligned}$$

Then Proposition 3.24, Theorem 1.7, and Theorem 3.2 together imply $\mathrm{BSD}(E,p)$ for all pairs as in the hypothesis of Theorem 3.27, except the pairs in $S \cup T$, since the representation $\overline{\rho}_{E,p}$ is surjective and we have verified that $p \nmid [E(K) : \mathbb{Z}y_K]$ for some K. We eliminate the pairs $(722D, 3)$ and $(726F, 3)$ from consideration because in each case $p \mid \prod c_\ell$.

For each $(E,p) \in T$ the representation $\overline{\rho}_{E,p}$ is irreducible and E does not have CM, so the hypotheses of Theorem 3.5 are satisfied. Next for each pair $(E,p) \in T$ except for $(722D, 3)$ and $(726F, 3)$, which we eliminated already, we find a K such that $p \nmid [E(K) : \mathbb{Z}y_K]$ and $\mathrm{disc}(K)$ is not divisible only be p. Theorem 3.5 implies that $p \nmid \#\text{Ш}(E)$, hence $\mathrm{BSD}(E,p)$ is true. □

3.6.3. *Two Descent.* In this section, we explain how descent computations imply that $\mathrm{BSD}(E,2)$ is true for curves of conductor $N \leq 1000$.

Theorem 3.31. *If E is an elliptic curve with $N \leq 1000$, then $\mathrm{BSD}(E,2)$ is true.*

Proof. According to Theorem 1.4, it suffices to prove the theorem for the set S of optimal elliptic curves with $N \leq 1000$. By doing an explicit 2-descent, Cremona computed $\mathrm{Sel}^{(2)}(E/\mathbb{Q})$ for every curve $E \in S$, as explained in [Cre97]. This implies that $\text{Ш}(E)[2]$ has order the predicted order of $\text{Ш}(E)[2^\infty]$ for all $E \in S$. Using MAGMA's `FourDescent` command, we compute $\mathrm{Sel}^{(4)}(E/\mathbb{Q})$ in the three cases in which $\text{Ш}(E)[2] \neq 0$, and find that $\text{Ш}(E)[4] = \text{Ш}(E)[2]$. By Theorem 1.7, it follows that $\mathrm{BSD}(E,2)$ is true for all $E \in S$. □

3.6.4. *Three Descent.* We sharpen Theorem 3.30 using Stoll's 3-descent package (see [Sto05]).

Proposition 3.32. *We have $3 \nmid \#\text{Ш}(E)$ for each of the curves listed in the Table in Proposition 3.28 with 3 in the second column and $\overline{\rho}_{E,3}$ irreducible, except for $681B$ where $\#\text{Ш}(E)[3^\infty] = 9$.*

Proof. We use Stoll's package [Sto05] to compute each of the Selmer groups

$$\mathrm{Sel}^{(3)}(E) \cong \text{Ш}(E)[3],$$

and obtain the claimed dimensions. When computing class groups in Stoll's package one must take care to not assume any conjectures (by slightly modifying the call to `ClassGroup` in `3descent.m`). Finally, that $\text{Ш}(E)[3^\infty] = 9$ follows by applying Theorem 3.2 with $K = \mathbb{Q}(\sqrt{-8})$, and noting that $\overline{\rho}_{E,3}$ is surjective and the index is exactly divisible by 3. □

4. The Kato Bound

Kato proved a theorem that bounds $\text{Ш}(E)$ from above when $L(E,1) \neq 0$.

Theorem 4.1 (Kato)**.** *Let E be an optimal elliptic curve over $\mathbb{Q}$ of conductor N, and let p be a prime such that $p \nmid 6N$ and $\rho_{E,p}$ is surjective. If $L(E,1) \neq 0$, then $\text{Ш}(E)$ is finite and*

$$\mathrm{ord}_p(\#\text{Ш}(E)) \leq \mathrm{ord}_p\left(\frac{L(E,1)}{\Omega_E}\right).$$

This theorem follows from the existence of an "optimal" Kato Euler system (see [Kat04] and [MR04]) combined with a recent result of Matsuno [Mat03] on finite submodules of Selmer groups over $\mathbb{Z}_p$-extensions. For more details, look at the proof of [Rub98, Cor. 8.9] where one replaces an unknown module with the module Matsuno computes. See also [Gri05] for further discussion and recent results on lower bounds on $\text{Ш}(E)$ that make use of optimal Kato Euler systems.

4.1. **Computations.** When $L(E,1) \neq 0$ the group $\text{Ш}(E)$ is finite, so $\operatorname{ord}_p(\#\text{Ш}(E))$ is even. Thus if $\operatorname{ord}_p\left(\frac{L(E,1)}{\Omega_E}\right)$ is odd, we conclude that

$$\operatorname{ord}_p(\#\text{Ш}(E)) \leq \operatorname{ord}_p\left(\frac{L(E,1)}{\Omega_E}\right) - 1.$$

Lemma 4.2. *There are no pairs (E,p) that satisfy the conditions of Theorem 4.1 with $N \leq 1000$, such that*

$$\operatorname{ord}_p(\#\text{Ш}(E)_{\mathrm{an}}) < \operatorname{ord}_p\left(\frac{L(E,1)}{\Omega_E}\right) - 1.$$

Proof. First we make a table of ratios $L(E,1)/\Omega_E$ for all curves of conductor $\leq$ 1000. For each of these with $L(E,1) \neq 0$, we factor the numerator of the rational number $L(E,1)/\Omega_E$. We then observe that the displayed inequality in the statement of the proposition does not occur. □

Theorem 4.3. *Suppose (E,p) is a pair such that $N \leq 1000$, $p \nmid 3N$, E is a non-CM elliptic curve of rank 0, and $\overline{\rho}_{E,p}$ is irreducible. Then $\mathrm{BSD}(E,p)$ is true.*

Proof. The statement for $p = 2$ follows from Theorem 3.31.

Let S be the set of pairs (E,p) as in the statement of Theorem 4.3 for which E is optimal and $p > 2$. By Theorem 1.7 it suffices to prove that $p \nmid \#\text{Ш}(E)$ for all $(E,p) \in S$. Using Proposition 2.5 with $A = 1000$, we compute for each rank 0 non-CM elliptic curve of conductor $N \leq 1000$, all primes $p \nmid 6N$ such that $\rho_{E,p}$ might not be surjective. This occurs for 53 pairs (E,p), with the E's all distinct. For these 53 pairs (E,p), we find that the representation $\overline{\rho}_{E,p}$ is reducible (since there is an explicit p isogeny listed in [Cre97]), except for the pair $(608B, 5)$, for which $\overline{\rho}_{E,5}$ is irreducible.

Thus Theorem 4.1 implies that for each pair $(E,p) \in S$, except $(608B, 5)$, we have the bound

$$\operatorname{ord}_p(\#\text{Ш}(E)) \leq \operatorname{ord}_p(L(E,1)/\Omega_E).$$

By Theorem 1.5, $\operatorname{ord}_p(\#\text{Ш}(E))$ is even, so $\text{Ш}(E)[p^\infty]$ is trivial whenever

$$\operatorname{ord}_p(L(E,1)/\Omega_E) \leq 1.$$

By Theorem 1.7, $\operatorname{ord}_p(\#\text{Ш}(E)_{\mathrm{an}}) = 0$ for all $p \geq 5$. Thus by Lemma 4.2, there are no pairs $(E,p) \in S$ with $\operatorname{ord}_p(L(E,1)/\Omega_E) > 1$ (since otherwise some $\operatorname{ord}_p(\#\text{Ш}(E)_{\mathrm{an}})$ would be nontrivial).

Finally, note that we dealt with $(608B, 5)$ in Lemma 3.4 using Cha's theorem. This completes the proof. □

4.2. **Combining Kato and Kolyvagin.** In this section we bound $\text{Ш}(E)$ for rank 0 curves by combining the Kato and Kolyvagin approaches.

Theorem 4.4. *Suppose E is a non-CM elliptic curve of rank 0 with conductor $N \leq 1000$, that $\overline{\rho}_{E,p}$ is irreducible, and that p does not divide any Tamagawa number of E. Then $\mathrm{BSD}(E,p)$ is true.*

Proof. Let (E, p) be as in the hypothesis to Theorem 4.4. By Theorem 4.3, $\mathrm{BSD}(E, p)$ is true, except possibly if $p \mid 3N$. Theorem 3.30 implies $\mathrm{BSD}(E, p)$, except if (E, p) appear in the Table of Proposition 3.28. Inspecting the table, we see that whenever a prime $p \geq 5$ is in the second column, then p does not divide the conductor N of E. This proves $\mathrm{BSD}(E, p)$ for $p \geq 5$.

Let E be the curve 681B. Then $\mathrm{BSD}(E, 3)$ asserts that $\#\text{Ш}(E)[3^\infty] = 9$. It follows from [CM00] and [AS05, App.], or from the 3-descent of Section 3.6.4 that $\#\text{Ш}(E)[3] = 9$. Also, $\overline{\rho}_{E,3}$ is surjective and for $D = -8$ we have $\mathrm{ord}_3([E(K) : \mathbb{Z}y_K]) = 1$, so $\#\text{Ш}(E)[3^\infty] \mid 9$, which proves $\mathrm{BSD}(E, 3)$.

Finally Proposition 3.32 implies $\mathrm{BSD}(E, 3)$ for the remaining curves, which proves the theorem. □

5. Proof of Theorem 3.5

In this section we prove Theorem 3.5. Assume that E and K are as in the statement of the theorem, and assume that $\mathrm{ord}_{s=1} L(E/K, 1) = 1$. Then the Heegner point y_K has infinite order. Kolyvagin ([Kol90]) shows that in this case the rank of $E(K)$ is 1 and $\text{Ш}(E/K)$ is finite.

5.1. Gross's Account.

Gross's account of Kolyvagin's work in [Gro91] contains a proof that if E does not have complex multiplication, then

$$\#\text{Ш}(E/K) \mid t \cdot [E(K) : \mathbb{Z}y_K]^2,$$

where t is an integer divisible only by primes p such that the representation $\overline{\rho}_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p])$ is not surjective. Gross makes no claim about the powers of primes that divide t (though Kolyvagin does in his papers). Our Theorem 3.5 provides a better bound, which removes the condition that E not have CM, and relaxes the surjectivity hypothesis on $\overline{\rho}_{E,p}$.

Gross uses surjectivity of $\overline{\rho}_{E,p}$ as a hypothesis only to prove the following two propositions. We will prove analogous propositions below, but under weaker hypotheses, which yields our claimed improvement to [Gro91].

Proposition 5.1 (Gross)**.** *Assume that $\overline{\rho}_{E,p}$ is surjective. For any integer n, let K_n be the ring class field of K of conductor n. The restriction map*

$$\mathrm{Res} : \mathrm{H}^1(K, E[p]) \to \mathrm{H}^1(K_n, E[p])^{\mathrm{Gal}(K_n/K)}$$

is an isomorphism.

Proof. That $\overline{\rho}_{E,p}$ is surjective implies that $E(K_n)[p] = 0$. The inflation-restriction-transgression sequence then implies that Res is an isomorphism. □

Gross also uses surjectivity of $\overline{\rho}_{E,p}$ when proving that the pairing

$$\mathrm{H}^1(K, E[p]) \otimes \mathrm{Gal}(K(E[p])/K) \to E[p]$$

is nondegenerate, as follows. Setting $L = K(E[p])$, we have that

$$\mathrm{H}^1(L/K, E(L)[p]) \to \mathrm{H}^1(K, E[p]) \to \mathrm{H}^1(L, E[p])^{\mathrm{Gal}(L/K)} \to \mathrm{H}^2(L/K, E(L)[p]).$$

To see that the pairing is nondegenerate, it suffices to know that the groups $\mathrm{H}^i(L/K, E[p])$ vanish for $i = 1, 2$. This is because we have

$$\mathrm{H}^1(L, E[p])^{\mathrm{Gal}(L/K)} = \mathrm{Hom}(G_L, E[p])^{\mathrm{Gal}(L/K)}$$

since $K(E[p]) \subset L$ and the pairing is $(c, \sigma) = \mathrm{res}_L(c)(\sigma)$. Thus nondegeneracy of the pairing then follows from the following proposition.

Proposition 5.2 (Gross)**.** *Let E be an elliptic curve over a number field K and let p be a prime. Assume that $\overline{\rho}_{E,p}$ is surjective. Then*

$$\mathrm{H}^i(K(E[p])/K, E[p]) = 0 \qquad \text{for all} \quad i \geq 1.$$

Proof. As above set $L = K(E[p])$. The surjectivity of $\overline{\rho}_{E,p}$ implies that

$$G = \mathrm{Gal}(L/K) \cong \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \cong \mathrm{GL}_2(\mathbb{F}_p).$$

If $Z \subset G$ is the subgroup corresponding to the scalars in $\mathrm{GL}_2(\mathbb{F}_p)$, then the Hochschild-Serre spectral sequence implies that

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

Since $\#Z = p-1$, and $E(L)[p]$ is a p-group, and p is odd, we have $\mathrm{H}^j(Z, E(L)[p]) = 0$ for all $j \geq 1$. Also, since p is odd, and non-identity scalars have no nonzero fixed points, $\mathrm{H}^0(Z, E(L)[p]) = 0$. Thus for all i, j we have

$$\mathrm{H}^i(G/Z, \mathrm{H}^j(Z, E(L)[p])) = 0,$$

which implies that the groups $\mathrm{H}^{i+j}(L/K, E(L)[p])$ are all 0. □

Thus our goal is to prove analogues of Propositions 5.1–5.2 under hypotheses that are more amenable to computation.

5.2. **Preliminaries.**

Lemma 5.3. *The determinant of $\overline{\rho}_{E,p}$ is the cyclotomic character, hence $\det(\overline{\rho}_{E,p})$ is surjective.*

Proof. For the convenience of the reader, we give a proof here. The Weil pairing induces an isomorphism of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules $E[p] \wedge E[p] \cong \mu_p$. 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

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

It follows that composition with the determinant gives the cyclotomic character (i.e., the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on μ_p), which is surjective since no nontrivial roots of unity lie in $\mathbb{Q}$. □

We will choose the quadratic field K to be linearly disjoint from $\mathbb{Q}(E[p])$, so $\mathrm{Gal}(K(E[p])/K) \cong \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$. Thus, for our application, it will suffice to show vanishing of $\mathrm{H}^i(\mathbb{Q}(E[p])/\mathbb{Q}, E[p])$, for $i > 0$.

Let $G \subseteq \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ be the image of $\overline{\rho}_{E,p}$. If $p \nmid \#G$, then for $i > 0$ we have $\mathrm{H}^i(G, E[p]) = 0$ since $E[p]$ is a p-group. Therefore we may assume that $p \mid \#G$. By [Ser72, Prop. 15], the image G either contains $\mathrm{SL}_2(\mathbb{F}_p)$ or is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. If G contains $\mathrm{SL}_2(\mathbb{F}_p)$ then properties of the Weil pairing imply that

$$\det : G \to \mathbb{F}_p^*$$

is surjective, so $G = \mathrm{GL}_2(\mathbb{F}_p)$. In this case, we already know Propositions 5.1–5.2.

Lemma 5.4. *Assume that G is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Moreover, assume that there is a basis of $E[p]$ so that G acts as $\left(\begin{smallmatrix} \chi & * \\ 0 & \psi \end{smallmatrix}\right)$ where χ and ψ are nontrivial characters. Then $\mathrm{H}^i(G, E[p]) = 0$.*

Proof. Let $W = \left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right)$ be the unique p-Sylow subgroup of $\left(\begin{smallmatrix}* & *\\ 0 & *\end{smallmatrix}\right) \subset \mathrm{GL}_2(\mathbb{F}_p)$. We may assume $W \subset G$, for otherwise G has order prime to p, and the cohomology vanishes.

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

$$\cdots \to \mathbb{Z}[W] \to \mathbb{Z}[W] \to \mathbb{Z} \to 0$$

where the boundary maps alternate between multiplication by $w - 1$ and $\mathrm{Norm} = \sum_{i=0}^{p-1} w^i$.

Then we see that

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

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

$$\mathrm{H}^i(G/W, \mathrm{H}^j(W, E[p])) \Rightarrow \mathrm{H}^{i+j}(G, E[p]).$$

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

5.3. **Analogue of Proposition 5.1.** In this section we verify that $\mathrm{H}^i(K_n/K, E(K_n)[p]) = 0$ under a simple condition on p-torsion over K.

Proposition 5.5. *Let E be an elliptic curve over $\mathbb{Q}$ and K be a quadratic imaginary extension of $\mathbb{Q}$. Assume that p is a prime with $p \nmid \#E(K)_{\mathrm{tor}}$ and if $p = 3$ assume that $K \neq \mathbb{Q}(\zeta_3)$. Then for every finite abelian extension L of K we have*

$$\mathrm{H}^i(L/K, E(L)[p]) = 0 \qquad \textit{for all} \quad i \geq 1.$$

Proof. Write the abelian group $\mathrm{Gal}(L/K)$ as a direct sum $P \oplus P'$, where P is its Sylow p-subgroup, so $p \nmid \#P'$. First we show that the subgroup of $E(L)[p]$ invariant under P' is trivial. Let $G = \mathrm{Gal}(L/K)/H$, where H is the subgroup of $\mathrm{Gal}(L/K)$ that acts trivially on $E(L)[p]$. Thus $G \subset \mathrm{Aut}(E(L)[p])$.

Case 1. If $p \nmid \#G$, then $P \subseteq H$, so P' surjects onto G. There is no nonzero element of $E(L)[p]$ invariant under $\mathrm{Gal}(L/K)$ by our assumption that $p \nmid \#E(K)$, so the same holds for P'.

Case 2. If $p \mid \#G$, we cannot have $E(L)[p] = \mathbb{F}_p$, since $\mathbb{F}_p$ has automorphism group isomorphic to $\mathbb{F}_p^*$, of order $p-1$, but $G \subset \mathrm{Aut}(E(L)[p])$ and $\#G > p - 1$. Thus, $E(L)[p]$ is the full p-torsion subgroup of E, and we identify G with a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ acting on $E(L)[p] = \mathbb{F}_p^2$.

We can choose a basis of $\mathbb{F}_p^2$ so that G contains the subgroup generated by $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. Since G is abelian, it must be contained in the normalizer of this subgroup, so $G \subseteq \{\left(\begin{smallmatrix}a & b\\ 0 & a\end{smallmatrix}\right) : a \in \mathbb{F}_p^*, b \in \mathbb{F}_p\}$. We claim that G contains an element with $a \neq 1$. Since $E[p] = E(L)[p]$, the representation $\mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{Aut}(E[p])$ factors through $\mathrm{Gal}(L/K)$. The determinant of $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$ is surjective onto $\mathbb{F}_p^*$, and $[K : \mathbb{Q}] = 2$, so the character $\mathrm{Gal}(\overline{K}/K) \to \mathbb{F}_p^*$ has image of index at most 2 in

F_p^*. That is, it contains at least $(p-1)/2$ elements, the squares in $\mathbb{F}_p^*$. Thus, for $p > 3$, the group 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 $a, b \in \mathbb{F}_p$, so $\mathrm{Gal}(L/K)$ contains an element that acts as a nontrivial scalar. Since the group of scalars in $\mathrm{GL}_2(\mathbb{F}_p)$ has $p-1)$ elements, this nontrivial scalar must be in P', so $E(L)[p]^{P'} = 0$.

We have shown in each case that $E(L)[p]^{P'} = 0$. Because $p \nmid \#P'$ we have $\mathrm{H}^i(P', E(L)[p]) = 0$ for all $i \geq 1$, so for each $i \geq 1$ there is an exact inflation-restriction sequence

$$0 \to \mathrm{H}^i(P, E(L)[p]^{P'}) \to \mathrm{H}^i(L/K, E(L)[p]) \to \mathrm{H}^i(P', E(L)[p]).$$

The first group vanishes since $E(L)[p]^{P'} = 0$, and the third group vanishes as mentioned above. We conclude that $\mathrm{H}^i(L/K, E(L)[p]) = 0$, as claimed.

Finally we deal with the case $p = 3$. The only situation in the above argument where $p = 3$ is relevant is in Case 2, when $3 \mid \#G$. Our hypothesis that $K \neq \mathbb{Q}(\zeta_3)$ implies that $\det(\rho_{E,3}) : \mathrm{Gal}(\overline{K}/K) \to \mathbb{F}_3^*$ is surjective, since the fixed field of the kernel of the mod 3 cyclotomic character is $\mathbb{Q}(\zeta_3)$. If we are in Case 2, then the image of $\mathrm{Gal}(\overline{K}/K)$ in $\mathrm{GL}_2(\mathbb{F}_3)$ is contained in $\{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) : a \in \mathbb{F}_p^*, b \in \mathbb{F}_p\}$. Since no upper triangular matrix has determinant 2, this contradicts surjectivity of $\det(\rho_{E,3})$. Thus our hypothesis that $K \neq \mathbb{Q}(\zeta_3)$ implies that Case 2 does not occur. □

Corollary 5.6. *Let E be an elliptic curve with $p \nmid \#E(K)_{\mathrm{tor}}$, where $p > 3$ or, if $p = 3$, $K \neq \mathbb{Q}(\zeta_3)$. Let K_n be the ring class field of conductor n of K. Then $\mathrm{H}^i(K_n/K, E(K_n)[p]) = 0$ for all $i \geq 1$.*

Lemma 5.7. *Let E be an elliptic curve over $\mathbb{Q}$, let K be a quadratic imaginary extension, and let $p \mid \#E(K)_{\mathrm{tor}}$ an odd prime. If $p = 3$, assume $K \neq \mathbb{Q}(\zeta_3)$. Then $\overline{\rho}_{E,p}$ is reducible.*

Proof. Let $P \in E(K)[p]$ be nonzero, and let τ be a lift of the generator of $\mathrm{Gal}(K/\mathbb{Q})$ to $G_{\mathbb{Q}}$. If τP is a multiple of P, then the one-dimensional subspace of $E[p]$ generated by P is $G_{\mathbb{Q}}$-stable, so $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$ is is reducible. If τP is not a multiple of P, then P and τP generate all of $E[p]$. Since $\tau P \in E(K)$, we have $E(K)[p] = E(\overline{\mathbb{Q}})[p]$. Because the Weil pairing in nondegenerate we have $\mu_p \subset K$. This is a contradiction by our hypothesis on K and p. Since $p > 3$, this is a contradiction. □

5.4. **Analogue of Proposition 5.2.** In this section we show how vanishing of $\mathrm{H}^i(\mathbb{Q}(E[p])/\mathbb{Q}, E[p])$ follows from a statement about torsion and rational isogenies.

Note that E has no $\mathbb{Q}$-rational p-isogeny if and only if $\overline{\rho}_{E,p}$ is irreducible.

Proposition 5.8. *If p is an odd prime and E has no $\mathbb{Q}$-rational p-isogeny, then $\mathrm{H}^i(\mathbb{Q}(E[p])/\mathbb{Q}, E[p]) = 0$ for all $i > 0$.*

Proof. Our hypothesis that E has no $\mathbb{Q}$-rational p-isogeny implies that $\overline{\rho}_{E,p}$ is irreducible. As we already noted, the problem reduces to the case when either G is contained in a Borel subgroup or $G = \mathrm{GL}_2(\mathbb{F}_p)$. The latter case follows from Proposition 5.2. The former case contradicts the hypothesis since the module $E[p]$ is reducible as a module over a Borel subgroup. □

For the above result, we used the irreducibility of the representation to deal with the case when G was contained in a Borel subgroup. The following proposition completes the proof of the general case:

Proposition 5.9. *Suppose p is an odd prime and that $E(\mathbb{Q})[p] = 0$ and for all elliptic curves E' that are p-isogenous to E over $\mathbb{Q}$ we have $E'(\mathbb{Q})[p] = 0$. Then*

$$\mathrm{H}^i(\mathbb{Q}(E[p])/\mathbb{Q}, E[p]) = 0 \qquad \textit{for all} \qquad i > 0.$$

Proof. If E admits no p-isogeny, then Proposition 5.8 implies the required vanishing. Thus E admits a rational p-isogeny, so $E[p]$ is reducible, and $G = \mathrm{Im}(\overline{\rho}_{E,p})$ is contained in a Borel subgroup. In particular, for some basis of $E[p]$, the image G acts as $\left(\begin{smallmatrix} \chi & * \\ 0 & \psi \end{smallmatrix}\right)$ for characters χ and ψ. If both χ and ψ are nontrivial, then Lemma 5.4 implies the proposition and we are done. Thus assume that either χ or ψ is trivial.

First suppose 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 $E(\mathbb{Q})[p] = 0$.

Next suppose 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 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable subspace of $E[p]$. In particular, there exists an isogeny over $\mathbb{Q}$ to a curve E' having this line as kernel. The image under this isogeny of the line generated by $\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$ is a 1-dimensional subspace of $E'[p]$, and since $\psi = 1$, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 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, $E'(\mathbb{Q})[p]$ is nontrivial, contradicting our assumption.

□

References

[ABC+] B. Allombert, K. Belabas, H. Cohen, X. Roblot, and I. Zakharevitch, `PARI/GP`, `http://pari.math.u-bordeaux.fr/`.

[ARS05] A. Agashe, K. A. Ribet, and W. A. Stein, *The manin constant, congruence primes, and the modular degree*, Preprint, `http://modular.fas.harvard.edu/papers/manin-agashe/` (2005).

[AS05] A. Agashe and W. Stein, *Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero*, Math. Comp. **74** (2005), no. 249, 455–484 (electronic), With an appendix by J. Cremona and B. Mazur. MR 2085902

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* **Q***: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic). MR 2002d:11058

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265, Computational algebra and number theory (London, 1993). MR 1 484 478

[BFH90] Daniel Bump, Solomon Friedberg, and Jeffrey Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. **102** (1990), no. 3, 543–618. MR MR1074487 (92a:11058)

[Cas62] J. W. S. Cassels, *Arithmetic on curves of genus* 1*. III. The Tate-Šafarevič and Selmer groups*, Proc. London Math. Soc. (3) **12** (1962), 259–296. MR 29 #1212

[Cas65] J. W. S. Cassels, *Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **217** (1965), 180–199. MR 31 #3420

[Cha03] Byungchul Cha, *Vanishing of Some Cohomology Groups and Bounds for the Shafarevich-Tate Groups of Elliptic Curves*, Johns-Hopkins Ph.D. Thesis (2003).

[Cha05] ———, *Vanishing of some cohomology groups and bounds for the Shafarevich-Tate groups of elliptic curves*, J. Number Theory. **111** (2005), 154–178.

[CK] Alina Carmen Cojocaru and Ernst Kani, *On the surjectivity of the galois representations associated to non-cm elliptic curves.*

[CM00] J. E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. **9** (2000), no. 1, 13–28. MR 1 758 797

[Coh93] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin, 1993. MR 94i:11105

[Crea] J. E. Cremona, *Elliptic curves of conductor* ≤ 25000, `http://www.maths.nott.ac.uk/personal/jec/ftp/data/`.

[Creb] ———, `mwrank` *(computer software)*, `http://www.maths.nott.ac.uk/personal/jec/ftp/progs/`.

[Cre97] ———, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997, `http://www.maths.nott.ac.uk/personal/jec/book/`.

[Edi91] B. Edixhoven, *On the Manin constants of modular elliptic curves*, Arithmetic algebraic geometry (Texel, 1989), Birkhäuser Boston, Boston, MA, 1991, pp. 25–39. MR 92a:11066

[Gri05] G. Grigorov, *Kato's Euler System and the Main Conjecture*, Harvard Ph.D. Thesis (2005).

[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

[Jor05] A. Jorza, *The Birch and Swinnerton-Dyer Conjecture for Abelian Varieties over Number Fields*, Harvard University Senior Thesis (2005).

[Kat04] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque (2004), no. 295, ix, 117–290, Cohomologies p-adiques et applications arithmétiques. III. MR MR2104361

[Kol88] V. A. Kolyvagin, *Finiteness of $E(\mathbf{Q})$ and $Ш(E, \mathbf{Q})$ for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671. MR 89m:11056

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

[Kol91] V. A. Kolyvagin, *On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves*, Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990) (Tokyo), Math. Soc. Japan, 1991, pp. 429–436. MR 93c:11046

[Lan91] S. Lang, *Number theory. III*, Springer-Verlag, Berlin, 1991, Diophantine geometry. MR 93a:11048

[Man72] J. I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66. MR 47 #3396

[Mat03] Kazuo Matsuno, *Finite Λ-submodules of Selmer groups of abelian varieties over cyclotomic $\mathbb{Z}_p$-extensions*, J. Number Theory **99** (2003), no. 2, 415–443. MR MR1969183 (2004c:11098)

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

[McC91] W. G. McCallum, *Kolyvagin's work on Shafarevich-Tate groups*, L-functions and arithmetic (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, pp. 295–316. MR 92m:11062

[Mil86] J. S. Milne, *Arithmetic duality theorems*, Academic Press Inc., Boston, Mass., 1986.

[MM91] M. Ram Murty and V. Kumar Murty, *Mean values of derivatives of modular L-series*, Ann. of Math. (2) **133** (1991), no. 3, 447–475. MR MR1109350 (92e:11050)

[MR04] Barry Mazur and Karl Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799, viii+96. MR MR2031496 (2005b:11179)

[Pri04] M. Prickett, *Saturation of Mordell-Weil Groups of Elliptic Curves over Number Fields*, U. Nottingham, Ph.D. thesis `http://etheses.nottingham.ac.uk/archive/00000052/` (2004).

[PS99] B. Poonen and M. Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149. MR 2000m:11048

[Rub98] K. Rubin, *Euler systems and modular elliptic curves*, Galois representations in arithmetic algebraic geometry (Durham, 1996), Cambridge Univ. Press, Cambridge, 1998, pp. 351–367. MR 2001a:11106

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

[Ser98] ———, *Abelian ℓ-adic representations and elliptic curves*, A K Peters Ltd., Wellesley, MA, 1998, With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

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

[Ste] W. A. Stein, `SAGE`, `http://modular.fas.harvard.edu/SAGE`.

[Sto05] M. Stoll, *Explicit* 3*-descent in Magma*
`http://www.faculty.iu-bremen.de/stoll/magma/explicit-3descent/`.

[Wal85] J.-L. Waldspurger, *Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie*, Compositio Math. **54** (1985), no. 2, 173–242. MR MR783511 (87g:11061b)

[Wil95] A. J. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

[Wil00] ———, *The Birch and Swinnerton-Dyer Conjecture*,
`http://www.claymath.org/prize_problems/birchsd.htm`.

[Zha04] Shou-Wu Zhang, *Gross-Zagier formula for* GL(2)*. II*, Heegner points and Rankin L-series, Math. Sci. Res. Inst. Publ., vol. 49, Cambridge Univ. Press, Cambridge, 2004, pp. 191–214. MR MR2083213