LMS J. Comput. Math. 14 (2011) 327–350 © 2011 Author
doi:10.1112/S1461157011000180

Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one

Robert L. Miller

Abstract

We describe an algorithm to prove the Birch and Swinnerton-Dyer conjectural formula for any given elliptic curve defined over the rational numbers of analytic rank zero or one. With computer assistance we rigorously prove the formula for 16714 of the 16725 such curves of conductor less than 5000.

1. *Introduction*

Let E be an elliptic curve defined over $\mathbb{Q}$, given by a global minimal Weierstrass equation. We denote the identity of E by $\mathcal{O}$, the rank of the Mordell–Weil group $E(\mathbb{Q})$ by r and the conductor of E by N. For each prime p, let $c_p(E)$ be the Tamagawa number at p and let $a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p)$, where $\tilde{E}(\mathbb{F}_p)$ is the mod-p reduction of E. Let $L(E/\mathbb{Q}, s)$ be the Hasse–Weil L-function of E, and denote its order of vanishing at $s = 1$ by $r_{\mathrm{an}}(E/\mathbb{Q})$. The regulator of $E(\mathbb{Q})$ is denoted $\mathrm{Reg}(E(\mathbb{Q}))$. Let ω denote the minimal invariant differential of E and let $\Lambda = \{\int_\alpha \omega : \alpha \in H_1(E, \mathbb{Z})\}$ be the canonical period lattice of E. Let $\Omega(E) = \int_{E(\mathbb{R})} |\omega|$ be the real period (the least positive real element of Λ) times the order of the component group of $E(\mathbb{R})$ and let $\|\omega\|^2 = \int_{E(\mathbb{C})} \omega \wedge \overline{i\omega}$ be twice the area of the fundamental domain of Λ. Denote the Shafarevich–Tate group by $Ш(\mathbb{Q}, E)$ and for G an abelian group let G_{tors} denote its torsion subgroup and let $G_{/\mathrm{tors}}$ denote the quotient group G/G_{tors}.

Let $\#Ш(\mathbb{Q}, E)_{\mathrm{an}}$ denote the following quantity:

$$\#Ш(\mathbb{Q}, E)_{\mathrm{an}} = \frac{L^{(r)}(E/\mathbb{Q}, 1)}{r!} \cdot \frac{\#E(\mathbb{Q})^2_{\mathrm{tors}}}{\Omega(E) \cdot \prod_p c_p(E) \cdot \mathrm{Reg}(E(\mathbb{Q}))}.$$

The Birch and Swinnerton-Dyer (BSD) conjecture states that the rank r of $E(\mathbb{Q})$ is equal to the analytic rank $r_{\mathrm{an}}(E/\mathbb{Q})$, the Shafarevich–Tate group is finite and its order is given by the formula

$$\#Ш(\mathbb{Q}, E) = \#Ш(\mathbb{Q}, E)_{\mathrm{an}}.$$

Definition 1.1. We denote by $\mathrm{BSD}(E/\mathbb{Q}, p)$ the following assertions.

(i) The rank r of $E(\mathbb{Q})$ is equal to the analytic rank $r_{\mathrm{an}}(E/\mathbb{Q})$.
(ii) The p-primary part $Ш(\mathbb{Q}, E)(p)$ of the Shafarevich–Tate group is finite.
(iii) The positive real number $\#Ш(\mathbb{Q}, E)_{\mathrm{an}}$ is rational.
(iv) The conjectural formula holds at p, that is,

$$\mathrm{ord}_p(\#Ш(\mathbb{Q}, E)_{\mathrm{an}}) = \mathrm{ord}_p(\#Ш(\mathbb{Q}, E)(p)).$$

We also denote $\mathrm{BSD}(E, p) = \mathrm{BSD}(E/\mathbb{Q}, p)$, and note that there is a definition of $\mathrm{BSD}(A/K, \mathfrak{p})$ for abelian varieties A over global fields K in general — see, for example, [**35**, III, Section 5] for details.

Received 10 April 2011; revised 27 June 2011.

2000 Mathematics Subject Classification 11G40 (primary), 14G10, 11-04 (secondary).

By the modularity theorem [6, 59], every elliptic curve E defined over $\mathbb{Q}$ has a modular parametrization $\psi : X_0(N) \to E$. If for each isogenous curve E' with modular parametrization $\psi' : X_0(N) \to E'$ we have that $\psi' = \varphi \circ \psi$ for some isogeny φ, then we say that E is an optimal elliptic curve, often called a strong Weil curve in the literature. Every elliptic curve over $\mathbb{Q}$ has an optimal elliptic curve in its isogeny class and by the characterizing property this curve is unique. Thus, we can use optimal curves as isogeny class representatives and, by isogeny invariance of $\mathrm{BSD}(E, p)$ which is proved in [10], focus on optimal curves.

If $r_{\mathrm{an}}(E/\mathbb{Q}) \leqslant 1$, then all but the last part of $\mathrm{BSD}(E/\mathbb{Q}, p)$ is known, so in this case $\mathrm{BSD}(E/\mathbb{Q}, p)$ is equivalent to the last equality. Clearly, the Birch and Swinnerton-Dyer conjecture holds if and only if $\#Ш(\mathbb{Q}, E)_{\mathrm{an}} > 0$ and, for each prime p, $\mathrm{BSD}(E/\mathbb{Q}, p)$ is true. The rank conjecture has been verified for $E/\mathbb{Q}$ of conductor $N < 130\,000$ [15]. This is possible because E is known to be modular and the analytic rank is at most three. We can compute the ratio $L(E, 1)/\Omega(E) \in \mathbb{Q}$ exactly, use the Gross–Zagier–Zhang formula (Theorem 4.1) to provably determine whether $L'(E, 1) = 0$, numerically compute the second and third derivatives to desired precision and use parity to determine the exact analytic rank in this case. It is worth noting that $\#Ш(\mathbb{Q}, E)_{\mathrm{an}}$ is not even known to be a rational number for a single curve such that $r_{\mathrm{an}}(E/\mathbb{Q}) > 1$.

In this note, we describe a well-known algorithm which computes the order of the Shafarevich–Tate group of any elliptic curve E such that $r_{\mathrm{an}}(E/\mathbb{Q}) \leqslant 1$ (see Theorem 4.7). This either proves the full conjecture for E or produces a counterexample. We aim to make this algorithm as explicit and efficient as possible. We also report the results of computer calculations which prove the following theorem.

THEOREM 1.2. *Suppose that $E/\mathbb{Q}$ is an elliptic curve of conductor $N < 5000$ and (analytic) rank at most one. If p is a prime such that $E[p]$ is irreducible, then* $\mathrm{BSD}(E, p)$ *holds. If $E[p]$ is reducible and the pair (E, p) is not one of the eleven pairs appearing in Table 10, then* $\mathrm{BSD}(E, p)$ *holds.*

Note that this gives the full Birch and Swinnerton-Dyer conjecture for 16714 curves of the 16725 of analytic rank at most one and conductor at most 5000. The remaining cases will be treated in forthcoming papers with Michael Stoll and with Brendan Creutz — see Section 9 for more details.

In their original work [4], Birch and Swinnerton-Dyer formulated a theory of reduced quartic forms in order to determine representations of the 2-Selmer groups of elliptic curves. They studied curves of the form $y^2 = x^3 - D$ and $y^2 = x^3 - Dx$ and did extensive computations to give lower and upper bounds for the ranks of the Mordell–Weil groups for $|D| \leqslant 400$ in the first case and $|D| \leqslant 200$ in the second case. In [5], they studied curves E_D of the form $y^2 = x^3 - Dx$ even more closely, expressing $L(E_D/\mathbb{Q}, 1)$ in terms of division values of the Weierstrass $\wp$-function. They showed that

$$L(E_D/\mathbb{Q}, 1) = \begin{cases} D^{-1/4}\omega_D\sigma(D) & \text{for } D > 0, \\ (-4D)^{-1/4}\omega_D\sigma(D) & \text{for } D < 0, \end{cases}$$

where ω_D is the real period of $\wp$ and $\sigma(D)$ is a rational number.

Swinnerton-Dyer was able to secure plenty of time on the computer *EDSAC* II by programming its first operating system. He and Birch used this opportunity to run numerical experiments for 1348 values of D, leading them at first to conjecture that $\sigma(D)$ was roughly the order of the Shafarevich–Tate group $Ш(\mathbb{Q}, E_D)$. Motivated by Cassels, they used these computations to formulate the conjecture that the order of $Ш(\mathbb{Q}, E_D)$ is $\#E_D(\mathbb{Q})^2/\tau(D)$, where $\tau(D) = \prod_{p \leqslant \infty} \int_{E_D(\mathbb{Q}_p)} \omega_p$ is the Tamagawa number and $\omega = dx/y$ is an invariant differential on E_D.

Razar further studied these curves E_D. Razar's studies were based on the observation of Tate that if there are no first descents for the 2-isogenies between E_D and E_{-4D}, then $E_D(\mathbb{Q})$ is finite and $Ш(\mathbb{Q}, E_D)[2^\infty]$ is trivial. In [42], Razar confirmed that when there are no first descents, the order of $Ш(\mathbb{Q}, E_D)$ predicted by the conjecture is a 2-adic unit for D equal to $\pm p, \pm p^2, \pm p^3, \pm 4p, \pm 4p^2$ and $\pm 4p^3$, where p is a prime. In [43], he showed that when D is p^2 or $-4p^2$, the prime p satisfies $p \equiv 9 \pmod{16}$ and p has 2 as a quartic residue, then $E_D(\mathbb{Q})$ is finite and $Ш(\mathbb{Q}, E_D)[2^\infty]$, which is now non-trivial, has the order predicted by the conjecture.

The full conjecture for abelian varieties over global fields can be found stated in [56], in which Tate extended Cassels' result [10] on the isogeny invariance of the conjectural formula from elliptic curves to abelian varieties over number fields. He also showed this invariance for abelian varieties over function fields $\mathbb{F}_q(t)$, as long as the isogeny is of degree prime to the characteristic to the field. In the same paper, Artin and Tate showed that over function fields, the L-function has a zero of order at least the rank of the Mordell–Weil group, and by [40, II.9.7] these two ranks are equal if and only if the Shafarevich–Tate group is finite.

Buhler, Gross and Zagier [7] studied the first curve over $\mathbb{Q}$ (ordered by conductor) of rank three, $E : y^2 = 4x^3 - 28x + 25$. In this case, it is not known that the order of the Shafarevich–Tate group predicted by the conjecture is a rational number, nor that the group itself is finite. Nonetheless, the authors managed to show that if E is modular, which is now known to be the case, then the analytic rank equals the algebraic rank and the two sides of the conjectural formula agree up to 29 decimal places. In [24], Flynn, Leprévost, Schaefer, Stein, Stoll and Wetherell considered 32 curves of genus 2 over $\mathbb{Q}$ whose Jacobians J are modular abelian surfaces. They computed to very high numerical precision the conjectured order of the Shafarevich–Tate group of $J/\mathbb{Q}$, and they found in each case that this is very close to an integer, which is in fact equal to the order of the 2-torsion of the Shafarevich–Tate group.

In the rest of this note, we will focus on elliptic curves over number fields, restricting our attention to $\mathbb{Q}$ and occasionally to certain quadratic imaginary number fields. Much more is known in these cases, especially when the L-function has a zero of order at most one: see Sections 2–4. This note was inspired by the work in [27], in which the full conjectural formula was shown to hold for a large number of curves of conductor up to 1000. In the present note, we extend this work to conductor 5000 and prove the formula for a much larger proportion of the curves considered, using various n-descents, Heegner point computations and Iwasawa theory. In contrast to the results in [7] and [24], the final results are not a numerical verification to high accuracy, but a complete proof of the truth of the Birch and Swinnerton-Dyer conjecture.

Whenever we prove a theorem with the help of a computer, questions regarding errors in both hardware and software arise. Any computer-assisted proof implicitly includes as a hypothesis the statement that the software used did not encounter any bugs (hardware or software errors) during execution. Few software programs for serious number theory research have been proven correct. However it is often noted in the literature, as it is in Birch and Swinnerton-Dyer's seminal note [4, p. 18] itself, that the kind of algorithms which occur in number theory (and more importantly the errors computational number theorists are likely to make implementing them) are often of a very particular sort. Either the software will work correctly or very quickly fail in an obvious way — perhaps it will crash or give answers that make no sense at all. In fact, the computational work behind the theorems of Section 8 uncovered several bugs (which have all been fixed). There are sometimes different implementations of the same algorithm or even different algorithms which implement the same theory. For example, the author used four different implementations of 2-descent to verify the computational claims of Theorem 8.1.

Throughout, E will denote an elliptic curve defined over $\mathbb{Q}$ of analytic rank zero or one. For such a curve, the Birch and Swinnerton-Dyer conjectural formula is known to hold up to a rational number, and Sections 2–4 explain this result in such a way as to make it explicit.

Sections 5 and 6 discuss what to do with the remaining primes and Sections 7 and 8 contain the proof of Theorem 1.2. Section 9 discusses the remaining cases, which all have reducible mod-p representations.

2. *Quadratic twists*

Below we will need to use several properties of the quadratic twist E^d of the elliptic curve E by a squarefree integer $d \notin \{0, 1\}$, so we establish these here. For any number field F, let G_F denote its absolute Galois group. Suppose that E is an elliptic curve over $\mathbb{Q}$ given in standardized ($a_1, a_3 \in \{0, 1\}$ and $a_2 \in \{-1, 0, 1\}$) global minimal Weierstrass form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The curve E^d can then be presented in the following Weierstrass form, which is not necessarily integral (and even when it is it may not be minimal):

$$E^d : y^2 + a_1xy + a_3y = x^3 + (a_2d + a_1^2(d-1)/4)x^2 + (a_4d^2 + a_1a_3(d^2-1)/2)x + a_6d^3 + a_3^2(d^3-1)/4.$$

Put $K = \mathbb{Q}(\theta)$, where $\theta^2 = 1/d$, and note that the curves are related by the K-isomorphism

$$\varphi : E \to E^d : \varphi(x, y) = \left(\theta^{-2}x, \theta^{-3}\left(y - \frac{a_1(\theta-1)}{2}x - \frac{a_3(\theta^3-1)}{2}\right)\right).$$

The L-series of E/K, $E/\mathbb{Q}$ and $E^d/\mathbb{Q}$ are related by the formula

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

Define as usual

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, & c_4 &= b_2^2 - 24b_4, \\ b_4 &= 2a_4 + a_1a_3, & c_6 &= b_2^3 + 36b_2b_4 - 216b_6, \\ b_6 &= a_3^3 + 4a_6, & \Delta &= (c_4^3 - c_6^2)/1728, \end{aligned}$$

noting that Δ is the minimal discriminant of E, hence $\omega = \mathrm{d}x/(2y + a_1x + a_3)$ is the minimal invariant differential of E. Let Δ' be the minimal discriminant of E^d, let $\mathrm{sig}(E) = (\mathrm{ord}_2(c_4), \mathrm{ord}_2(c_6), \mathrm{ord}_2(\Delta))$ and, for each prime p, let

$$\lambda_p = \min\{3\mathrm{ord}_p(c_4), 2\mathrm{ord}_p(c_6), \mathrm{ord}_p(\Delta)\}.$$

The following proposition is a correction of [**13**, Proposition 5.7.3].

PROPOSITION 2.1. *For each prime $p \mid 2d$, define δ_p as follows.*

(1) *If p is odd, then define $\delta_p = 1$ if either $\lambda_p < 6$ or $p = 3$ and $\mathrm{ord}_p(c_6) = 5$. Otherwise, define $\delta_p = -1$.*

(2) *If $d \equiv 1 \pmod 4$, then $\delta_2 = 0$.*

(3) *If $d \equiv 3 \pmod 4$, then*
- *$\delta_2 = 2$ if $\mathrm{sig}(E) = (0, 0, \cdot)$ or $(\cdot, 3, 0)$;*
- *$\delta_2 = -2$ if $\mathrm{sig}(E) = (4, 6, c)$ with $c \geqslant 12$ and $2^{-6}c_6d \equiv -1 \pmod 4$ or if $\mathrm{sig}(E) = (a, 9, 12)$ with $a \geqslant 8$ and $2^{-9}c_6d \equiv 1 \pmod 4$;*
- *$\delta_2 = 0$ otherwise.*

(4) *If $d \equiv 2 \pmod 4$, then*
- *$\delta_2 = 3$ if $\mathrm{sig}(E) = (0, 0, \cdot)$;*
- *$\delta_2 = -3$ if $\mathrm{sig}(E) = (6, 9, c)$ with $c \geqslant 18$ and $2^{-10}c_6d \equiv -1 \pmod 4$;*
- *$\delta_2 = 1$ if $\mathrm{ord}_2(c_4) \in \{4, 5\}$, or if $\mathrm{ord}_2(c_6) \in \{3, 5, 7\}$, or if $\mathrm{sig}(E) = (a, 6, 6)$ with $a \geqslant 6$ and $2^{-7}c_6d \equiv -1 \pmod 4$;*
- *$\delta_2 = -1$ otherwise.*

Then

$$\Delta' = \Delta\delta^6 \quad \textit{where } \delta = \delta(E,d) = \prod_{p|2d} p^{\delta_p}.$$

The original statement of the proposition in [13] does not include some of the congruence conditions when $d \equiv 3 \pmod 4$. This is simply a transcription omission from the correctly stated and more general Proposition 5.7.1.

The invariant differential ω_d associated to the given Weierstrass equation for E^d has pullback $\varphi^*\omega_d = \theta\omega$ by [49, p. 49], and it may not be minimal. In fact, if Δ_d is the discriminant of the above equation for E^d, then $\theta^{12}\Delta_d = \Delta$. Since $\Delta = \Delta'\delta^{-6}$, we have $(\delta/d)^6\Delta_d = \Delta'$. The transformation taking E^d to its minimal model must be defined over $\mathbb{Q}$, so $|\delta/d| \in \mathbb{Q}$ must be a square (or one can just read this off from the above proposition) and if ω' is the minimal invariant differential of E^d, then $\pm|\delta/d|^{-1/2}\omega_d = \omega'$. Finally, since $\varphi^*\omega' = \pm|\delta/d|^{-1/2}\theta\omega$, we find the relationship between the canonical period lattices of E and E^d:

$$\Lambda_d = |\delta/d|^{-1/2}\theta\Lambda.$$

Next we will consider the relationship between the Mordell–Weil and Shafarevich–Tate groups of the curve E and its twist E^d. Let σ denote the non-trivial element of $G = \mathrm{Gal}(K/\mathbb{Q})$. Define an action of G on $H^1(K,E)$ by setting $\xi^\sigma(\tau) = \xi(\sigma\tau\sigma^{-1})^\sigma$ for $\tau \in G_K$ and $\{\xi\}^\sigma = \{\xi^\sigma\}$. Let $E(K)^\pm$, $H^1(K,E)^\pm$ denote the ±1-eigenspaces of $E(K)$, $H^1(K,E)$, respectively. By the definition of E^d (see [49, X, Section 2]), we have that $\varphi^\sigma = [-1]\circ\varphi$. Then for $P \in E(K)$ we have

$$P^\sigma = \pm P \Rightarrow \varphi(P)^\sigma = \varphi^\sigma(P^\sigma) = \mp\varphi(P),$$

and for $\xi : G_K \to E$ representing a cocycle class $\{\xi\} \in H^1(K,E)$ we have

$$\{\xi^\sigma \pm \xi\} = 0 \Rightarrow \{(\varphi\circ\xi)^\sigma \mp \varphi\circ\xi\} = \{[-1]\circ\varphi\circ(\xi^\sigma \pm \xi)\} = 0,$$

which show that φ exchanges $E(K)^+$ with $E(K)^-$ and $H^1(K,E)^+$ with $H^1(K,E)^-$.

We now give the relationship between the Mordell–Weil groups $E(\mathbb{Q})$, $E^d(\mathbb{Q})$ and $E(K)$.

LEMMA 2.2. *We have $E(\mathbb{Q}) = E(K)^+$ and under φ^{-1} we may identify $E^d(\mathbb{Q}) = E(K)^-$. Under this identification, we have:*

(1) *the intersection is 2-torsion:*

$$E(\mathbb{Q}) \cap E^d(\mathbb{Q}) = E(\mathbb{Q})[2];$$

(2) *if $E(K)$ has rank r and $E(K)[2]$ has rank s, then*

$$[E(K)_{/\mathrm{tors}} : (E(\mathbb{Q}) + E^d(\mathbb{Q}))_{/\mathrm{tors}}] \leqslant 2^r$$

and

$$[E(K) : E(\mathbb{Q}) + E^d(\mathbb{Q})] \leqslant 2^{r+s};$$

(3) *if $E(K)$ has rank one, $E(\mathbb{Q})$ has rank zero and $E(\mathbb{Q})[2] = 0$, then*

$$E(K)_{/\mathrm{tors}} = E^d(\mathbb{Q})_{/\mathrm{tors}}.$$

Proof. The identifications are by definition and the above observations.

(1) Note that $P \in E(K)^+ \cap E(K)^-$ is equivalent to $P = P^\sigma = -P$ and hence to $P \in E(\mathbb{Q})[2]$.

(2) Let $P \in E(K)$ and note that

$$2P = (P + P^\sigma) + (P - P^\sigma) \in E(K)^+ + E(K)^-.$$

Therefore, since $2E(K) \subseteq E(K)^+ + E(K)^-$, we have that

$$[E(K)_{/\mathrm{tors}} : (E(K)^+ + E(K)^-)_{/\mathrm{tors}}] \leqslant [E(K)_{/\mathrm{tors}} : 2E(K)_{/\mathrm{tors}}] = 2^r$$

and

$$[E(K) : E(K)^+ + E(K)^-] \leqslant [E(K) : 2E(K)] = 2^{r+s}.$$

(3) Choose P such that $E(K) = \mathbb{Z}P \oplus E(K)_{\mathrm{tors}}$. We have that $T := P^\sigma + P \in E(K)^+$ must be torsion, so choose a, b so that the order of T is $2^b(2a+1)$. With $W = P + aT$, we have that

$$W^\sigma + W = P^\sigma + aT + (P + aT) = P^\sigma + P + 2aT = (2a+1)T$$

must be in $E(\mathbb{Q})(2)$, which is trivial since $E(\mathbb{Q})[2] = 0$. Thus, $W \in E(K)^-$ and, since $W \equiv P$ modulo torsion, we have $E(K)_{/\mathrm{tors}} = E(K)^-_{/\mathrm{tors}}$. □

LEMMA 2.3. *If $Ш(K, E)$ is finite, then for some integer t we have*

$$\#Ш(K, E) = \#Ш(\mathbb{Q}, E) \cdot \#Ш(\mathbb{Q}, E^d) \cdot 2^t.$$

Proof. Let v be a place of K and let $\mathbb{Q}_v$ be the completion of $\mathbb{Q}$ at v. The Hochschild–Serre spectral sequence [30] can be used to extend the inf–res sequence, which we fit into a commutative diagram.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^1(K/\mathbb{Q}, E(K)) & \xrightarrow{\inf} & H^1(\mathbb{Q}, E) & \xrightarrow{\mathrm{res}} & H^1(K, E)^+ & \longrightarrow & H^2(K/\mathbb{Q}, E(K)) \\
 & & & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & H^1(K_v/\mathbb{Q}_v, E(K_v)) & \xrightarrow{\inf} & H^1(\mathbb{Q}_v, E) & \xrightarrow{\mathrm{res}} & H^1(K_v, E)^+ & \longrightarrow & H^2(K_v/\mathbb{Q}_v, E(K_v))
\end{array}$$

If G is a finite group, then $H^i(G, \cdot)$ is killed by $\#G$ for all i. Therefore, the finite groups on the far left and right of the above diagram are all killed by 2.

Given a $\xi \in Ш(K, E)$, we have $2\xi = (\xi + \xi^\sigma) + (\xi - \xi^\sigma)$ and $\xi \pm \xi^\sigma \in H^1(K, E)^\pm$. Since $H^2(K/\mathbb{Q}, E(K))$ is killed by 2, there is a $\xi' \in H^1(\mathbb{Q}, E)$ with $\mathrm{res}(\xi') = 2(\xi + \xi^\sigma)$. Because $\xi + \xi^\sigma \in Ш(K, E)$, we know that $\mathrm{res}(\xi') \in H^1(K_v, E)^+$ is trivial for all v and, since $H^1(K_v/\mathbb{Q}_v, E(K_v))$ is killed by 2, we have $2\xi' = 0$ in $H^1(\mathbb{Q}_v, E)$ for all v, that is, we have $2\xi' \in Ш(\mathbb{Q}, E)$ and hence $4(\xi + \xi^\sigma) \in \mathrm{res}(Ш(\mathbb{Q}, E))$. Using φ to identify $H^1(K, E)^-$ with $H^1(K, E^d)^+$, we may show by a similar argument that $4(\xi - \xi^\sigma) \in \mathrm{res}(Ш(\mathbb{Q}, E^d))$. This shows that

$$8Ш(K, E) \subseteq \mathrm{res}(Ш(\mathbb{Q}, E)) + \mathrm{res}(Ш(\mathbb{Q}, E^d)) \subseteq Ш(K, E).$$

The claim then follows from the fact that the kernel of each restriction map is a finite 2-group. □

The following lemma is a generalization of a formula which appeared in [29, p. 312] without proof.

LEMMA 2.4. *Suppose $d < 0$ is a squarefree integer. Then with $\delta = \delta(E, d)$ as defined above, we have*

$$\Omega(E) \cdot \Omega(E^d) \cdot \delta^{1/2} = [E(\mathbb{R}) : E^0(\mathbb{R})] \cdot \|\omega\|^2.$$

Proof. Let x be the least positive real element of the period lattice Λ, and choose a fundamental domain for Λ with base $[0, x] \subset \mathbb{R}$ and upper left corner with positive imaginary part y and real part in $[0, x)$. Then $\Omega(E)/[E(\mathbb{R}) : E^0(\mathbb{R})] = x$ and $\|\omega\|^2 = 2xy$.

We compute

$$\delta^{1/2}\Omega(E^d) = \delta^{1/2}\int_{E^d(\mathbb{R})} |\omega'| = \int_{E(\mathbb{C})^-} \delta^{1/2}|\varphi^*\omega'| = \int_{E(\mathbb{C})^-} |\omega| = 2y.$$

The claim follows. □

3. *Complex multiplication*

Let E be an elliptic curve over $\mathbb{Q}$, let R denote the endomorphism ring $\mathrm{End}(E/\mathbb{C})$, let K denote its field of fractions and let $\mathrm{Aut}_R(E[p])$ denote the set of automorphisms of $E[p]$ commuting with the action of R. Consider the map $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$, which we call the mod-$p$ Galois representation.

If E does not have complex multiplication (CM), then $R = \mathbb{Z}$, $K = \mathbb{Q}$ and the groups $\mathrm{Aut}_R(E[p])$ and $\mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$ are identical. If E does have CM, then R is an order in the quadratic imaginary field K and we have $\overline{\rho}_{E,p}|_{G_K} : G_K \to \mathrm{Aut}_R(E[p]) \subsetneq \mathrm{Aut}(E[p])$. In either case, we will say that $\overline{\rho}_{E,p}$ is *surjective* if the image of G_K is $\mathrm{Aut}_R(E[p])$. Often in the literature one sees this defined as being 'as surjective as possible' in the CM case. In Section 7, we will give several examples of this.

Note that there is always an isogeny defined over $\mathbb{Q}$ from E to an elliptic curve E' with CM by a maximal order. E has CM by a non-maximal order if and only if its j-invariant is in the set $\{-12288000, 54000, 287496, 16581375\}$ [**50**, p. 483].

Suppose that E is an elliptic curve defined over K with CM by the ring of integers $\mathcal{O}_K$. The period lattice Λ of E is an $\mathcal{O}_K$-module and, since K has trivial class group, Λ is a free $\mathcal{O}_K$-module. Both are free $\mathbb{Z}$-modules of rank two, so let $\tau \in \mathbb{C}^\times$ be a generator of Λ, that is, $\tau\mathcal{O}_K = \Lambda$.

We have the following theorem of Rubin.

THEOREM 3.1. *With E, K, τ as above and $w = \#\mathcal{O}_K^\times$, we have:*

(1) *if $L(E/K, 1) \neq 0$, then $E(K)$ is finite, $Ш(K, E)$ is finite and there is a $u \in \mathcal{O}_K[w^{-1}]^\times$ such that*

$$L(E/K, 1) = \frac{\#Ш(K, E) \cdot \tau\overline{\tau}}{u \cdot (\#E(K))^2};$$

(2) *if $L(E/K, 1) = 0$, then either $E(K)$ is infinite or the $\mathfrak{p}$-part of $Ш(K, E)$ is infinite for all primes $\mathfrak{p} \nmid \#\mathcal{O}_K^\times$;*

(3) *if E is defined over $\mathbb{Q}$ and $r_{\mathrm{an}}(E/\mathbb{Q}) = 1$, then $\mathrm{BSD}(E/\mathbb{Q}, p)$ is true for all odd p which split in K.*

Proof. See [**45**]. □

COROLLARY 3.2. *If E is defined over $\mathbb{Q}$, has CM by K and $r_{\mathrm{an}}(E/\mathbb{Q}) = 0$, then $\mathrm{BSD}(E/\mathbb{Q}, p)$ is true for all $p \geqslant 5$. If $K \neq \mathbb{Q}(\sqrt{-3})$, then $\mathrm{BSD}(E/\mathbb{Q}, 3)$ is true.*

Proof. Let $K = \mathbb{Q}(\sqrt{d})$ for $d < 0$ a squarefree integer and without loss of generality suppose that E has CM by $\mathcal{O}_K$. Letting E^d be the model defined in Section 2 so that $\Lambda_d = \theta\Lambda$, note that since $[\theta^{-1}]$ is an endomorphism of E we have $\theta^{-1}\Lambda \subset \Lambda$, which implies $\Lambda \subset \Lambda_d$. Thus, E is isogenous to E^d, and this degree-$|d|$ isogeny is defined over $\mathbb{Q}$ since its kernel is $\theta\Lambda/\Lambda$ and $G_{\mathbb{Q}}$ acts by multiplying θ by ± 1. Thus, we have that

$$L(E/K, s) = L(E/\mathbb{Q}, s)^2.$$

Since $L(E/\mathbb{Q},1)\neq 0$, we have $L(E/K,1)\neq 0$, so $E(K)$ and $Ш(K,E)$ are finite. By Lemmas 2.2 and 2.3, we have that $E(\mathbb{Q})$ and $Ш(\mathbb{Q},E)$ are finite and

$$L(E/\mathbb{Q},1)^2=\frac{\#Ш(\mathbb{Q},E)\cdot\#Ш(\mathbb{Q},E^d)\cdot\tau\overline{\tau}}{(\#E(\mathbb{Q})\cdot\#E^d(\mathbb{Q}))^2}\cdot 2^t u^{-1},$$

where $t\in\mathbb{Z}$. Since E and E^d are isogenous over $\mathbb{Q}$, we have [10, Corollary 1.3]

$$\frac{\#Ш(\mathbb{Q},E^d)}{\#E^d(\mathbb{Q})^2}=\frac{\#Ш(\mathbb{Q},E)}{\#E(\mathbb{Q})^2}\cdot\frac{\Omega(E)}{\Omega(E^d)}\prod_p\frac{c_p(E)}{c_p(E^d)}.$$

By Lemma 2.4, we have

$$\frac{L(E/\mathbb{Q},1)^2}{\Omega(E)^2}=\frac{\#Ш(\mathbb{Q},E)^2}{\#E(\mathbb{Q})^4}\cdot\frac{\tau\overline{\tau}\delta^{1/2}}{\|\omega\|^2}\cdot\frac{2^t}{[E(\mathbb{R}):E^0(\mathbb{R})]\cdot u}\cdot\prod_p\frac{c_p(E)}{c_p(E^d)}.$$

Note that $\|\omega\|^2/2$ is the area of $\Lambda=\tau\mathcal{O}_K$, that is, $\tau\overline{\tau}$ times the area of $\mathcal{O}_K$. So, we have

$$\frac{\tau\overline{\tau}\delta^{1/2}}{\|\omega\|^2}=2^v\frac{\delta^{1/2}}{|d|^{1/2}},$$

where $v=1$ and $\delta\in\{|d|,1/|d|\}$ if $d\equiv 1 \pmod 4$; and $v=-1$ and $\delta/|d|\in\{4,1,1/4,1/16\}$ otherwise.

In summary, we have that

$$\frac{L(E/\mathbb{Q},1)^2}{\Omega(E)^2}=\left(\frac{\#Ш(\mathbb{Q},E)}{\#E(\mathbb{Q})^2}\right)^2\cdot\left(\frac{2^{v+t}\delta^{1/2}}{[E(\mathbb{R}):E^0(\mathbb{R})]\cdot|d|^{1/2}}\right)\cdot\left(\frac{1}{u}\prod_p\frac{c_p(E)}{c_p(E^d)}\right).$$

Since $L(E/\mathbb{Q},1)/\Omega(E)$ is a rational number, we have $\delta^{1/2}/(|d|^{1/2}u)\in\mathbb{Q}$. But, since $\delta>0$ and $u\in K$, we must have $u\in\mathbb{Q}$ and hence $\delta^{1/2}/|d|^{1/2}\in\mathbb{Q}$. As noted in [50, p. 176], since E has CM, it must be of additive reduction at all the bad primes. For each prime p, by [49, Corollary 15.2.1, p. 359], the Tamagawa numbers $c_p(E)$ and $c_p(E^d)$ are at most 4.

Let p be a prime and suppose $p\geqslant 5$. Since neither the Tamagawa numbers nor the error term u are divisible by p, we will show that $\mathrm{ord}_p(\delta^{1/2}/|d|^{1/2})=0$. If $d\not\equiv 1 \pmod 4$, then this is true as observed above, so suppose $d\equiv 1 \pmod 4$. Since d is divisible by exactly one prime and δ is divisible by at most two and that prime, we may assume $p=|d|$. Since $p\geqslant 5$, the quantity $\mathrm{ord}_p(\delta^{1/2}/|d|^{1/2})$ must be even and hence $\delta=|d|$. Since p does not divide any Tamagawa number, the first claim is proved.

Now suppose $p=3$ and $d\neq -3$, hence $\mathrm{ord}_3(u)=0$. If $d>-3$, then from the above we have $\mathrm{ord}_3(\delta^{1/2}/|d|^{1/2})=0$, so further suppose $d<-3$; in particular, we have $d\equiv 1 \pmod 4$ and $\delta^{1/2}/|d|^{1/2}\in\{1,|d|^{-1}\}$. Since the prime $|d|$ is not 3, we must have $\mathrm{ord}_3(\delta^{1/2}/|d|^{1/2})=0$. It only remains to show that when $d\neq -3$, no Tamagawa number $c_q(E)$ is divisible by 3. This can be done as follows.

E is isomorphic to one of the ten curves in the table on [50, p. 483] which do not have CM discriminant -3. Call this representative curve F and note that E is a twist of F by a character whose order divides 4. Since 3 does not divide the discriminant of F, we have $4\cdot\mathrm{ord}_3(\Delta(E))\equiv 0 \pmod{12}$. By [50, Table 4.1, p. 365], if $q\neq 3$, then Kodaira types IV and IV* cannot occur at q since in those cases $\mathrm{ord}_q(\Delta(E))\in\{4,8\}$ and therefore $c_q(E)$ is not divisible by 3. For $q=3$, one may write down an explicit equation for E as a twist of one such F and run Tate's algorithm [50, IV.9.4] over $\mathbb{Q}_3$. For example, suppose $j(E)=1728$ and hence F is the curve $y^2=x^3+x$, noting that this is the only case in which the twisting character could be of order four.

If the order is four, then E is given by $y^2=x^3+Dx$ for some $D\in\mathbb{Q}^*$. Since we are assuming that E is in minimal integral form, we have that $D\in\mathbb{Z}$. We have that $b_2=b_6=0$, $b_4=2D$, $b_8=-D^2$ and $\Delta=-2^6\cdot D^3$. Tate's algorithm shows that if $\mathrm{ord}_3(D)=0$, the Kodaira symbol

is I_0, if $\mathrm{ord}_3(D)=1$ it is III, if $\mathrm{ord}_3(D)=2$ it is I_0^*, if $\mathrm{ord}_3(D)=3$ it is III^* and if $\mathrm{ord}_3(D)\geqslant 4$ then the model of E is not minimal. If the order is two, then either E is the exceptional quadratic twist $y^2=x^3-4x$, whose Kodaira symbol at $q=3$ is I_0, or E is given by $y^2=x^3+D^2x$ for some non-zero $D\in\mathbb{Z}$. So, $b_2=b_6=0$, $b_4=2D^2$ and $b_8=-D^4$. If $\mathrm{ord}_3(D)=0$, then the Kodaira symbol is I_0, if $\mathrm{ord}_3(D)=1$ then it is I_0^* and if $\mathrm{ord}_3(D)\geqslant 2$ then the given model of E is not minimal.

The other nine cases proceed similarly, in each case ruling out the possibility of Kodaira types IV and IV^* at $q=3$. Therefore, $3\nmid c_q(E)$ for all primes q and hence the second claim is proved. □

LEMMA 3.3. *With E and K as above, let $\mathfrak{p}$ be a prime of K of good reduction for E which does not divide $\#\mathcal{O}_K^\times$. Then $K(E[\mathfrak{p}])/K$ is a cyclic extension of degree $\mathrm{Norm}(\mathfrak{p})-1$ in which $\mathfrak{p}$ is totally ramified.*

Proof. See [44, Lemma 21(i)]. □

LEMMA 3.4. *With E and K as above, we have $\mathrm{Aut}_{\mathcal{O}_K}(E[p])\cong(\mathcal{O}_K/p\mathcal{O}_K)^\times$ for all primes p.*

Proof. $E[p]$ is a free $\mathcal{O}_K/p\mathcal{O}_K$-module of rank one [50, II.1.4(b)]. □

PROPOSITION 3.5. *If p is a prime of good reduction for E not dividing $\#\mathcal{O}_K^\times$ which is inert in K, then $\overline{\rho}_{E,p}$ is surjective.*

Proof. When p is inert in K, $\mathrm{Norm}(\mathfrak{p})=p^2$. By Lemma 3.3, we find that the order of the Galois group is $\#\mathrm{Gal}(K(E[p])/K)=p^2-1$. Since $\overline{\rho}_{E,p}:\mathrm{Gal}(K(E[p])/K)\to\mathrm{Aut}_{\mathcal{O}_K}(E[p])$ is injective, it suffices to show that $\#\mathrm{Aut}_{\mathcal{O}_K}(E[p])=p^2-1$. Since $\dim_{\mathbb{Z}}(\mathcal{O}_K)=2$, we have that $\#(\mathcal{O}_K/p\mathcal{O}_K)^\times=p^2-1$, which by Lemma 3.4 is equal to $\#\mathrm{Aut}_{\mathcal{O}_K}(E[p])$. □

4. *Heegner points*

If E is an elliptic curve over $\mathbb{Q}$ of conductor N and $D<0$ is a squarefree integer, we say that the quadratic imaginary field $K=\mathbb{Q}(\sqrt{D})$ satisfies the Heegner hypothesis for E if each prime $p\mid N$ splits in K. If K satisfies the Heegner hypothesis for E, then the Heegner point $y_K\in E(K)$ is defined as follows (see [28] for details). By hypothesis, there is an ideal $\mathcal{N}$ of $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N}$ is cyclic of order N. Since $\mathcal{O}_K\subset\mathcal{N}^{-1}$, we have a cyclic N-isogeny $\mathbb{C}/\mathcal{O}_K\to\mathbb{C}/\mathcal{N}^{-1}$ of elliptic curves with CM by $\mathcal{O}_K$ and hence a point $x_1\in X_0(N)$. By the theory of CM, x_1 is defined over the Hilbert class field H of K. We fix a modular parametrization $\psi:X_0(N)\to E$ of minimal degree taking ∞ to $\mathcal{O}$, which exists by [6, 59]. As above, denote the minimal invariant differential on E by ω. Then $\psi^*(\omega)$ is the differential associated to a newform on $X_0(N)$. We have $\psi^*(\omega)=\alpha\cdot f$, where f is a normalized cusp form and α is some non-zero integer [21] constant. The Manin constant is $c:=|\alpha|$ and the Heegner point is $y_K:=\mathrm{Tr}_{H/K}(\psi(x_1))\in E(K)$. It has been conjectured that $c=1$ if E is optimal, and this has been verified for $N<130000$ by Cremona [1]. Define $I_K:=[E(K)_{/\mathrm{tors}}:\mathbb{Z}y_K]$, which we call the Heegner index. Note that sometimes we may denote the Heegner index by I_D to emphasize the dependence $K=\mathbb{Q}(\sqrt{D})$.

Gross, Zagier and Zhang have proved a deep theorem which expresses the first derivative of the L-series of E/K at 1 in terms of the canonical height $\hat{h}$ of the Heegner point y_K.

THEOREM 4.1 (Gross–Zagier–Zhang). *If K satisfies the Heegner hypothesis for E, then*

$$L'(E/K,1)=\frac{2\|\omega\|^2\hat{h}(y_K)}{c^2\cdot u_K^2\cdot\sqrt{|\Delta(K)|}},$$

where $\|\omega\|^2 = \int_{E(\mathbb{C})} \omega \wedge \overline{i\omega}$ *and the quadratic imaginary number field* K *has* $2u_K$ *roots of unity and discriminant* $\Delta(K)$.

Proof. Gross and Zagier first proved this in [29] when D is odd and Zhang generalized it in [62]. □

Note that $u_{\mathbb{Q}(\sqrt{-1})} = 2$, $u_{\mathbb{Q}(\sqrt{-3})} = 3$ and, for all other quadratic imaginary fields K, we have $u_K = 1$. Often, one requires that $D \notin \{-1, -3\}$ but, since there are infinitely many D satisfying the Heegner hypothesis for E if $r_{\mathrm{an}}(E) \leqslant 1$, this is a minor issue (see the proof of Theorem 4.4). Note also that the $\hat{h}$ appearing in the formula as stated here is the absolute height, whereas the one appearing in [29, Theorem 2.1, p. 311] is equal to our $2\hat{h}$. Recall that the Néron–Tate canonical (absolute) height is defined for $P \in E(K)$ by

$$\hat{h}(P) = \frac{1}{2[K:\mathbb{Q}]} \lim_{n\to\infty} 4^{-n} \log(H_K(x(2^N P))),$$

where $H_K(x) = \prod_v |x|_v^{[K_v:\mathbb{Q}_v]}$ with the product running over the places v of K.

We have the following theorem of Kolyvagin.

THEOREM 4.2. *If* y_K *is non-torsion, then* $E(K)$ *has rank one (hence* $I_K < \infty$*),* Ш(K, E) *is finite and*

$$\#Ш(K, E) | c_4 I_K^2,$$

where c_4 *is a positive integer (explicitly defined in* [34]*) such that every odd prime* p *dividing* c_4 *is such that* $\overline{\rho}_{E,p}$ *is not surjective.*

Proof. This is [34, Theorem A]. □

COROLLARY 4.3. *If* y_K *is non-torsion, then* Ш$(\mathbb{Q}, E)$ *and* Ш$(\mathbb{Q}, E^D)$ *are finite and have orders whose odd parts divide* $c_4 I_K^2$.

Proof. By Lemma 2.3, we have that $\#Ш(\mathbb{Q}, E) \cdot \#Ш(\mathbb{Q}, E^D)$ divides $\#Ш(K, E)$ up to a power of two. □

THEOREM 4.4. *If* $r_{\mathrm{an}}(E) \leqslant 1$*, then there exists a quadratic field* K *satisfying the Heegner hypothesis such that* y_K *is non-torsion. In particular,*

$$r(E) = r_{\mathrm{an}}(E),$$

Ш$(\mathbb{Q}, E)$ *is finite and, if* p *is an odd prime unramified in the CM field such that* $\overline{\rho}_{E,p}$ *is surjective, then*

$$\mathrm{ord}_p(\#Ш(\mathbb{Q}, E)) \leqslant 2 \cdot \mathrm{ord}_p(I_K).$$

Note that the if E does not have CM, then by the CM field we mean $\mathbb{Q}$.

Proof. We follow the proof given in [20]. If $\varepsilon = -1$ (that is, $r_{\mathrm{an}}(E) = 1$), then a result of Waldspurger (see [57]) implies that there are infinitely many $D < 0$ such that $K = \mathbb{Q}(\sqrt{D})$ satisfies the Heegner hypothesis for E and $r_{\mathrm{an}}(E^D) = 0$. If $\varepsilon = 1$ (that is, $r_{\mathrm{an}}(E) = 0$), then results of Bump, Friedberg and Hoffstein (see [8]) or independently results of Murty and Murty (see [41]) imply that there are infinitely many $D < 0$ such that $K = \mathbb{Q}(\sqrt{D})$ satisfies the Heegner hypothesis for E and $r_{\mathrm{an}}(E^D) = 1$.

We have that

$$\mathrm{ord}_{s=1} L(E/K, s) = \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) + \mathrm{ord}_{s=1} L(E^D/\mathbb{Q}, s),$$

which implies that in either case $r_{\mathrm{an}}(E/K) = 1$, which, by the Gross–Zagier–Zhang formula (Theorem 4.1), implies that y_K is non-torsion. Then Kolyvagin's Theorem 4.2 implies that $E(K)$ has rank one, that $I_K < \infty$ and that Ш(K, E) is finite.

By Lemma 2.2, we have

$$\mathrm{rank}(E(K)) = \mathrm{rank}(E(\mathbb{Q})) + \mathrm{rank}(E^D(\mathbb{Q})).$$

By [**20**, Proposition 3.11], the point y_K belongs to $E(\mathbb{Q})$ (up to torsion) if and only if $\varepsilon = -1$. It follows that the rank of $E(\mathbb{Q})$ is equal to $r_{\mathrm{an}}(E/\mathbb{Q})$. □

The following collects previous results in a way to make them more computationally explicit.

COROLLARY 4.5. *Suppose that E has CM by the full ring of integers $\mathcal{O}_K$.*

(1) *If $r_{\mathrm{an}}(E) = 0$, then* BSD$(E/\mathbb{Q}, p)$ *is true for $p \nmid \#\mathcal{O}_K^\times$.*

(2) *If $r_{\mathrm{an}}(E) = 1$, then:*

   (a) *if $p \geqslant 3$ is split, then* BSD$(E/\mathbb{Q}, p)$ *is true;*

   (b) *if $p \geqslant 5$ is inert and p is a prime of good reduction for E, then*

$$\mathrm{ord}_p(\#Ш(\mathbb{Q}, E)) \leqslant 2 \cdot \mathrm{ord}_p(I),$$

   where $I = I_{\mathbb{Q}(\sqrt{D})}$ is any Heegner index for $D < -4$ satisfying the Heegner hypothesis.

Proof. Part (1) is Corollary 3.2. Part (2a) is part (3) of Theorem 3.1. Part (2b) is obtained from Proposition 3.5 by Theorem 4.4. □

We now describe an algorithm for computing the Mordell–Weil and Shafarevich–Tate groups when the analytic rank of $E/\mathbb{Q}$ is bounded above by one. In the next section, we will make this more explicit, with the aim of developing a practical procedure for verifying the Birch and Swinnerton-Dyer conjecture for a specific elliptic curve.

LEMMA 4.6. *If $B > 0$ is such that $S = \{P \in E(\mathbb{Q}) : \hat{h}(P) \leqslant B\}$ contains a set of generators for $E(\mathbb{Q})/2E(\mathbb{Q})$, then S generates $E(\mathbb{Q})$.*

Proof. See [**14**, § 3.5]. □

THEOREM 4.7. *If $r_{\mathrm{an}}(E/\mathbb{Q}) \leqslant 1$, then there are algorithms to compute both the Mordell–Weil group $E(\mathbb{Q})$ and the Shafarevich–Tate group* Ш$(\mathbb{Q}, E)$.

Proof. In general, 2-descent is not known to terminate, but in this case $r = r_{\mathrm{an}}(E)$ is known. Therefore, 2-descent will determine $E(\mathbb{Q})/2E(\mathbb{Q})$. Then we can search for points up to the maximum height of points in $E(\mathbb{Q})/2E(\mathbb{Q})$ and by Lemma 4.6 we will find a set of generators for $E(\mathbb{Q})$. (Note that point searching suffices to prove the existence of an algorithm, since the condition $r = r_{\mathrm{an}}(E)$ gives a termination condition for the search. We mention 2-descent here because it is much more effective in practice, especially for finding points of large height.)

To compute Ш$(\mathbb{Q}, E)$, note that Kolyvagin's Theorem 4.4 gives an explicit upper bound B for $\#Ш(\mathbb{Q}, E)$. For primes p dividing this upper bound, we can (in theory at least) perform successive p^k-descents for $k = 1, 2, 3, \ldots$ to compute Ш$(\mathbb{Q}, E)[p^k]$. As soon as Ш$(\mathbb{Q}, E)[p^k] =$ Ш$(\mathbb{Q}, E)[p^{k+1}]$, we have Ш$(\mathbb{Q}, E)[p^k] =$ Ш$(\mathbb{Q}, E)[p^\infty]$ and can move on to the next prime. Once we do this for each prime, we have Ш$(\mathbb{Q}, E) = \bigoplus_{p|B}$ Ш$(\mathbb{Q}, E)[p^\infty]$. □

For $r_{\mathrm{an}}(E) \leqslant 1$, we can (at least in theory) compute $\#Ш(\mathbb{Q}, E)_{\mathrm{an}}$ exactly, as first described in [29, p. 312]. Together with the previous theorem, this shows that the BSD formula for E can be proved for specific elliptic curves via computation.

The main ingredient in applying Kolyvagin's work to a specific elliptic curve E of analytic rank at most one is to compute the Heegner index $I_K = [E(K)_{/\mathrm{tors}} : \mathbb{Z}\overline{y_K}]$, where $K = \mathbb{Q}(\sqrt{D})$ satisfies the Heegner hypothesis for E and $y_K \in E(K)$ is a Heegner point (and $\overline{y_K}$ is its image in $E(K)_{/\mathrm{tors}}$). Let $z \in E(K)$ generate $E(K)_{/\mathrm{tors}}$.

We can provably compute $\hat{h}(y_K)$ to desired precision using the Gross–Zagier–Zhang formula (Theorem 4.1), reducing the index calculation to the computation of the height of z, since

$$I_K^2 = \frac{\hat{h}(y_K)}{\hat{h}(z)}.$$

We have the following corollary of Lemma 2.2.

Corollary 4.8. *Suppose that E is an elliptic curve of analytic rank zero or one over $\mathbb{Q}$, in particular $\mathrm{rank}(E(\mathbb{Q})) = r_{\mathrm{an}}(E(\mathbb{Q}))$. Let $D < 0$ be a squarefree integer such that $K = \mathbb{Q}(\sqrt{D})$ satisfies the Heegner hypothesis for E.*

(1) *If we have $r_{\mathrm{an}}(F(\mathbb{Q})) = 1$, where F is one of E or E^D, and if $x \in F(\mathbb{Q})$ generates $F(\mathbb{Q})_{/\mathrm{tors}}$, then*

$$I_K = \begin{cases} \sqrt{\dfrac{\hat{h}(y_K)}{\hat{h}(x)}}, & \dfrac{1}{2}x \notin F(K), \\ 2\sqrt{\dfrac{\hat{h}(y_K)}{\hat{h}(x)}}, & \dfrac{1}{2}x \in F(K). \end{cases}$$

(2) *Suppose $r_{\mathrm{an}}(E(\mathbb{Q})) = 0$. If $E(\mathbb{Q})[2] = 0$, then let $A = 1$, otherwise let $A = 4$. Let $C = C(E^D/\mathbb{Q})$ denote the Cremona–Prickett–Siksek height bound [18]. If there are no non-torsion points P on $E^D(\mathbb{Q})$ with naive absolute height*

$$h(P) \leqslant \frac{A \cdot \hat{h}(y_K)}{M^2} + C,$$

then

$$I_K < M.$$

Note that this is a correction to the results stated in [27]. However, for each case in which [27] uses this result, the corresponding A is equal to 1. Therefore, this mistake does not impact any of the other results there.

If $\mathrm{rank}(E(\mathbb{Q})) = 1$, then we will have a generator x from the rank verification, and we can simply check whether $\frac{1}{2}x$ is in $E(K)$ and use part 1 of the corollary. If $\mathrm{rank}(E(\mathbb{Q})) = 0$, then we may not so easily find a generator of the twist, because a point search may very well fail since the conductor of E^D is D^2N. However, a failed point search can still be useful as long as we search sufficiently hard, because of part 2 of the corollary.

It is also worthwhile to point out that in each case where we use the computation of $\hat{h}(y_K)$ to prove bounds on I_K or to compute I_K exactly, we must compute $\hat{h}(y_K)$ to sufficient precision. One can either compute the Heegner point algebraically and then compute its height directly, or one can compute its height via the Gross–Zagier formula. Any time such a computation was used in a proof, it was done with sufficient precision to prove the resulting conclusion on I_K.

5. *Bounding the order of* $Ш(\mathbb{Q}, E)$

Suppose $r_{\mathrm{an}}(E) \leqslant 1$ for $E/\mathbb{Q}$ and that K is a quadratic imaginary field satisfying the Heegner hypothesis for E. We have already seen that for analytic rank-zero curves, $\mathrm{BSD}(E, p)$ is true for primes $p > 3$ if E has CM. Otherwise, we have the following theorem.

THEOREM 5.1. *Suppose that E is an optimal non-CM curve, and let p be a prime such that $p \nmid 6N$ and $\rho_{E,p}$ is surjective. If $r_{\mathrm{an}}(E) = 0$, then $Ш(\mathbb{Q}, E)$ is finite and*

$$\mathrm{ord}_p(\#Ш(\mathbb{Q}, E)) \leqslant \mathrm{ord}_p\left(\frac{L(E/\mathbb{Q}, 1)}{\Omega(E)}\right).$$

Proof. As outlined in [**27**, § 4], this is due to Kato's Euler system [**33**] together with a result of Matsuno [**36**]. □

As a corollary to this theorem, $\mathrm{BSD}(E, p)$ is true for primes $p > 3$ of good reduction, where $\overline{\rho}_{E,p}$ is surjective and p does not divide $\#Ш(\mathbb{Q}, E)_{\mathrm{an}}$. Under certain technical conditions on p (explained in [**26**]), Grigorov has proved the bound on the other side. In addition, recent work of Skinner and Urban [**51**] showed that if $r_{\mathrm{an}}(E) = 0$, E has good ordinary reduction at p, $\overline{\rho}_{E,p}$ is surjective and there is a prime $q \neq p$ such that $q||N$ and $\overline{\rho}_{E,p}$ is ramified at q, then

$$\mathrm{ord}_p(\#Ш(\mathbb{Q}, E)) = \mathrm{ord}_p\left(\frac{L(E/\mathbb{Q}, 1)}{\Omega(E) \cdot \prod_q c_q(E)}\right).$$

Because Theorem 5.1 often eliminates most of the primes $p > 3$, one often does not need to compute the Heegner index for rank-zero curves. However, if there is a bad prime $p > 3$ such that $\overline{\rho}_{E,p}$ is not surjective, then Theorem 5.1 does not apply and descents are in general not feasible. For example, this happens with the pair $(E, p) = (2900\mathrm{d}1, 5)$. Interestingly, $\#Ш(\mathbb{Q}, E) = 25$ in this case (this will be proved in Section 8). Theorem 4.4 still gives an upper bound, provided we have some kind of bound on the Heegner index. In the example above, the methods of Section 4 show that $I_K \leqslant 23$, implying $\mathrm{ord}_5(I_K) \leqslant 1$ and hence $\mathrm{ord}_5(\#Ш(\mathbb{Q}, E)) \leqslant 2$.

The following theorems give alternate hypotheses under which Kolyvagin's machinery still gives the same result. These should be viewed as extensions of Theorem 4.4.

THEOREM 5.2. *If $r_{\mathrm{an}}(E/\mathbb{Q}) \leqslant 1$ and p is a prime such that $p \nmid 2 \cdot \Delta(K)$, $p^2 \nmid N$ and $\overline{\rho}_{E,p}$ is irreducible, then*

$$\mathrm{ord}_p(\#Ш(\mathbb{Q}, E)) \leqslant 2 \cdot \mathrm{ord}_p(I_K).$$

Proof. See [**11**, **12**]. □

THEOREM 5.3. *Suppose $r_{\mathrm{an}}(E/\mathbb{Q}) \leqslant 1$ and that p is an odd prime which does not divide $\#E'(\mathbb{Q})_{\mathrm{tors}}$ for any E' which is $\mathbb{Q}$-isogenous to E. If $\Delta(K)$ is divisible by exactly one prime, further suppose $p \nmid \Delta(K)$. Then*

$$\mathrm{ord}_p(\#Ш(\mathbb{Q}, E)) \leqslant 2 \cdot \mathrm{ord}_p(I_K).$$

Proof. See [**27**, Theorem 3.5]. Note that the statement of this theorem in [**27**] includes the hypothesis that E does not have CM, but the proof never uses it. □

Jetchev [**31**] has improved the upper bound with the following theorem.

THEOREM 5.4 (Jetchev). *If the hypotheses of any of Theorems 4.4, 5.2 or 5.3 apply to p, then*

$$\operatorname{ord}_p(\#Ш(\mathbb{Q}, E)) \leqslant 2 \cdot \left(\operatorname{ord}_p(I_K) - \max_{q|N} \operatorname{ord}_p(c_q) \right).$$

If p divides at most one Tamagawa number, then this upper bound is equal to $\operatorname{ord}_p(\#Ш(\mathbb{Q}, E)_{\mathrm{an}})$.

There is also a relevant algorithm of Stein and Wuthrich based on the work of Kato, Perrin-Riou and Schneider (a preprint is available at [54] and the algorithm is implemented in Sage [55]). Suppose that the elliptic curve E and the prime $p \neq 2$ are such that E does not have additive reduction at p and $\overline{\rho}_{E,p}$ is either surjective or reducible. These conditions hold for all but finitely many p if E does not have CM. Given a pair (E, p) satisfying this hypothesis, the algorithm either gives an upper bound for $\#Ш(\mathbb{Q}, E)[p^\infty]$ or terminates with an error. In the case that $r_{\mathrm{an}}(E) \leqslant 1$, an error only happens when the p-adic height pairing cannot be shown to be non-degenerate. For curves of conductor up to 5000 and of rank zero or one, this never happens for those p considered. Note that it is a standard conjecture that the p-adic height pairing is non-degenerate and, if this is true for a particular case, it can be shown via a computation.

There are also techniques for bounding the order of $Ш(\mathbb{Q}, E)$ from below. In [17], Cremona and Mazur established a method for visualizing pieces of $Ш(\mathbb{Q}, E)$ as pieces of Mordell–Weil groups via modular congruences, which is fully explained in the appendix of [2]. They have also carried out computations for curves of conductor up to 5500, which are listed in [17]. In addition, Stein established a method for doing this for abelian varieties as part of his PhD thesis [53].

6. *Descent*

Cremona's program `mwrank` is one of various implementations of 2-descents on elliptic curves, and consists of Birch and Swinnerton-Dyer's original algorithm [4] together with a range of improvements spanning years in the literature. This is frequently called the 'principal homogeneous space' method, since it essentially involves a search for principal homogeneous spaces which represent elements of the 2-Selmer group. These are hyperelliptic curves defined by $y^2 = f(x)$, where f is a quartic. As such, these curves are called quartic covers of the elliptic curve. It is very well described in [14], as long as one is also aware of the various improvements and clarifications: [16] works out computing equivalences of the involved quartics, [19] completes the classification of minimal models begun in [4] at $p = 2$ and even this was further refined in certain cases in [47, 48] includes an asymptotic improvement over [4] in determining local solubility. Further, the situation regarding what `mwrank` does in higher descents (extensions of ϕ-descents to 2-descents when ϕ is an isogeny of degree two) is documented mostly in slides entitled 'Higher Descents on Elliptic Curves' on Cremona's website[†], as well as some unpublished notes he was kind enough to share. There is also Denis Simon's `gp` [3] script, which computes the same information as `mwrank`, but via what is called the 'number field method'. Both of these programs are available in Sage [55].

The various descent methods in Magma [9] were written by Geoff Bailey, John Cremona, Steve Donnelly, Michael Stoll, Mark Watkins, Tom Womack and others. Magma's 4-descent routines are based on [38, 60], and here the homogeneous spaces each come from the intersection of two quadric surfaces in $\mathbb{P}^3$. The 8-descent routines are based on [52], and the homogeneous spaces are intersections of three quartics. Tom Fisher has written 6-descent methods which are due to appear in a future Magma release, based on [23].

[†]See http://www.warwick.ac.uk/staff/J.E.Cremona/papers item 26.

Jeechul Woo, a 2010 PhD student of Noam Elkies, has implemented a gp script for doing 3-isogeny descents when the curve has a rational 3-torsion point, based on [61]. Magma's 3-descent implementation is due mainly to J. Cremona and M. Stoll.

Where explicit computer calculations of descents were used in the proofs below, each available implementation, as mentioned above, was used to verify the results. The computations were done on machines funded by the US National Science Foundation grant number DMS-0821725.

7. *Examples*

The following examples are not only useful in illustrating the preceding discussion, but will also be needed to prove the main results of this note. We begin by proving that several mod-p Galois representations are surjective, where the elliptic curve has CM. This will allow us to use Theorem 4.4 for these curve–prime pairs in Section 8.

EXAMPLE 7.1. Each of the curves in Table 1 has CM by K, in which p is inert. By Lemma 3.4, we can think of the representation as a map $\overline{\rho} : G_K \to (\mathcal{O}_K/p\mathcal{O}_K)^\times \cong \mathbb{F}_{p^2}^\times$. If $\ell \neq p$ is a prime of good reduction, then $N(\overline{\rho}(\sigma_\ell)) = \ell$ and $\mathrm{Tr}(\overline{\rho}(\sigma_\ell)) = a_\ell$, where the norm and trace maps are from $\mathbb{F}_{p^2}$ to $\mathbb{F}_p$ and σ_ℓ is a Frobenius element at ℓ. Since in dimension two the norm and trace determine the characteristic polynomial, it suffices to show that there is an ℓ for which these agree with the norm and trace of a generator of $\mathbb{F}_{p^2}^\times$. In Table 1, we give a witnessing ℓ and the corresponding a_ℓ.

If K is an étale algebra over $\mathbb{Q}$, then K decomposes uniquely into a direct product of number fields $K \cong \prod_i K_i$. If S is a set of places of $\mathbb{Q}$, Schaefer and Stoll [46] defined $K(S, p)$ to be the elements $\alpha \in K^\times/(K^\times)^p$ such that all the extensions $K_i(\sqrt[p]{\alpha})/K_i$ are unramified at all primes of K_i lying above a finite place outside of S. In [46], they described a way of computing the p-Selmer group of an elliptic curve. If $S = \{p\} \cup \{\ell : p | c_\ell\}$, then $\mathrm{Sel}^{(p)}(\mathbb{Q}, E)$ corresponds to the subgroup of elements of $H^1(\mathbb{Q}, E; S)$ whose localizations are in the image of the local connecting homomorphisms for each place in S. In practice, one computes the S-Selmer group $K(S, p)$ of the étale algebra K corresponding to a Galois-invariant spanning subset of $E[p]\backslash\{\mathcal{O}\}$ in terms of the class group and S-units. Here we give two useful examples of this technique, which proves that the 5-primary part of $Ш(\mathbb{Q}, E)$ is trivial.

TABLE 1. *Surjective mod-p representations for CM curves.*

Cremona label	E	p	ℓ	a_ℓ
675a1	$y^2 + y = x^3 + 31$	5	7	1
900c1	$y^2 = x^3 + 100$	5	7	−1
1568g1	$y^2 = x^3 - 49x$	7	5	2
2700h1	$y^2 = x^3 + 625$	5	7	−1
2700l1	$y^2 = x^3 + 5$	5	7	1
2700p1	$y^2 = x^3 + 500$	5	13	7
3600bd1	$y^2 = x^3 - 100$	5	7	1
3136t1	$y^2 = x^3 + 49x$	7	5	−2
3136u1	$y^2 = x^3 - 343x$	7	5	4
3136v1	$y^2 = x^3 - 7x$	7	5	−4
3267d1	$y^2 + y = x^3 - 333$	11	7	1
3872a1	$y^2 = x^3 + 1331x$	11	13	4
4356a1	$y^2 = x^3 - 44$	11	7	1
4356b1	$y^2 = x^3 + 58564$	11	7	−1
4356c1	$y^2 = x^3 - 1331$	11	7	4

EXAMPLE 7.2. Let $p = 5$. Usually, 5-descents are infeasible due to the number fields involved; for example, if the mod-5 representation is surjective, the étale algebra will be a single number field of degree 24, for which class group and S-unit calculations will be too difficult to complete without assuming the generalized Riemann hypothesis (GRH). However, the following two examples illustrate cases in which a 5-descent is actually possible without assuming the GRH. Here the 5-division polynomial has a factor of degree four which corresponds to a Galois invariant spanning subset X of $E[p]\backslash\{\mathcal{O}\}$ of size 8. In each case $g(y)$ is the resultant of this factor and the defining polynomial of E, which defines a number field A_1.

(1) Let $E = 225a1$. Then we have

$$g(y) = y^8 + 4y^7 + 97y^6 + 277y^5 - 80y^4 - 617y^3 - 548y^2 - 194y + 331.$$

(2) Let $E = 3600be$. Then we have

$$g(y) = y^8 - 720000y^6 - 27000000000y^4 + 1458000000000000000.$$

In both cases the set S is of order one, consisting of the primes above 5, and the dimension of $A_1(S,p)$ is 6. Computations show that the dimension of $A_1(S,p)^{(1)} = \ker(\sigma_g - g)$ (the notation again comes from [46]) is at most two in both cases. Since the Selmer group $\mathrm{Sel}^{(5)}(\mathbb{Q},E)$ is contained in $A_1(S,p)^{(1)}$, it has dimension at most two. Since the dimension of $E(\mathbb{Q})/5E(\mathbb{Q})$ is exactly one, we have that in these two cases $\#Ш(\mathbb{Q},E)[5] \leqslant 5$ and hence that $\#Ш(\mathbb{Q},E)[5] = 1$.

8. *Curves of conductor $N < 5000$, irreducible mod-p representations*

There are 17314 isogeny classes of elliptic curves of conductor up to 5000. There are 7914 of rank zero, 8811 of rank one, 589 of rank two and none of higher rank. There are only 116 optimal curves which have CM in this conductor range. Every rank-two curve in this range has $\#Ш(\mathbb{Q},E)_{\mathrm{an}} \approx 1.000000$. For any curve E with $r_{\mathrm{an}}(E) \leqslant 1$ in this range, $\mathrm{ord}_p(Ш(\mathbb{Q},E)_{\mathrm{an}}) \leqslant 6$ for all primes p. If such an E is optimal, then $\mathrm{ord}_p(Ш(\mathbb{Q},E)_{\mathrm{an}}) \leqslant 4$ for all primes p.

THEOREM 8.1. *If $E/\mathbb{Q}$ has conductor $N < 5000$ and $r_{\mathrm{an}}(E) \leqslant 1$, then* BSD$(E,2)$ *is true.*

Proof. Assume that E is an optimal curve and let $T(E) = \mathrm{ord}_2(\#Ш(\mathbb{Q},E)_{\mathrm{an}})$. For each curve we are considering, if $T(E) = 0$, then a 2-descent proves BSD$(E,2)$ and if $T(E) > 0$, then a 2-descent proves $Ш(\mathbb{Q},E)[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$. If $T(E) = 2$, then a 4-descent proves BSD$(E,2)$ and if $T(E) > 2$, then a 4-descent proves $Ш(\mathbb{Q},E)[4] \cong (\mathbb{Z}/4\mathbb{Z})^2$. For the range of curves we are considering, $T(E)$ is at most four and, if $T(E) = 4$, an 8-descent proves $Ш(\mathbb{Q},E)[8] = Ш(\mathbb{Q},E)[4]$ and hence proves BSD$(E,2)$. □

THEOREM 8.2. *If $E/\mathbb{Q}$ has conductor $N < 5000$ and $r_{\mathrm{an}}(E) \leqslant 1$, then* BSD$(E,3)$ *is true.*

Proof. For optimal curves where $\mathrm{ord}_3(\#Ш(\mathbb{Q},E)_{\mathrm{an}})$ is trivial, a 3-descent suffices. For the rest, we have that $\mathrm{ord}_3(\#Ш(\mathbb{Q},E)_{\mathrm{an}}) = 2$, and in this case a 3-descent proves $Ш(\mathbb{Q},E)[3] \cong (\mathbb{Z}/3\mathbb{Z})^2$. These 31 remaining optimal curves are shown in Table 2. If E is in the set

$$\{681b1, 1913b1, 2006e1, 2429b1, 2534e1, 2534f1, 2541d1, 2674b1, 2710c1, 2768c1, 2849a1,$$
$$2955b1, 3054a1, 3306b1, 3536h1, 3712j1, 3954c1, 4229a1, 4592f1, 4606b1\},$$

then the algorithm of Stein and Wuthrich [54] proves the desired upper bound. For the rest of the curves except for 2366d1 and 4914n1, the mod-3 representations are surjective. Table 3 displays selected Heegner indexes in this case, which together with Theorem 4.4 (and Theorem 5.4 for 4675j1 since $c_{17}(4675j1) = 3$) proves the desired upper bound.

Finally, we are left with 2366d1 and 4914n1. Each isogeny class contains a curve F for which $\#Ш(\mathbb{Q}, F)_{\mathrm{an}} = 1$, so we replace these curves with 2366d2 and 4914n2. Then 3-descent shows that $Ш(\mathbb{Q}, F)[3] = 0$, and hence $\mathrm{BSD}(F, 3)$ holds for both curves. □

COROLLARY 8.3. *If* $\mathrm{rank}(E(\mathbb{Q})) = 0$, *$E$ has conductor $N < 5000$ and E has CM, then the full BSD conjecture is true.*

Proof. This is a direct result of Corollary 3.2 and Theorems 8.1 and 8.2. □

THEOREM 8.4. *If $E/\mathbb{Q}$ is an optimal curve with conductor $N < 5000$ and non-trivial analytic* Ш, *that is,* $\#Ш(\mathbb{Q}, E)_{\mathrm{an}} \neq 1$, *then, for every* $p \mid \#Ш(\mathbb{Q}, E)_{\mathrm{an}}$, $\mathrm{BSD}(E, p)$ *is true.*

Proof. By [**15**], we have that $p \leqslant 7$ and, by the theorems of the previous section, we may assume $p \geqslant 5$.

For $p = 5$, E is one of the twelve curves listed in Table 4. These are all rank-zero curves with $\overline{\rho}_{E,5}$ surjective, so, if $5 \nmid N$, Theorem 5.1 provides an upper bound of 2 for $\mathrm{ord}_5(\#Ш(\mathbb{Q}, E))$. This leaves just 2900d1 and 3185c1. For 2900d1, Corollary 4.8 together with a point search shows that the Heegner index is at most 23 for discriminant -71; hence, Kolyvagin's inequality provides the upper bound of 2 in this case. For 3185c1, the algorithm of Stein and Wuthrich [**54**] provides the upper bound of 2. In all twelve cases [**17**] (and the appendix of [**2**]) found visible non-trivial parts of $Ш(\mathbb{Q}, E)[5]$. Since the order must be a square, $\#Ш(\mathbb{Q}, E)$ must be exactly 25 in each case.

For $p = 7$, there is only one curve $E = 3364c1$ and $\overline{\rho}_{E,7}$ is surjective. Since $7 \nmid 3364$ and E is a rank-zero curve without CM, Theorem 5.1 bounds $\mathrm{ord}_7(\#Ш(\mathbb{Q}, E))$ from above by 2. Furthermore, Grigorov's thesis [**26**, p. 88] showed that $\mathrm{ord}_7(\#Ш(\mathbb{Q}, E))$ is bounded from below by 2. Alternatively, the elements of $Ш(\mathbb{Q}, E)[7]$ are visible at three times the level, as Tom Fisher kindly pointed out — one should also be aware of his tables of non-trivial elements of Ш of order three and five, available on his website[†]. □

TABLE 2. *Optimal E with* $\mathrm{ord}_3(\#Ш(\mathbb{Q}, E)_{\mathrm{an}}) = 2$.

681b1	2429b1	2601h1	2768c1	3054a1	3712j1	4229a1	4675j1
1913b1	2534e1	2674b1	2849a1	3306b1	3879e1	4343b1	4914n1
2006e1	2534f1	2710c1	2932a1	3536h1	3933a1	4592f1	4963c1
2366d1	2541d1	2718d1	2955b1	3555e1	3954c1	4606b1	

TABLE 3. *Heegner indexes where* $\mathrm{ord}_3(\#Ш(\mathbb{Q}, E)_{\mathrm{an}}) = 2$.

E	D	I_D	$\mathrm{ord}_3(I_D)$	E	D	I_D	$\mathrm{ord}_3(I_D)$
2601h1	−8	12	1	3933a1	−56	24	1
2718d1	−119	48	1	4343b1	−19	12	1
2932a1	−31	3	1	4675j1	−19	18	2
3555e1	−56	6	1	4963c1	−19	3	1
3879e1	−35	24	1				

TABLE 4. *Optimal E with* $\mathrm{ord}_5(\#Ш(\mathbb{Q}, E)_{\mathrm{an}}) = 2$.

1058d1	1664k1	2574d1	2900d1	3384a1	4092a1
1246b1	2366f1	2834d1	3185c1	3952c1	4592d1

[†] http://www.dpmms.cam.ac.uk/~taf1000/.

THEOREM 8.5. *If $E/\mathbb{Q}$ is an optimal rank-zero curve with conductor $N < 5000$ and p is a prime such that $E[p]$ is irreducible, then* $\mathrm{BSD}(E, p)$ *is true.*

Proof. By theorems of the previous two sections, we may assume $p > 3$, that E does not have CM and $\mathrm{ord}_p(\#Ш(\mathbb{Q}, E)_{\mathrm{an}}) = 0$. In this case, Theorem 5.1 applies to E (since the rank part of the conjecture is known for $N < 130000$ by [**15**]). At first, suppose that E does not have additive reduction at p.

Suppose that $\overline{\rho}_{E,p}$ is surjective. In this case, we need only consider primes dividing the conductor N. For such pairs (E, p), we can compute the Heegner index or an upper bound for it, which gives an upper bound on $\mathrm{ord}_p(Ш(\mathbb{Q}, E))$. When the results of Kolyvagin and Jetchev were not strong enough to prove $\mathrm{BSD}(E, p)$ using the first available Heegner discriminant, the algorithm of Stein and Wuthrich [**54**] was (although to be fair the former may be strong enough using other Heegner discriminants in these cases). This algorithm always provides a bound in this situation, since $p > 3$ is prime of non-additive reduction such that $\overline{\rho}_{E,p}$ is surjective and E is rank zero.

Now suppose that $\overline{\rho}_{E,p}$ is not surjective. The curve–prime pairs matching these hypotheses can be found in Table 5 along with selected Heegner indexes. The only prime to occur in these pairs is 5, and each chosen Heegner discriminant and index is not divisible by 5 except for $E = 3468\mathrm{h}$. Further, 5 does not divide the conductor of any of these curves, so, by Cha's Theorem 5.2, $\mathrm{BSD}(E, 5)$ is true for these pairs. For $E = 3468\mathrm{h}$, note that one of the Tamagawa numbers is 5, so, by Theorem 5.4, $\mathrm{BSD}(E, 5)$ is true for this curve.

We are now left to consider the 1964 pairs (E, p) for which E has additive reduction at p. There are fourteen pairs where $\overline{\rho}_{E,p}$ is not surjective, and Theorem 5.3 applies to all of them. The Heegner point height calculations listed in Table 6 prove that $\mathrm{BSD}(E, p)$ is true in these cases. Note that when p may divide the Heegner index, it must do so of order at most one, and in these cases it also divides a Tamagawa number, so Theorem 5.4 assists Theorem 5.3.

Now we may also assume that $\overline{\rho}_{E,p}$ is surjective. In these cases, Heegner index computations sufficed to prove $\mathrm{BSD}(E, p)$, using Theorems 4.4 and 5.4. For 79 of these curves, the Heegner

TABLE 5. *Non-additive reduction, irreducible but not surjective.*

E	p	D	I_D	E	p	D	I_D	E	p	D	I_D
324b1	5	−23	6	1296g1	5	−23	2	3468c1	5	−47	2
324d1	5	−23	2	1296i1	5	−23	2	3468h1	5	−47	⩽11
608b1	5	−31	2	1444a1	5	−31	2	4176n1	5	−23	⩽3
648c1	5	−23	4	2268a1	5	−47	6	4232b1	5	−7	2
1044a1	5	−23	12	2268b1	5	−47	⩽3	4232d1	5	−7	6
1216i1	5	−31	1	3132a1	5	−23	6				

TABLE 6. *Additive reduction, irreducible but not surjective.*

E	p	D	I_D	τ_p	E	p	D	I_D	τ_p
675d1	5	−11	2	1	2400bg1	5	−71	20	10
675f1	5	−11	2	1	2450d1	7	−31	1	1
800e1	5	−31	6	3	2450bd1	7	−31	<13	7
800f1	5	−31	2	1	4800n1	5	−71	<5	3
1600i1	5	−31	4	2	4800u1	5	−71	10	5
1600k1	5	−31	4	2	4900s1	5	−31	4	2
2400f1	5	−191	<5	2	4900u1	5	−31	12	6

$\tau_p = \mathrm{ord}_p(\prod_q c_q)$.

index computation required 4- and even 6-descent [**23**]. These are listed in Table 7, thanks to Tom Fisher. □

For example, if $E = 1050c1$, the first available Heegner discriminant is -311. Bounding the Heegner index is more difficult in such cases, since it involves point searches to large heights. However, in two and a half seconds the algorithm of Stein and Wuthrich provides an upper bound of 0 for the 7-primary part of the Shafarevich–Tate group, which eliminates the last prime for that curve.

PROPOSITION 8.6. *If E is the elliptic curve 1155k1 and $p = 7$, then* BSD(E, p) *is true.*

Note that for $(E, p) = (1155k1, 7)$, we have $c_3(E) = 7, c_5(E) = 7$,

$$\mathrm{ord}_7(\#Ш(\mathbb{Q}, E)_{\mathrm{an}}) = 0 \quad \text{and} \quad \mathrm{ord}_7(\#Ш(\mathbb{Q}, E)) \leqslant 2,$$

by Theorem 5.4. The following proof is due to C. Wuthrich.

TABLE 7. *Additive reduction, surjective.*

E	p	D	I_D	τ_p	E	p	D	I_D	τ_p
1050l1	5	−311	3	0	3850m1	5	−2351	2	0
1050n1	5	−2399	19	0	3850y1	5	−1399	54	0
1050q1	5	−311	7	0	3900k1	5	−1199	4	0
1350o1	5	−239	4	0	3900l1	5	−191	30	1
1470q1	7	−479	26	0	4050bi1	5	−71	4	0
1764h1	7	−167	6	0	4050s1	5	−551	6	0
1850d1	5	−471	6	0	4050x1	5	−119	6	0
2100o1	5	−311	4	0	4200bd1	5	−479	27	0
2352x1	7	−551	6	0	4200m1	5	−719	32	0
2450bd1	5	−559	14	0	4350q1	5	−719	11	0
2450k1	5	−159	2	0	4350w1	5	−719	24	0
2550bc1	5	−191	7	0	4410b1	7	−671	4	0
2550j1	5	−239	23	0	4410bi1	7	−1319	18	0
2550z1	5	−1511	45	1	4410bj1	7	−311	6	0
2646ba1	7	−47	11	0	4410q1	7	−839	4	0
2646bd1	7	−143	10	0	4410u1	7	−2231	10	0
2650k1	5	−679	28	0	4550p1	5	−1119	14	0
3038m1	7	−55	6	0	4606b1	7	−31	12	0
3150bc1	5	−1511	6	0	4650bo1	5	−119	18	0
3150bd1	5	−1991	64	0	4650bs1	5	−239	84	0
3150bj1	5	−311	2	0	4650bt1	5	−1511	2	0
3150bn1	5	−1991	22	0	4650bu1	5	−1199	170	1
3150t1	5	−1151	6	0	4650q1	5	−119	6	0
3185c1	7	−199	10	0	4650w1	5	−719	46	0
3225b1	5	−119	4	0	4725q1	5	−59	8	0
3234c1	7	−503	16	0	4800ba1	5	−71	7	0
3350d1	5	−79	12	0	4850h1	5	−31	22	0
3450p1	5	−479	13	0	4900w1	5	−311	8	0
3450v1	5	−191	180	1	4950bj1	5	−239	6	0
3630c1	11	−1559	4	0	4950bk1	5	−239	14	0
3630l1	11	−239	35	0	4950bm1	5	−479	56	0
3630r1	11	−239	7	0	4950bp1	5	−431	22	0
3630u1	11	−1319	9	0	4950w1	5	−1151	4	0
3650j1	5	−79	14	0	4950x1	5	−359	12	0
3822bc1	7	−647	18	0	4998bg1	7	−47	18	0
3822e1	7	−1511	2	0	4998bk1	7	−47	36	0
3822u1	7	−503	10	0	4998k1	7	−47	30	0
3822w1	7	−503	6	0	4998t1	7	−1487	6	0
3822z1	7	−1823	32	0	4998u1	7	−47	6	0
3850e1	5	−1399	6	0					

$\tau_p = \mathrm{ord}_p(\prod_q c_q)$.

Proof. First, note that $E/\mathbb{Q}$ has non-split multiplicative reduction at 7. Let $D=-8$ and let $K=\mathbb{Q}(\sqrt{D})$, noting that $E(K)=E(\mathbb{Q})\cong\mathbb{Z}$ and that $\#E^D(\mathbb{Q})=1$. Since 7 is inert in K, the reduction of E/K at $7\mathcal{O}_K$ is split multiplicative. Kato's theorem [**33**, Theorem 17.4] is known to hold for curves with multiplicative reduction over abelian fields unramified at p. The characteristic series $f(T)$ of the dual of the Selmer group therefore divides the p-adic L-series

$$L_p(E/K,T)=L_p(E/\mathbb{Q},T)\cdot L_p(E^D/\mathbb{Q},T).$$

By work of Jones [**32**, Theorem 3.1], we can compute the order of vanishing of $f(T)$ at $T=0$, which is 2 since the reduction is split multiplicative, and the leading term, which is, up to a unit in $\mathbb{Z}_p^\times$,

$$\frac{\prod_v c_v\cdot\#\tilde{E}(\mathbb{F}_{49})\cdot\#Ш(K,E)[7^\infty]\cdot\mathrm{Reg}_p(E(K))\cdot\mathcal{L}}{\#E(K)_{\mathrm{tors}}^2},$$

where $\mathcal{L}$ is the L-invariant and Reg_p is the p-adic regulator as defined in the split multiplicative case in [**37**] and corrected in [**58**].

We compute $\prod_v c_v=7^3$, $\tilde{E}(\mathbb{F}_{49})\cong\mathbb{Z}/48\mathbb{Z}$ and

$$L_p(E/\mathbb{Q},T)=(6\cdot7+O(7^2))\cdot T+(4\cdot7+O(7^2))\cdot T^2+O(T^3),$$
$$L_p(E^D/\mathbb{Q},T)=(2\cdot7+O(7^2))\cdot T+(4\cdot7+O(7^2))\cdot T^2+O(T^3).$$

To compute the L-invariant $\mathcal{L}$, we switch to the Tate curve. Since $E^D/\mathbb{Q}$ has split multiplicative reduction at 7 and the parameter is the same as for E/K, we have

$$q_E=3\cdot7+3\cdot7^2+4\cdot7^3+7^5+O(7^6).$$

Hence, the L-invariant is

$$\mathcal{L}=\log_p(q_E)/\mathrm{ord}_p(q_E)=2\cdot7+6\cdot7^2+2\cdot7^3+5\cdot7^4+O(7^6).$$

Finally, we wish to compute the p-adic regulator. If P is a generator of $E(K)$, then $Q=7\cdot8\cdot P$ has good reduction everywhere and lies in the formal group at the place $7\mathcal{O}_K$. One computes, as in [**54**, § 4.2], the p-adic height of Q and so that of P:

$$h_p(P)=\frac{h_p(Q)}{(7\cdot8)^2}=2\cdot7^{-1}+4+5\cdot7+2\cdot7^2+7^3+3\cdot7^5+O(7^6).$$

Since the leading term of the p-adic L-function is $5\cdot7^2+O(7^3)$ and the leading term of $f(T)$ must have smaller valuation, we have

$$\mathrm{ord}_p\left(7^3\cdot48\cdot\#Ш(K,E)[7^\infty]\cdot\frac{h_p(P)}{7}\cdot\mathcal{L}\right)\leqslant2.$$

Therefore,

$$\mathrm{ord}_p(\#Ш(K,E)[7^\infty])\leqslant-\mathrm{ord}_p(h_p(P))-\mathrm{ord}_p(\mathcal{L})=0.$$

In particular, $\mathrm{ord}_7(\#Ш(\mathbb{Q},E))=0$. □

It may also be possible to prove this using [**25**], since there is a modular congruence $E[7]\cong F[7]$, where F is the curve 77a1.

THEOREM 8.7. *If $E/\mathbb{Q}$ is a rank-one curve with conductor $N<5000$ and p is a prime such that $E[p]$ is irreducible, then* BSD(E,p) *is true.*

Proof. We may assume in addition that E is optimal, since reducibility is isogeny-invariant. By Theorems 8.1 and 8.2, if $p<5$, then BSD(E,p) is true. Thus, we may assume $p\geqslant5$. Computing the Heegner index is much easier when E has rank one, as noted in Section 4. Kolyvagin's Theorem 4.4 then rules out many pairs (E,p) right away. Then some combination of

Theorems 5.2, 5.3 and 5.4 and the algorithm of Stein and Wuthrich [**54**] will rule out many more pairs. If no combination of these techniques works for the first Heegner index one computes, then another Heegner discriminant must be used. Table 8 lists rank-one curves E for which this is necessary, such that $E[p]$ is irreducible, E does not have CM and $(E,p)\neq(1155\mathrm{k},7)$. All these curves have $\overline{\rho}_{E,p}$ surjective and p does not divide any Tamagawa numbers, so it is sufficient to demonstrate a Heegner index which p does not divide. The case $(1155\mathrm{k},7)$ is Proposition 8.6.

If E has CM, we may also rule out primes which split in the CM field. There are seventeen pairs (E,p) left, namely the fifteen pairs in Example 7.1 and the two in Example 7.2. Table 9 lists Heegner indexes, which, together with Theorem 4.4, prove the fifteen cases not handled in Example 7.2. □

9. *Curves of conductor $N<5000$, reducible mod-p representations*

Suppose that E is an optimal elliptic curve of conductor $N<5000$ and p is a prime such that $E[p]$ is reducible, that is, there is a p-isogeny $\phi:E\to E'$. Further, assume $r_{\mathrm{an}}(E)\leqslant 1$. If $p<5$ or E is a rank-zero curve with CM, results of the previous sections show that $\mathrm{BSD}(E,p)$ is true. This leaves 462 pairs (E,p). The results of Theorem 5.3 can be applied to 339 of these curve–prime pairs, using Corollary 4.8 and various descents, including [**23**]. This leaves 123 pairs of the original 462: 102 isogenies of degree 5, sixteen isogenies of degree 7, two isogenies of degree 11, and one isogeny each of degrees 19, 43 and 67. Of the 123 rank-zero and rank-one cases remaining, 104 more at $p\in\{5,7\}$ are covered in [**22**].

Of the nineteen remaining cases, eight are proved in a paper by Michael Stoll and the author [**39**]. The eleven remaining are listed in Table 10: if (E,p) does not appear in Table 10 for $E[p]$ reducible, then $\mathrm{BSD}(E,p)$ is true. These eleven remaining cases will be handled in a

TABLE 8. *Some Heegner indexes using larger discriminants.*

E	p	D	I_D	E	p	D	I_D	E	p	D	I_D
1450c1	5	−151	3	3150i1	5	−479	8	4440f1	5	−259	2
1485e1	5	−131	4	3150bb1	5	−479	4	4485d1	5	−296	2
1495a1	5	−79	3	3310b1	5	−151	3	4550j1	5	−199	4
1735a1	5	−24	4	3450b1	5	−551	28	4675t1	5	−84	9
2090c1	5	−431	8	3480h1	5	−239	2	4680h1	5	−311	8
2145a1	5	−131	2	3630h1	5	−431	3	4725c1	5	−104	8
2275b1	5	−139	2	3760k1	5	−39	1	4800bx1	5	−119	7
2550n1	5	−239	9	3900n1	5	−599	2	4815e1	5	−71	6
2860a1	5	−519	9	3920y1	5	−159	6	4950r1	5	−359	6
2970j1	5	−359	3	4050h1	5	−239	32				
2990e1	5	−159	12	4140c1	5	−359	6	2660a1	7	−439	11
3060h1	5	−359	18	4200t1	5	−551	4	4158a1	7	−215	2
3075a1	5	−119	14	4400z1	5	−79	24	4704t1	7	−143	8
3140b1	5	−39	2	4410i1	5	−479	2	4914x1	7	−335	12

TABLE 9. *Heegner indexes of some rank-one curves with CM.*

E	p	D	I_D	E	p	D	I_D
675a	5	−11	2	3136v	7	−47	2
900c	5	−119	6	3267d	11	−8	2
1568g	7	−31	2	3600bd	5	−71	12
2700h	5	−119	3	3872a	11	−7	2
2700l	5	−119	3	4356a	11	−95	4
2700p	5	−71	6	4356b	11	−167	6
3136t	7	−55	2	4356c	11	−95	2
3136u	7	−31	4				

forthcoming paper with Brendan Creutz, in which we will show that the corresponding p-torsion elements of $Ш(\mathbb{Q}, E')$ are not divisible by p.

TABLE 10. *Remaining curves: reducible representations.*

E	p	E	p
546f	7	1938j	5
570l	5	1950y	5
858k	7	2370m	5
870i	5	2550be	5
1050o	5	3270h	5
1230k	7		

Acknowledgements. The author wishes to thank John Coates, John Cremona, Tim and Vlad Dokchitser, Tom Fisher, Ralph Greenberg, Dimitar Jetchev, William Stein, Michael Stoll and Christian Wuthrich for their help and encouragement. It is also a pleasure to thank the anonymous referees for many helpful comments and suggestions. The author was supported in part by NSF DMS Grants #0354131, #0757627, #61-5655, #61-5801 and #61-7586.

References

1. A. AGASHE, K. RIBET and W. A. STEIN, 'The Manin constant', *Pure Appl. Math. Q.* 2 (2006) no. 2, 617–636 part 2; MR 2251484(2007c:11076).
2. 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.
3. K. BELABAS, H. COHEN *et al.*, PARI/GP, The Bordeaux Group, http://pari.math.u-bordeaux.fr/.
4. B. J. BIRCH and H. P. F. SWINNERTON-DYER, 'Notes on elliptic curves. I', *J. Reine Angew. Math.* 212 (1963) 7–25.
5. B. J. BIRCH and H. P. F. SWINNERTON-DYER, 'Notes on elliptic curves. II', *J. Reine Angew. Math.* 218 (1965) 79–108.
6. C. BREUIL, B. CONRAD, F. DIAMOND and R. TAYLOR, 'On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises', *J. Amer. Math. Soc.* 14 (2001) no. 4, 843–939.
7. J. P. BUHLER, B. H. GROSS and D. B. ZAGIER, 'On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3', *Math. Comp.* 44 (1985) no. 170, 473–481; MR 777279(86g:11037).
8. D. BUMP, S. FRIEDBERG and J. HOFFSTEIN, 'Non-vanishing theorems for L-functions of modular forms and their derivatives', *Invent. Math.* 102 (1990) no. 3, 543–618.
9. J. CANNON, A. STEELE *et al.*, MAGMA Computational Algebra System, The University of Sydney, http://magma.maths.usyd.edu.au/magma/.
10. 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.
11. B. CHA, 'Vanishing of some cohomology groups and bounds for the Shafarevich–Tate groups of elliptic curves', PhD Thesis, Johns Hopkins University, 2003.
12. B. CHA, 'Vanishing of some cohomology goups and bounds for the Shafarevich–Tate groups of elliptic curves', *J. Number Theory* 111 (2005) 154–178.
13. I. CONNELL, Elliptic curve handbook, http://www.math.mcgill.ca/connell/public/ECH1, 1999.
14. J. E. CREMONA, *Algorithms for modular elliptic curves*, 2nd edn (Cambridge University Press, Cambridge, UK, 1997).
15. J. CREMONA, 'The elliptic curve database for conductors to 130000', *Algorithmic number theory*, Lecture Notes in Computer Science 4076 (Springer, Berlin, 2006) 11–29; MR 2282912(2007k:11087).
16. J. E. CREMONA and T. A. FISHER, 'On the equivalence of binary quartics', *J. Symbolic Comput.* 44 (2009) no. 6, 673–682.
17. J. E. CREMONA and B. MAZUR, 'Visualizing elements in the Shafarevich–Tate group', *Experiment. Math.* 9 (2000) no. 1, 13–28.
18. J. E. CREMONA, M. PRICKETT and S. SIKSEK, 'Height difference bounds for elliptic curves over number fields', *J. Number Theory* 116 (2006) no. 1, 42–68.
19. J. E. CREMONA and M. STOLL, 'Minimal models for 2-coverings of elliptic curves', *LMS J. Comput. Math.* 5 (2002) 220–243 (electronic).
20. H. DARMON, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics 101 (Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004).

21. B. Edixhoven, 'On the Manin constants of modular elliptic curves', *Arithmetic algebraic geometry (Texel, 1989)* (Birkhäuser, Boston, MA, 1991) 25–39.

22. T. Fisher, 'On 5 and 7 descents for elliptic curves', PhD Thesis, University of Cambridge, 2000.

23. T. Fisher, 'Finding rational points on elliptic curves using 6-descent and 12-descent', *J. Algebra* 320 (2008) no. 2, 853–884.

24. E. V. Flynn, F. Leprévost, E. F. Schaefer, W. A. Stein, M. Stoll and J. L. Wetherell, 'Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves', *Math. Comp.* 70 (2001) no. 236, 1675–1697; MR 1836926(2002d:11072)(electronic).

25. R. Greenberg and V. Vatsal, 'On the Iwasawa invariants of elliptic curves', *Invent. Math.* 142 (2000) no. 1, 17–63; MR 1784796(2001g:11169).

26. G. Grigorov, 'Kato's Euler system and the main conjecture', PhD Thesis, Harvard University, 2005.

27. G. Grigorov, A. Jorza, S. Patrikis, W. Stein and C. Tarniţă, 'Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves', *Math. Comp.* 78 (2009) 2397–2425.

28. B. H. Gross, 'Kolyvagin's work on modular elliptic curves', *L-functions and arithmetic (Durham, 1989)*, London Mathematical Society Lecture Note Series 153 (Cambridge University Press, Cambridge, UK, 1991) 235–256.

29. B. Gross and D. Zagier, 'Heegner points and derivatives of *L*-series', *Invent. Math.* 84 (1986) no. 2, 225–320.

30. G. Hochschild and J.-P. Serre, 'Cohomology of group extensions', *Trans. Amer. Math. Soc.* 74 (1953) 110–134.

31. D. Jetchev, 'Global divisibility of Heegner points and Tamagawa numbers', *Compos. Math.* 144 (2008) no. 4, 811–826.

32. J. W. Jones, 'Iwasawa *L*-functions for multiplicative abelian varieties', *Duke Math. J.* 59 (1989) no. 2, 399–420; MR 1016896(90m:11094).

33. K. Kato, '*p*-adic Hodge theory and values of zeta functions of modular forms', *Astérisque* 295 (2004) 117–290 ix.

34. V. A. Kolyvagin, 'Euler systems', *The Grothendieck festschrift,* vol. II, Progress in Mathematics 87 (Birkhäuser, Boston, MA, 1990) 435–483.

35. S. Lang, *Number theory. III,* vol. 60 (Springer, 1991).

36. K. 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 1969183(2004c:11098).

37. B. Mazur, J. Tate and J. Teitelbaum, 'On *p*-adic analogues of the conjectures of Birch and Swinnerton-Dyer', *Invent. Math.* 84 (1986) no. 1, 1–48; MR 830037(87e:11076).

38. J. R. Merriman, S. Siksek and N. P. Smart, 'Explicit 4-descents on an elliptic curve', *Acta Arith.* 77 (1996) no. 4, 385–404.

39. R. L. Miller and M. Stoll, Explicit isogeny descent on elliptic curves, http://arxiv.org/abs/1010.3334, 2010.

40. J. S. Milne, *Arithmetic duality theorems*, second edn (BookSurge, Charleston, SC, 2006).

41. M. R. Murty and V. K. Murty, 'Mean values of derivatives of modular L-series', *Ann. of Math.* (2) 133 (1991) no. 3, 447–475.

42. M. J. Razar, 'The non-vanishing of $L(1)$ for certain elliptic curves with no first descents', *Amer. J. Math.* 96 (1974) 104–126; MR 0360596(50#13044a).

43. M. J. Razar, 'A relation between the two-component of the Tate–Šafarevič group and $L(1)$ for certain elliptic curves', *Amer. J. Math.* 96 (1974) 127–144; MR 0360597(50#13044b).

44. K. Rubin, 'Congruences for special values of *L*-functions of elliptic curves with complex multiplication', *Invent. Math.* 71 (1983) no. 2, 339–364.

45. K. Rubin, 'The main conjectures of Iwasawa theory for imaginary quadratic fields', *Invent. Math.* 103 (1991) no. 1, 25–68.

46. E. F. Schaefer and M. Stoll, 'How to do a *p*-descent on an elliptic curve', *Trans. Amer. Math. Soc.* 356 (2004) 1209–1231.

47. P. Serf, 'The rank of elliptic curves over real quadratic number fields of class number 1', PhD Thesis, Universität des Saarlandes, 1995.

48. S. Siksek, 'Descents on curves of genus 1', PhD Thesis, University of Exeter, 1995.

49. J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics 106 (Springer, New York, 1992).

50. J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics 151 (Springer, New York, 1994).

51. E. Skinner and C. Urban, 'The Iwasawa main conjectures for GL_2', http://www.math.columbia.edu/∼urban/eurp/MC.pdf.

52. S. Stamminger, 'Explicit 8-descent on elliptic curves', PhD Thesis, International University Bremen, 2005.

53. W. Stein, 'Explicit approaches to modular abelian varieties', PhD Thesis, University of California at Berkeley, 2000.

54. W. Stein and C. Wuthrich, 'Algorithms for the arithmetic of elliptic curves using Iwasawa theory', http://wstein.org/papers/shark, 2011.

55. W. Stein *et al.*, Sage: Open Source Mathematical Software, The Sage Group, http://www.sagemath.org, 2010.
56. J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki 9 (Société Mathématique de France, Paris, 1995) 415–440. Exp. No. 306.
57. J.-L. Waldspurger, 'Sur les valuers de certaines fonctions L automorphes en leur centre de symétrie', *Compositio Math.* 54 (1985) no. 2, 173–242.
58. A. Werner, 'Local heights on abelian varieties with split multiplicative reduction', *Compositio Math.* 107 (1997) no. 3, 289–317; MR 1458753(98c:14039).
59. A. J. Wiles, 'Modular elliptic curves and Fermat's last theorem', *Ann. of Math.* (2) 2 (1995) no. 3, 443–551.
60. T. Womack, 'Explicit descent on elliptic curves', PhD Thesis, University of Nottingham, 2003.
61. J. Woo, 'Arithmetic of elliptic curves and surfaces: descents and quadratic sections', PhD Thesis, Harvard University, 2010.
62. S.-W. Zhang, 'Gross–Zagier formula for GL(2) II', *Heegner points and Rankin L-series*, Mathematical Sciences Research Institute Publications 49 (Cambridge University Press, Cambridge, 2004) 191–214.

Robert L. Miller
Warwick Mathematics Institute
Zeeman Building
University of Warwick
Coventry CV4 7AL
United Kingdom

and

The Mathematical Sciences Research Institute
17 Gauss Way, Berkeley
CA 94720-5070
USA

and

Current address: Quid, Inc.
733 Front Street, C1A, San Francisco
CA 94111
USA

rmiller@quid.com