Empirical Evidence for the Birch and Swinnerton-Dyer Conjecture

Robert L. Miller

A dissertation submitted in partial fulfillment of
the requirements for the degree of

Doctor of Philosophy

University of Washington

2010

Program Authorized to Offer Degree: Mathematics

University of Washington
Graduate School

This is to certify that I have examined this copy of a doctoral dissertation by

Robert L. Miller

and have found that it is complete and satisfactory in all respects,
and that any and all revisions required by the final
examining committee have been made.

Chair of the Supervisory Committee:

_____

William Stein

Reading Committee:

_____

William Stein

_____

Ralph Greenberg

_____

Neal Koblitz

Date: _____

Signature_____

Date_____

University of Washington

Abstract

Empirical Evidence for the Birch and Swinnerton-Dyer Conjecture

Robert L. Miller

Chair of the Supervisory Committee:
Professor William Stein
Mathematics

The current state of knowledge about the Birch and Swinnerton-Dyer conjecture relies on some of the deepest and most difficult mathematical endeavors, including the modularity theorem of Wiles, Breuil, Conrad, Diamond and Taylor, which was instrumental in the proof of Fermat's last theorem. There are also the Euler systems of Kato and Kolyvagin, Rubin's work on curves with complex multiplication, Néron's classification and Tate's algorithm, and the formula of Gross and Zagier. Despite all of this mathematical energy there is still much to be learned. Many facts about the conjecture only become clear one case at a time, after hard computation. We prove the full Birch and Swinnerton-Dyer conjecture for many specific elliptic curves of analytic rank zero and one and conductor up to 5000 by combining theoretical and computational methods.

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

In this chapter we recall the statement of the Birch and Swinnerton-Dyer conjecture for elliptic curves over the rational numbers. In the second chapter we collect results about the conjecture for elliptic curves over the rational numbers of analytic rank at most one. In the third chapter we examine some techniques for performing descents on elliptic curves, which is useful in many of the cases where the more general theory breaks down. New results are found in the fourth chapter, in which we use the theory established in the previous two chapters when the analytic rank is at most one, in particular proving Theorem 1.1. Appendix A contains the tables referred to in Chapter 4 and in Theorem 1.1. For a statement of the conjecture for abelian varieties over global fields, see Appendix B. For the remainder we specialize to E an elliptic curve over $\mathbb{Q}$.

Suppose $E/\mathbb{Q}$ is an elliptic curve and let $E(\mathbb{Q})$ denote the set of points of E with coordinates in $\mathbb{Q}$, noting that $E(\mathbb{Q})$ is an abelian group whose identity we will denote $\mathcal{O}$. The Mordell-Weil theorem states that $E(\mathbb{Q})$ is finitely generated, i.e.,

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})_{\text{tors}}.$$

Let $a_p = p + 1 - \#E(\mathbb{F}_p)$ where $E(\mathbb{F}_p)$ is the mod-p reduction of E—this requires that E be a minimal Weierstrass model. In cases of good reduction ($p \nmid \Delta(E)$ where $\Delta(E)$ is the discriminant), $E(\mathbb{F}_p)$ is a group and in cases of bad reduction, $E(\mathbb{F}_p)$ is singular and the nonsingular points form a group. Define

$$L(E/\mathbb{Q}, s) = \prod_{p|\Delta(E)} \frac{1}{1 - a_p p^{-s}} \prod_{p \nmid \Delta(E)} \frac{1}{1 - a_p p^{-s} + p \cdot p^{-2s}},$$

which converges for $\Re(s) > 3/2$ and has an analytic continuation to the complex plane. The Birch and Swinnerton-Dyer conjecture asserts that $\text{rank}(E(\mathbb{Q})) = \text{ord}_{s=1} L(E/\mathbb{Q}, s)$[1]. For

[1]If you can prove this for every elliptic curve E over $\mathbb{Q}$, the Clay Mathematics Institute will give you a million dollars. [54]

this reason we define $r_{\mathrm{an}}(E/\mathbb{Q}) = \mathrm{ord}_{s=1} L(E/\mathbb{Q}, s)$ to be the *analytic rank* of E.

The determinant of the height pairing matrix, i.e., the regulator of $E(\mathbb{Q})$, is denoted $\mathrm{Reg}(E(\mathbb{Q}))$. With ω denoting the minimal invariant differential let $\Omega(E) = \int_{E(\mathbb{R})} |\omega|$ be the so-called "real period" of E, which is the real period (the least positive real element of the canonical period lattice) times the order of the component group of $E(\mathbb{R})$. Let $c_p(E)$ denote the Tamagawa numbers and let $Ш(\mathbb{Q}, E)$ denote the Shafarevich-Tate group. The Birch and Swinnerton-Dyer conjectural formula (assuming that $r = r_{\mathrm{an}}$) is:

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

which of course requires that $Ш(\mathbb{Q}, E)$ is finite, which is part of the conjecture. $\#Ш(\mathbb{Q}, E)_{\mathrm{an}}$ denotes the order predicted by the conjecture, which is not even known to be a rational number for a single curve of analytic rank greater than one.

For simplicity of notation (following [22]) we define the following:

Definition. $\mathrm{BSD}(E/\mathbb{Q}, p)$: We have $\mathrm{rank}(E(\mathbb{Q})) = r_{\mathrm{an}}(E/\mathbb{Q})$, $\#Ш(\mathbb{Q}, E)(p) < \infty$, $\#Ш(\mathbb{Q}, E)_{\mathrm{an}}$ is a rational number and

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

Note that the full conjecture for $E/\mathbb{Q}$ is equivalent to $\mathrm{BSD}(E/\mathbb{Q}, p)$ for all primes p. The rest of this paper if devoted to proving the following result:

Theorem 1.1. *Suppose $E/\mathbb{Q}$ is an elliptic curve of rank at most 1 and conductor $N(E) < 5000$. If $(E, p) \neq (1155k, 7)$ and (E, p) is not isogenous to one of the 223 pairs listed in Tables A.9, A.11, A.12, A.13 and A.15, then* $\mathrm{BSD}(E/\mathbb{Q}, p)$ *is true.*

Note that this gives the full Birch and Swinnerton-Dyer conjecture for 16501 curves of the 16725 of rank at most one and conductor at most 5000. The essential obstructions to proving BSD (for $\mathrm{rank}(E(\mathbb{Q})) \leq 1$ and $N(E) < 5000$) are reducible representations (the 127 curves in Tables A.11, A.12 and A.13), additive reduction (the 96 curves in Table A.9 and A.15) and situations in which p divides two distinct Tamagawa numbers (the pair $(E, p) = (1155\mathrm{k}, 7)$).

Suppose the conductor of $E/\mathbb{Q}$ is N. By [53] and [6] every elliptic curve over $\mathbb{Q}$ has a *modular parametrization,* which is a nonconstant morphism $\psi : X_0(N) \longrightarrow E$. In other words, every elliptic curve is a *Weil curve.* If for each isogenous curve E' with modular parametrization $\psi' : X_0(N) \longrightarrow E'$ 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 $E/\mathbb{Q}$ has an optimal elliptic curve in its isogeny class, and by the characterizing property this optimal curve is unique. Thus we can use optimal curves as isogeny class representatives and, by isogeny invariance of the BSD formula, focus on optimal curves.

A remark about computation is in order: Whenever we prove a theorem with the help of a computer, interesting questions arise. Aside from the philosophical points, there is the very real question of errors, both in hardware and software. Any computer-assisted proof implicitly includes as a hypothesis the statement that the software used did not encounter any bugs during execution.

There is a also benefit to computation which some may not expect, which comes in this investigation in the form of some of the tables and exceptions at the end of Chapter 4. These kinds of examples can point to areas of inquiry not fully addressed in the current theory—in particular the curves in Table A.9 are all rank 1 curves with CM where there are no known techniques to bound the p-primary subgroup of the Shafarevich-Tate group at all. These sorts of examples arising from computation often lead to innovation and discovery and they challenge us to think about what is necessary to provably verify something.

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 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 Chapter 4 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 3.8.

Chapter 2

ELLIPTIC CURVES OVER $\mathbb{Q}$

2.1 Imaginary quadratic twists

Since a fair amount of material to come will depend on the properties of a quadratic twist E^D of an elliptic curve E by $D < 0$, let us establish some of its properties here. Suppose E is an elliptic curve over $\mathbb{Q}$, and let $\mathrm{Isom}_{\mathbb{Q}}(E)$ denote the set of isomorphisms $E \longrightarrow E$ defined over $\mathbb{Q}$.

Given a cocycle $\xi \in H^1(G_{\mathbb{Q}}, \mathrm{Isom}_{\mathbb{Q}}(E))$ we can construct an elliptic curve as described in [43, ch. X] by constructing its field of functions. Let $\overline{\mathbb{Q}}(E)_\xi$ be a field isomorphic to $\overline{\mathbb{Q}}(E)$ via some $\mathbb{Q}$-isomorphism $Z : \overline{\mathbb{Q}}(E) \longrightarrow \overline{\mathbb{Q}}(E)_\xi$. We can define an action of $G_{\mathbb{Q}}$ on $\overline{\mathbb{Q}}(E)_\xi$ via Z:

$$Z(f)^\sigma = Z\left(\xi_\sigma^*(f^\sigma)\right) \text{ for all } \sigma \in G_{\mathbb{Q}} \text{ and all } f \in \overline{\mathbb{Q}}(E),$$

where $\xi_\sigma^* : \overline{\mathbb{Q}}(E) \longrightarrow \overline{\mathbb{Q}}(E)$ is induced by $\xi_\sigma : E \longrightarrow E$. Letting $\mathcal{F}$ denote the fixed field of $\overline{\mathbb{Q}}(E)_\xi$ under the action of $G_{\mathbb{Q}}$, we have $\mathcal{F} \cap \overline{\mathbb{Q}} = \mathbb{Q}$ and that $\overline{\mathbb{Q}}\mathcal{F} = \overline{\mathbb{Q}}(E)_\xi$. Thus $\mathcal{F}$ is an extension of $\mathbb{Q}$ of transcendence degree 1 with $\mathcal{F} \cap \overline{\mathbb{Q}} = \mathbb{Q}$, i.e., there exists a curve $E_\xi/\mathbb{Q}$ with $\mathbb{Q}(E_\xi) \cong \mathcal{F}$.

Let $\chi : G_{\mathbb{Q}} \longrightarrow \{\pm 1\}$ denote the quadratic character associated to $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$, i.e., $\chi(\sigma) = \sqrt{D}^\sigma/\sqrt{D}$, and use it to define a cocycle $\xi : G_{\mathbb{Q}} \longrightarrow \mathrm{Isom}_{\mathbb{Q}}(E)$ by $\xi_\sigma = [\chi(\sigma)]$. If E is given in short Weierstrass form

$$E : y^2 = x^3 + ax + b,$$

then $[-1](x, y) = (x, -y)$. We can express the action of $\sigma \in G_{\mathbb{Q}}$ on $\overline{\mathbb{Q}}(x, y)_\xi$ by

$$\sqrt{D}^\sigma = \chi(\sigma)\sqrt{D}, \quad x^\sigma = x, \quad y^\sigma = \chi(\sigma)y.$$

Thus $u = x$ and $v = y/\sqrt{D}$ are functions in $\overline{\mathbb{Q}}(x, y)_\xi$ fixed by $G_{\mathbb{Q}}$ and satisfy the equation $Dv^2 = u^3 + au + b$. If the given Weierstrass equation for E is minimal and the minimality

of its twist is needed, then multiplying u by D and v by D^2, we obtain the alternate form

$$E^D : v^2 = u^3 + aD^2u + bD^3.$$

The discriminant of the twist will be minimal as long as we assume $\gcd(\Delta(E), D) = 1$, since $\Delta(E^D) = -16\left(4\left(aD^2\right)^3 + 27\left(bD^3\right)^2\right) = D^6\Delta(E)$. The two curves are related by the $\mathbb{Q}(\sqrt{D})$-isomorphism

$$\varphi : E \longrightarrow E^D : \varphi(x, y) = \left(Dx, D^{3/2}y\right).$$

Let σ denote complex conjugation and note that if $x^\sigma = x$ and $y^\sigma = \pm y$ then

$$\varphi(x, y)^\sigma = (Dx, D^{3/2}y)^\sigma = (Dx, \mp D^{3/2}y) = \varphi((x, \mp y)) = [\mp 1]\varphi(x, y).$$

This shows that φ exchanges the ± 1-eigenspaces of σ. With $K = \mathbb{Q}(\sqrt{D})$, the following lemma gives a relationship between the Mordell-Weil groups $E(\mathbb{Q}), E^D(\mathbb{Q})$ and $E(K)$.

Lemma 2.1. *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 that*

1. *the intersection is two 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*

$$[E(K)_{/\text{tors}} : (E(\mathbb{Q}) + E^D(\mathbb{Q}))_{/\text{tors}}] \leq 2^r$$

and

$$[E(K) : E(\mathbb{Q}) + E^D(\mathbb{Q})] \leq 2^{r+s},$$

3. *and if $E(K)$ has rank 1, $E(\mathbb{Q})$ has rank 0 and $E(\mathbb{Q})[2] = 0$, then*

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

Proof. Let σ be the nontrivial element of $G = \mathrm{Gal}(K/\mathbb{Q})$, which is induced by complex conjugation since $D < 0$. Considering $E(K)$ as a $\mathbb{Z}[G]$-module, since $\sigma^2 - 1 = 0$, we are interested in the +1-eigenspace $E(K)^+ = \ker(\sigma - 1)$ and the -1-eigenspace $E(K)^- = \ker(\sigma + 1)$ of $E(K)$, which are interchanged by the K-isomorphism φ. The former is simply $E(\mathbb{Q})$ by definition and the latter is $\varphi^{-1}(E^D(\mathbb{Q}))$. We have that $E(K)^+ \cap E(K)^- = E(\mathbb{Q})[2]$, since $P \in E(K)^+ \cap E(K)^-$ is equivalent to $P = P^\sigma = -P$.

Let $z \in E(K)$ and note that

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

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

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

and

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

Now suppose that $E(K)$ has rank 1 and choose z such that $E(K) = \mathbb{Z}z \oplus E(K)_{\mathrm{tors}}$. Suppose further that $E(K)^+$ has rank 0. Then $z^\sigma + z \in E(K)^+$ must be torsion—say $z^\sigma + z = t$. Choose a so that $2a + 1$ is equal to the odd part of the order of t and let $w = z + at$. The element

$$w^\sigma + w = z^\sigma + at + (z + at) = z^\sigma + z + 2at = (2a + 1)t$$

is in $E(\mathbb{Q})[2]$. If we further suppose that $E(\mathbb{Q})[2] = 0$, then $w^\sigma + w = 0$, which implies that $w \in E(K)^-$. Since $w \equiv z$ modulo torsion, we have $E(K)_{/\mathrm{tors}} = E(K)^-_{/\mathrm{tors}}$. □

From the identifications of Lemma 2.1, we have an exact sequence

$$0 \longrightarrow T_1 \longrightarrow Ш(\mathbb{Q}, E) \times Ш(\mathbb{Q}, E^D) \longrightarrow Ш(K, E) \longrightarrow T_2 \longrightarrow 0, \qquad (2.1)$$

where T_1 and T_2 are finite 2-groups.

The following lemma is a correction to a formula which appeared in [23, p. 312] without proof.

Lemma 2.2. *Suppose $E/\mathbb{R}$ is an elliptic curve and $D < 0$ is a square-free fundamental discriminant. Then*

$$\Omega(E) \cdot \Omega(E^D) \cdot \sqrt{|D|} = [E(\mathbb{R}) : E^0(\mathbb{R})] \cdot ||\omega||^2.$$

Proof. Without loss of generality we may assume that E and E^D are in short Weierstrass form and $\varphi : E \longrightarrow E^D$ is defined as above. In this case the minimal invariant differentials for E and E^D are $\omega = \frac{dx}{2y}$ and $\omega_D = \frac{du}{2v}$, respectively. We calculate their relationship via φ:

$$\varphi^*(\omega_D) = \varphi^* \left(\frac{du}{2v} \right) = \varphi^* \left(\frac{d(Dx)}{2D^{3/2}y} \right) = D^{-1/2} \frac{dx}{2y} = D^{-1/2}\ \omega.$$

If $E(\mathbb{C})^{\pm}$ denotes the ± 1-eigenspace of $E(\mathbb{C})$ under the action of σ, then we have

$$\Omega(E^D) = \int_{E^D(\mathbb{R})} |\omega_D| = \int_{\varphi(E(\mathbb{C})^-)} |\omega_D| = \int_{E(\mathbb{C})^-} |\varphi^* \omega_D| = |D|^{-1/2} \int_{E(\mathbb{C})^-} |\omega|$$

and

$$\Omega(E) = \int_{E(\mathbb{R})} |\omega| = \int_{E(\mathbb{C})^+} |\omega|.$$

The constant $||\omega||^2$ is defined by the formula

$$||\omega||^2 = \int_{E(\mathbb{C})} \omega \wedge \overline{i\omega}.$$

We now switch to a complex variable via the Weierstrass map. Let $\Lambda \subset \mathbb{C}$ be the period lattice of ω, noting that the image of the invariant differential under the Weierstrass map $f : E(\mathbb{C}) \longrightarrow \mathbb{C}/\Lambda$ is $\frac{d\wp(z)}{\wp'(z)} = dz$. In order to avoid overloaded notation, we fix the complex variable $z = x_z + iy_z$ and compute $dz \wedge \overline{idz} = 2\ dy_z \wedge dx_z$. If $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$ where $\Re(\omega_1) > 0$, $\Im(\omega_1) = 0$, $\Im(\omega_2) > 0$ and $\Re(\omega_2) < \omega_1$, then the geometry of $\mathbb{C}/\Lambda$ breaks into two cases, depending on whether the fundamental domain is rectangular (when $\Delta(E) > 0$) or not (when $\Delta(E) < 0$). See Figure 2.1, in which $E(\mathbb{C})^+$ (colored red) is either one or two horizontal pieces, and $E(\mathbb{C})^-$ (colored green) is two vertical pieces. Let h be the height of the fundamental domain $\mathcal{D}$ and let b be the width of its base. Then we have

$$||\omega||^2 = \int_{\mathcal{D}} 2\ dy_z \wedge dx_z = 2 \iint_{\mathcal{D}} dy_z\ dx_z = 2bh,$$

and

$$\Omega(E) \cdot \Omega(E^D) \cdot \sqrt{|D|} = \int_{\mathcal{D}^+} |dz| \cdot \int_{\mathcal{D}^-} |dz| = 2bh[E(\mathbb{R}) : E^0(\mathbb{R})],$$

which together prove the claim. □

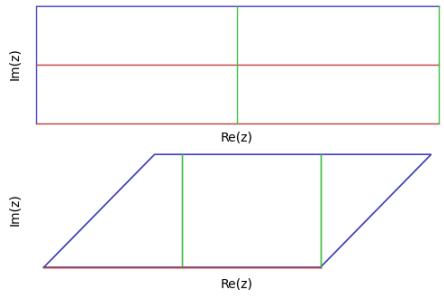

Figure 2.1: The ± 1-eigenspaces of $\mathbb{C}/\Lambda$ under complex conjugation.

2.2 Gross-Zagier-Zhang and Kolyvagin

If E is an elliptic curve over $\mathbb{Q}$ of conductor $N(E)$, we say that the quadratic imaginary field $K = \mathbb{Q}(\sqrt{D})$ satisfies the *Heegner hypothesis* for E if each prime $p \mid N(E)$ splits in K. If E^D is the twist of E by D then

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

If K satisfies the Heegner hypothesis for E, then the Heegner point $y_K \in E(K)$ is defined as follows (see [24] for details). By hypothesis (and some elbow grease) there is an ideal $\mathcal{N}$ of $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N}$ is cyclic of order $N = N(E)$. 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 complex multiplication by $\mathcal{O}_K$ and a point $x_1 \in X_0(N)$. By the theory of complex multiplication one can show that 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 [53] and [6]. There is a unique minimal invariant differential ω on E over $\mathbb{Z}$ and $\psi^*(\omega)$ is the differential associated to a normalized newform on $X_0(N)$. We have $\psi^*(\omega) = \alpha \cdot f$ where f is a normalized cusp form and α is some integer [20] constant which we may assume is nonzero. The *Manin constant* is $c := |\alpha|$ and the Heegner point is $y_K := \mathrm{Tr}_{H/K}(\varphi(x_1)) \in E(K)$. It has been conjectured that $c = 1$ if E is optimal. 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 proven 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 2.3 (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 $||\omega||^2 = \int_{E(\mathbb{C})} \omega \wedge \overline{i\omega}$, the quadratic imaginary number field K has $2u_K$ roots of unity and $\Delta(K)$ is the discriminant.

Proof. [23] when D is odd and [57] in general. □

Note that $u_{\mathbb{Q}(\sqrt{-1})} = 2$, $u_{\mathbb{Q}(\sqrt{-3})} = 3$ and for all other quadratic imaginary fields K (in particular those satisfying the Heegner hypothesis) 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 $r_{\mathrm{an}}(E) \leq 1$, this is a minor issue (see the proof of Theorem 2.6). Note also that the $\hat{h}$ appearing in the formula as stated here is the absolute height, whereas the one appearing in [23, Theorem 2.1, p. 311] is equal to our $2\hat{h}$.

Consider the map $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$, which we call the mod-$p$ representation since $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^2$ as abelian groups. Let R denote the endomorphism ring $R = \mathrm{End}(E/\mathbb{C})$. We have $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}_R(E[p])$, where $\mathrm{Aut}_R(E[p])$ is the subgroup of automorphisms commuting with the action of R. If E does not have complex multiplication, then $R = \mathbb{Z}$ and $\mathrm{Aut}_R(E[p]) = \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$. If E does have complex multiplication, then R is an order in a quadratic imaginary field and $\mathrm{Aut}_R(E[p]) \subsetneq \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$. In either case, we will say that $\overline{\rho}_{E,p}$ is *surjective* if its image is $\mathrm{Aut}_R(E[p])$. Often in the literature one sees this defined as being "as surjective as possible" in the complex multiplication case.

We have the following powerful theorem of Kolyvagin:

Theorem 2.4. *If y_K is nontorsion, then $E(K)$ has rank 1 (hence $I_K < \infty$), $Ш(K,E)$ is finite,*

$$c_3 I_K Ш(K,E) = 0 \text{ and } \#Ш(K,E) \big| c_4 I_K^2,$$

where c_3 and c_4 are positive integers explicitly defined in [29]. The primes dividing c_4 are at most 2 and the odd primes p for which $\overline{\rho}_{E,p}$ is surjective.

Proof. [29, Theorem A] □

Corollary 2.5. *If y_K is nontorsion, 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 the exact sequence (2.1), we have that $\#Ш(\mathbb{Q}, E) \cdot \#Ш(\mathbb{Q}, E^D)$ divides $\#Ш(K, E)$ up to a power of two. □

Theorem 2.6. *If $r_{an}(E) \leq 1$, then y_K is nontorsion. In particular,*

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

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

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

Proof. We follow the proof given in [19]. If $\varepsilon = -1$ (i.e., $r_{\mathrm{an}}(E) = 1$), then [52] 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 $\varepsilon = 1$ (i.e., $r_{\mathrm{an}}(E) = 0$), then results of [7] and [33] imply that there are infinitely many $D < 0$ such that $K = \mathbb{Q}(\sqrt{D})$ satisfies the Heegner hypothesis for E. In this case, for parity reasons, $L(E^D/\mathbb{Q}, 1)$ is always 0.

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 2.3), implies that y_K is nontorsion. Then Kolyvagin's theorem implies that $E(K)$ has rank 1, $I_K < \infty$ and that $Ш(K, E)$ is finite.

By Lemma 2.1, we have

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

The point y_K belongs to $E(\mathbb{Q})$ (up to torsion) if and only if $\varepsilon = -1$. If $\varepsilon = -1$, then $\mathrm{rank}(E(\mathbb{Q})) = 1$ since $y_K \in E(\mathbb{Q})_{/\mathrm{tors}}$. If $\varepsilon = 1$, then some multiple of y_K is in $E(K)^-$, which implies that $\mathrm{rank}(E^D(\mathbb{Q})) = 1$, hence $\mathrm{rank}(E(\mathbb{Q})) = 0$. □

Lemma 2.7. *If $B > 0$ is such that $S = \{P \in E(\mathbb{Q}) : \hat{h}(P) \leq B\}$ contains a set of generators for $E(\mathbb{Q})/2E(\mathbb{Q})$ then S generates $E(\mathbb{Q})$.*

Proof. See [13, §3.5]. □

Theorem 2.8. *If $r_{an}(E) \leq 1$, then there are algorithms to compute both the Mordell-Weil group $E(\mathbb{Q})$ and the Shafarevich-Tate group $Ш(\mathbb{Q}, E)$.*

Proof. Following [46], we can naively search for points in $E(\mathbb{Q})$ and the rank of what we find will eventually climb to r. We can also compute $L^{(k)}(E, 1)$ to a given precision which will give an upper bound on r_{an}. This upper bound will eventually converge to r_{an} as we increase the precision. Once our bounds for r and r_{an} are equal, we have computed the rank.

We can compute the subgroup $E(\mathbb{Q})[2]$ to obtain the rank of $E(\mathbb{Q})/2E(\mathbb{Q})$. A point search to compute the rank of $E(\mathbb{Q})$ will find independent points $P_1, ..., P_r$ of infinite order. If any sum of P_i is equal to $2Q$ for $Q \in E(\mathbb{Q})$, then we replace one of the P_i involved in the sum with Q and start over—this halves the index of what we have inside of $E(\mathbb{Q})$. If no subset of the (modified) P_i sums to twice a rational point, these plus the 2-torsion generators found above generate $E(\mathbb{Q})/2E(\mathbb{Q})$. Call these generators $P_1, ..., P_s$. Let $C = C(E)$ be the constant given in [15] such that $|\hat{h}(P) - h(P)| < C$ for all $P \in E(\mathbb{Q})$ and let $B = \max\{\hat{h}(P_1), ..., \hat{h}(P_s)\}$. We then perform a point search up to naive height $B + C$, and by the previous lemma this will guarantee a set of generators of $E(\mathbb{Q})$.

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

Note that if the full BSD conjecture holds, we may theoretically do a single n-descent, where $n^2 = \#Ш(\mathbb{Q}, E) = \#Ш(\mathbb{Q}, E)_{\text{an}}$, to determine the group structure of $Ш(\mathbb{Q}, E)$. However, for even moderately sized n this is impractical.

[1]Recall, we are only proving that an algorithm exists: this scheme quickly becomes computationally infeasible as p varies.

For $r_{\text{an}}(E) \leq 1$, the following theorem will allow us (at least in theory) to compute $\#Ш(\mathbb{Q}, E)_{\text{an}}$ exactly, which, together with the previous theorem, shows that the BSD formula for E can be proven for specific elliptic curves via computation.

Theorem 2.9. *If $r_{an}(E) \leq 1$, then $\#Ш(\mathbb{Q}, E)_{an}$ is a rational number with bounded denominator (i.e., there is an easily computed integer $n = n(E)$ such that $\#Ш(\mathbb{Q}, E)_{an} \in \mathbb{Z}[n^{-1}]$).*

Proof. The first fact we will need is that the L-ratio $L(F/\mathbb{Q}, 1)/\Omega(F)$ of any elliptic curve $F/\mathbb{Q}$ is a rational number. By [53] and [6] F is modular. Cremona [13, §2.8] gives an algorithm for computing these quantities for modular curves, however the original result (that the ratio is rational) is due to Birch.

If $r_{\text{an}}(E) = 0$, we have $\text{Reg}(E(\mathbb{Q})) = 1$ and

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

If $r_{\text{an}}(E) = 1$, then suppose $K = \mathbb{Q}(\sqrt{D})$ satisfies the Heegner hypothesis for E. Note that $L'(E/K, s) = L'(E, s) \cdot L(E^D/\mathbb{Q}, s)$. If z is a generator[2] of $E(\mathbb{Q})_{/\text{tors}}$, then since $\hat{h}_K(z) = 2\hat{h}_{\mathbb{Q}}(z)$, we have

$$\frac{\hat{h}_K(y_K)}{\hat{h}_{\mathbb{Q}}(z)} = \frac{2\hat{h}_K(y_K)}{\hat{h}_K(z)} = 2[E(K) : \mathbb{Z}y_K]^2.$$

By Theorem 2.3 (and since $\text{Reg}_{E(\mathbb{Q})} = \hat{h}_{\mathbb{Q}}(z)$) we have

$$\begin{aligned}
\#Ш(\mathbb{Q}, E)_{\text{an}} &= \frac{L'(E/K, 1)}{L(E^D/\mathbb{Q}, 1) \cdot \Omega(E) \cdot \hat{h}_{\mathbb{Q}}(z)} \cdot \frac{(\#E(\mathbb{Q})_{\text{tors}})^2}{\prod_p c_p} \\
&= \frac{\hat{h}_K(y_K)}{\hat{h}_{\mathbb{Q}}(z)} \cdot \frac{||\omega||^2}{\sqrt{|\Delta(K)|} \cdot L(E^D/\mathbb{Q}, 1) \cdot \Omega(E)} \cdot \frac{(\#E(\mathbb{Q})_{\text{tors}})^2}{c^2 \cdot \prod_p c_p} \\
&= \frac{||\omega||^2}{\sqrt{|\Delta(K)|} \cdot L(E^D/\mathbb{Q}, 1) \cdot \Omega(E)} \cdot \frac{2 \cdot [E(K) : \mathbb{Z}y_K]^2 \cdot (\#E(\mathbb{Q})_{\text{tors}})^2}{c^2 \cdot \prod_p c_p}.
\end{aligned}$$

By Lemma 2.2, we have that $\left(\Omega(E) \cdot \Omega(E^D) \cdot \sqrt{|\Delta(K)|}\right) / ||\omega||^2$ is a rational number. Since $L\left(E^D/\mathbb{Q}, 1\right)/\Omega(E^D)$ is a rational number, we have

$$\frac{||\omega||^2}{\sqrt{|\Delta(K)|} \cdot L(E^D/\mathbb{Q}, 1) \cdot \Omega(E)} \in \mathbb{Q},$$

and since the rest of the expression involves integers, we have $\#Ш(\mathbb{Q}, E)_{\text{an}} \in \mathbb{Q}$. □

[2]Here we are treating z as a generator of $E(K)$ for simplicity—it may be twice a generator, see Section 2.1. We can do this if we are only concerned with showing that a quantity is rational.

Gross and Zagier first proved this in [23, p. 312].

2.3 Complex Multiplication

If E is an elliptic curve over $\mathbb{Q}$, then $\mathrm{End}(E/\mathbb{C})$ is either $\mathbb{Z}$ or an order $\mathcal{O}$ in a quadratic imaginary number field K. If the latter is the case, there is an isogeny defined over $\mathbb{Q}$ from E to an elliptic curve E' with complex multiplication by the maximal order $\mathcal{O}_K$. Note that E has complex multiplication by a non-maximal order if and only if its j-invariant is in the set $\{-12288000, 54000, 287496, 16581375\}$. Suppose, without loss, that E is an elliptic curve defined over a quadratic imaginary field K and that E has complex multiplication by the ring of integers $\mathcal{O}_K$. The purpose of this section is to prove the following theorem:

Theorem 2.10. *Suppose E has CM by the full ring of integers $\mathcal{O}_K$.*

1. *If $r_{an}(E) = 0$, then $\mathrm{BSD}(E/\mathbb{Q}, p)$ is true for $p \geq 5$.*

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

   (a) *If $p \geq 3$ is split, then $\mathrm{BSD}(E/\mathbb{Q}, p)$ is true.*

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

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

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

We will prove this theorem in a sequence of smaller statements, beginning with a theorem of Rubin:

Theorem 2.11. *With $w = \#\mathcal{O}_K^\times$, 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*

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

   In other words, $\mathrm{BSD}(E/K, p)$ is true for $p \nmid w$.

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

Proof. [37] □

Corollary 2.12. *If E is defined over $\mathbb{Q}$, has complex multiplication and $r_{an}(E/\mathbb{Q})=0$, then $\mathrm{BSD}(E/\mathbb{Q},p)$ is true for all $p \geq 5$.*

Proof. Since $a_p(E)=0$ for primes p which are inert in K, and since these are exactly the primes where the twisting character is nontrivial, we have that

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

As Silverman notes in [44, p. 176], since E has complex multiplication it must be of additive reduction at all the bad primes. By [43, Cor. 15.2.1, p. 359] the Tamagawa product (not including archimedean primes) is at most 4. By Lemma 2.1, we have that $[E(K) : E(\mathbb{Q}) + E^D(\mathbb{Q})]$ is a power of two, hence the odd part of $\#E(K)_{\mathrm{tors}}$ is the square of the odd part of $\#E(\mathbb{Q})_{\mathrm{tors}}$. Lemma 2.2 shows that $c_\infty(E/K) = \Omega(E)^2$ up to a power of two since E is isogenous to E^D. (See Appendix B for the full statement of what BSD means for E/K, and in particular for a definition of $c_\infty(E/K)$.) Finally, by the exact sequence (2.1), $\mathrm{BSD}(E/\mathbb{Q},p)$ is equivalent to $\mathrm{BSD}(E/K,p)$ for odd primes$p$. By the first part of the theorem $\mathrm{BSD}(E/\mathbb{Q},p)$ is true for $p \nmid \#\mathcal{O}_K^\times$. Since K is quadratic imaginary, only 2 and 3 can divide $\#\mathcal{O}_K^\times$. □

Lemma 2.13. *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. [36, Lemma 21(i)] □

Lemma 2.14. $(\mathcal{O}_K/p\mathcal{O}_K)^\times \cong \mathrm{Aut}_{\mathcal{O}_K}(E[p])$.

Proof. Following unpublished work of A. Lum and W. Stein, let $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Then via the isomorphism $E[p] \cong \mathbb{F}_p^2$, the element α acts on $\mathbb{F}_p^2$ by a matrix $M \in \mathrm{GL}_2(\mathbb{F}_p)$. Then $\mathrm{Aut}_{\mathcal{O}_K}(E[p])$ is isomorphic to the centralizer of M in $\mathrm{GL}_2(\mathbb{F}_p)$. The centralizer of M is equal to the subgroup it generates since M cannot be a scalar element. In other words, we can make the identification $\mathrm{Aut}_{\mathcal{O}_K}(E[p]) = \langle\alpha\rangle$ by viewing α as an element of $\mathrm{Aut}(E[p])$. We define an isomorphism $\mathrm{Aut}_{\mathcal{O}_K}(E[p]) \to (\mathcal{O}_K/p\mathcal{O}_K)^\times$ by sending α^n to $\alpha^n + p\mathcal{O}_K \in (\mathcal{O}_K/p\mathcal{O}_K)^\times$. If $\alpha^n \in p\mathcal{O}_K$ then $M^n = 0$ in $\mathrm{GL}_2(\mathbb{F}_p)$, hence the map is injective. It is surjective since $\mathcal{O}_K = \mathbb{Z}[\alpha]$. □

Proposition 2.15. *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 2.13 $\#\mathrm{Gal}(K(E[p])/K) = p^2 - 1$. 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 $\#\mathrm{Aut}_{\mathcal{O}_K}(E[p]) = p^2 - 1$. By Lemma 2.14 this reduces to showing $\#(\mathcal{O}_K/p\mathcal{O}_K)^\times = p^2 - 1$ which is true since $[\mathcal{O}_K/p\mathcal{O}_K : \mathbb{Z}/p\mathbb{Z}] = 2$. □

2.4 Bounding the order of Ш$(\mathbb{Q}, E)$

Suppose $r_{\mathrm{an}}(E) \leq 1$ for $E/\mathbb{Q}$ and that K is a quadratic imaginary field satisfying the Heegner hypothesis for E with $I_K = [E(K) : \mathbb{Z}y_K]$. We have already seen that for analytic rank zero curves $\mathrm{BSD}(E/\mathbb{Q}, p)$ is true for primes $p > 3$ if E has complex multiplication. Otherwise we have the following theorem of Kato:

Theorem 2.16 (Kato)**.** *Suppose E is an optimal non-CM curve, and let p be a prime such that $p \nmid 6N(E)$ and $\rho_{E,p}$ is surjective. If $r_{an}(E) = 0$ then Ш$(\mathbb{Q}, E)$ is finite and*

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

Proof. [28] □

As a corollary to this theorem $\mathrm{BSD}(E/\mathbb{Q}, p)$ is true for primes $p > 3$ of good reduction where $E[p]$ is surjective and p does not divide $\#Ш(\mathbb{Q}, E)_{\mathrm{an}}$. Under certain technnical

conditions on p (explained in [21]), Grigorov has proven the bound on the other side:

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

Because Kato's theorem 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 $p > 3$ with $E[p]$ surjective then Kato's theorem 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 proven in Chapter 4). Kolyvagin's theorem still gives an upper bound in this case, provided we can get some kind of bound on the Heegner index. In the example above the methods of Section 2.5 show that $I_K \leq 23$, implying that $\mathrm{ord}_5(I_K) \leq 1$ and hence $\mathrm{ord}_5(\#Ш(\mathbb{Q},E)) \leq 2$.

Theorem 2.17 (Kolyvagin's inequality)**.** *If p is an odd prime unramified in the CM field such that $\overline{\rho}_{E,p}$ is surjective then*

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

We have the following alternative hypotheses which lead to the same result:

Theorem 2.18 (Cha)**.** *If $p \nmid 2 \cdot \Delta(K)$, $p^2 \nmid N(E)$ and $\overline{\rho}_{E,p}$ is irreducible then*

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

Proof. [11, 12] □

Theorem 2.19. *Suppose E is non-CM and p is an odd prime such that $p \nmid \#E'(\mathbb{Q})_{\mathrm{tors}}$ for any E' which is $\mathbb{Q}$-isogenous to E. If $\Delta(K)$ is divisible by exactly one prime, further suppose that $p \nmid \Delta(K)$. Then*

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

Proof. [22] □

Jetchev [27] has improved the upper bound with the following:

Theorem 2.20 (Jetchev)**.** *If the hypotheses of any of Theorems 2.17, 2.18 or 2.19 apply to p, then*

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

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

All the work done in Chapter 4 was originally inspired by the following result in [22]:

Theorem 2.21. *Suppose E is a non-CM elliptic curve over $\mathbb{Q}$ of* $\mathrm{rank}(E(\mathbb{Q})) \leq 1$ *and conductor $N(E) \leq 1000$, and p is a prime. If p is odd, suppose further that $\overline{\rho}_{E,p}$ is irreducible and p does not divide any Tamagawa number of E. Then* $\mathrm{BSD}(E/\mathbb{Q},p)$ *is true.*

Proof. In the paper [22], the authors used 2-descent to compute $\#Ш(\mathbb{Q},E)[2]$, and in the cases where this was nontrivial, they used 4-descent to prove that $Ш(\mathbb{Q},E)[2] = \#Ш(\mathbb{Q},E)[4]$. This gives the order of $Ш(\mathbb{Q},E)[2^\infty]$, which agrees with the conjectured order, thus proving $\mathrm{BSD}(E/\mathbb{Q},2)$ for each curve satisfying the hypothesis.

In the rank 1 case the authors used Theorem 2.17 when $\overline{\rho}_{E,p}$ is irreducible and surjective, leaving a set of pairs (E,p) such that $\overline{\rho}_{E,p}$ is irreducible but not surjective. The remaining cases all have $p^2 \mid N(E)$, so Theorem 2.18 does not apply. These are dealt with using Theorem 2.19.

In the rank 0 case, when $p \nmid 3N(E)$, the pairs (E,p) such that $\rho_{E,p}$ is not known to be surjective which satisfy the hypothesis is the single pair (608B, 5). Theorem 2.16 deals with all the other cases, and Theorem 2.18 handles (608B, 5).

In the general rank 0 case, Theorem 2.17 applies when $\overline{\rho}_{E,p}$ is surjective and $p \nmid I_K$, and Theorem 2.19 works for thirteen additional pairs. For the pairs (E,p) which are left, if $p \geq 5$ then $p \nmid N(E)$. Together with the previous paragraph, this shows that $\mathrm{BSD}(E/\mathbb{Q},p)$ is true if $p \neq 3$.

Finally, 3-descents prove all of the remaining cases except for 681B, where 3-descent shows that $Ш(\mathbb{Q},E)[3]$ is nontrivial. Then Theorem 2.17 with $D = -8$ proves that $\#Ш(\mathbb{Q},E)[3^\infty] \leq 9$, proving the last case. □

There is also an algorithm of Stein and Wuthrich based on the work of Kato, Perrin-Riou and Schneider (a preprint is available at [47] and the algorithm is implemented in

Sage [49]). Suppose that the elliptic curve E and the prime $p \neq 2$ are such that E does not have additive reduction at p and the image of $\overline{\rho}_{E,p}$ is either equal to the full group $\mathrm{GL}_2(\mathbb{F}_p)$ or is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. (We recall that a Borel subgroup is a maximal closed connected solvable subgroup. In $\mathrm{GL}_2(\mathbb{F}_p)$ these are subgroups which are conjugate to the group of upper triangular matrices. See [26, Section 21] for more details.) These conditions hold for all but finitely many p if E does not have complex multiplication. 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 $r_{\mathrm{an}}(E) \leq 1$, an error only happens when the p-adic height pairing can not be shown to be nondegenerate. For curves up to conductor 5000 of rank 0 or 1 this never happened for those p considered. Note that it is a standard conjecture that the p-adic height pairing is nondegenerate, 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 from below. In [17], Cremona and Mazur establish a method for visualizing pieces of Ш as pieces of Mordell-Weil groups via modular congruences, which is explained only in the appendix of [1]. 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 Ph.D. thesis [48].

2.5 The Heegner index

The main ingredient to applying Kolyvagin's work to a specific elliptic curve E of analytic rank at most 1 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 efficiently compute $\hat{h}(y_K)$ provably and to desired precision using the Gross-Zagier-Zhang formula (Theorem 2.3)), 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 2.1:

Corollary 2.22. *Suppose E is an elliptic curve of analytic rank 0 or 1 over $\mathbb{Q}$, in particular* $\operatorname{rank}(E(\mathbb{Q})) = r_{\mathrm{an}}(E(\mathbb{Q}))$. *Let $D < 0$ be a squarefree integer such that $K = \mathbb{Q}(\sqrt{D})$ satisfies the Heegner hypothesis for E.*

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

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

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-Pricket-Siksek height bound [15]. If there are no nontorsion points P on $E^D(\mathbb{Q})$ with naive absolute height*

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

then

$$I_K < M.$$

Note that this is a correction to the results stated in [22]. However, for each case in which [22] uses this result, the corresponding A is equal to 1. Therefore this mistake does not impact any of the other results there.

If $\operatorname{rank}(E(\mathbb{Q})) = 1$, 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 $\operatorname{rank}(E(\mathbb{Q})) = 0$ 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 $D^2N(E)$. However, a failed point search can still be useful as long as we search sufficiently hard, because of part 2 of the corollary.

Cremona and Siksek [16] describe an algorithm which allows the quick computation of the minimum height for a nontorsion point on an elliptic curve. This algorithm has been implemented in Sage [49] by Robert Bradshaw.

Theorem 2.23. *Suppose $r_{\mathrm{an}}(E/\mathbb{Q}) = 0$. If $E(\mathbb{Q})[2] = 0$ then let $A = 1$, otherwise let $A = 4$, and let $D < 0$ be a Heegner discriminant. There is an easily computed constant $H(E^D)$ such that if $z \in E^D(\mathbb{Q})$ is nontorsion then $\hat{h}(z) > H(E^D)$.*

Corollary 2.24. *With the same hypotheses,*

$$I_K < \sqrt{A \cdot \hat{h}(y_K)/H(E^D)}.$$

We will use this Corollary when a point search is infeasible, to at least give some bound on the order of the Shafarevich-Tate group. If we compute A, $\hat{h}(y_K)$ and $H(E^D)$ as above, then we let $S_1 = S_1(E, D, p)$ denote the largest nonnegative even integer such that $p^{S_1} < A \cdot \hat{h}(y_K)/H(E^D)$.

If the hypotheses of any of Theorems 2.17, 2.18 or 2.19 apply to p (and hence we can also use Theorem 2.20), then we will have

$$\mathrm{ord}_p(\#Ш(\mathbb{Q}, E)) \leq S_1 - 2 \max_{q|N(E)} \mathrm{ord}_p(c_q).$$

In the tables the quantity S will be equal to the right hand side of the above inequality. In particular, S will be an upper bound on the exponent of p in the order of $Ш(\mathbb{Q}, E)$.

Chapter 3

DESCENT

In studying the arithmetic of the abelian group $E(\mathbb{Q})$ it is natural to consider the map $[n] : E \longrightarrow E$, which is multiplication by an integer n. We can use this map to define the sequence

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{[n]} E \longrightarrow 0,$$

(where $E[n]$ denotes the kernel) which leads us to the descent sequence

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \xrightarrow{\delta} H^1(\mathbb{Q}, E[n]) \longrightarrow H^1(\mathbb{Q}, E)[n] \longrightarrow 0,$$

via the long exact sequence of Galois cohomology.

By localizing at all primes p, we obtain the commutative diagram with exact rows which is used to define the n-Selmer group and the Shafarevich-Tate group:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(\mathbb{Q})/nE(\mathbb{Q}) & \xrightarrow{\delta} & H^1(\mathbb{Q}, E[n]) & \longrightarrow & H^1(\mathbb{Q}, E)[n] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & \searrow^{\alpha} & \downarrow & & \\
0 & \longrightarrow & \prod_p E(\mathbb{Q}_p)/nE(\mathbb{Q}_p) & \xrightarrow{\delta} & \prod_p H^1(\mathbb{Q}_p, E[n]) & \longrightarrow & \prod_p H^1(\mathbb{Q}_p, E)[n] & \longrightarrow & 0.
\end{array}$$

Recall that the n-Selmer group $\mathrm{Sel}^{(n)}(\mathbb{Q}, E)$ is the kernel of the map α. If $\phi : E \longrightarrow E'$ is an isogeny of degree n over a number field K, we obtain the analogous diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E'(K)/\phi E(K) & \xrightarrow{\delta} & H^1(K, E[\phi]) & \longrightarrow & H^1(K, E)[\phi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & \searrow^{\alpha} & \downarrow & & \\
0 & \longrightarrow & \prod_{\mathfrak{p}} E'(K_{\mathfrak{p}})/\phi E(K_{\mathfrak{p}}) & \xrightarrow{\delta} & \prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}}, E[\phi]) & \longrightarrow & \prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}}, E)[\phi] & \longrightarrow & 0.
\end{array}$$

The ϕ-Selmer group $\mathrm{Sel}^{(\phi)}(K,E)$ is the kernel of the map α and the image of δ is contained in it, by exactness of the bottom row and commutativity. By the definition of the Shafarevich-Tate group, we obtain the short exact *descent sequence:*

$$0 \longrightarrow E'(K)/\phi E(K) \xrightarrow{\delta} \mathrm{Sel}^{(\phi)}(K,E) \longrightarrow Ш(K,E)[\phi] \longrightarrow 0.$$

To see how the various Selmer and Shafarevich-Tate groups relate to each other under an isogeny, suppose $\phi : E \longrightarrow E'$ has prime degree p, let $\phi' : E' \longrightarrow E$ denote the dual isogeny and consider the diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E[\phi] & \longrightarrow & E & \xrightarrow{\phi} & E' & \longrightarrow & 0 \\
 & & \downarrow & & \| & & \downarrow{\scriptstyle \phi'} & & \\
0 & \longrightarrow & E[p] & \longrightarrow & E & \xrightarrow{[p]} & E & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} & & \| & & \\
0 & \longrightarrow & E'[\phi'] & \longrightarrow & E' & \xrightarrow{\phi'} & E & \longrightarrow & 0.
\end{array}$$

By taking long exact sequences and truncating, we obtain

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E'(K)/\phi E(K) & \xrightarrow{\delta_\phi} & H^1(K,E[\phi]) & \longrightarrow & H^1(K,E)[\phi] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \phi'} & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta_{[p]}} & H^1(K,E[p]) & \longrightarrow & H^1(K,E)[p] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{id}_{E(K)}} & & \downarrow{\scriptstyle \phi^*} & & \downarrow{\scriptstyle \phi^*} & & \\
0 & \longrightarrow & E(K)/\phi' E'(K) & \xrightarrow{\delta_{\phi'}} & H^1(K,E'[\phi']) & \longrightarrow & H^1(K,E')[\phi'] & \longrightarrow & 0.
\end{array}$$

By restricting to the Selmer groups, we obtain

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E'(K)/\phi E(K) & \xrightarrow{\delta_\phi} & \mathrm{Sel}^{(\phi)}(K,E) & \longrightarrow & Ш(K,E)[\phi] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \phi'} & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E(K)/pE(K) & \xrightarrow{\delta_{[p]}} & \mathrm{Sel}^{(p)}(K,E) & \longrightarrow & Ш(K,E)[p] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \phi^*} & & \downarrow{\scriptstyle \phi^*} & & \\
0 & \longrightarrow & E(K)/\phi' E'(K) & \xrightarrow{\delta_{\phi'}} & \mathrm{Sel}^{(\phi')}(K,E') & \longrightarrow & Ш(K,E')[\phi'] & \longrightarrow & 0.
\end{array}$$

In [38] (Lemma 9.1), the authors use this diagram to show that the following sequence is exact:

$$\begin{array}{ccccccc}
0 & \longrightarrow & E'(K)[\phi']/\phi(E(K)[p]) & & & & \\
 & \searrow & & & & & \\
 & & \mathrm{Sel}^{(\phi)}(K,E) & \longrightarrow & \mathrm{Sel}^{(p)}(K,E) & \longrightarrow & \mathrm{Sel}^{(\phi')}(K,E) \\
 & & & \searrow & & & \\
 & & & & Ш(K,E')[\phi']/\phi^*(Ш(K,E)[p]) & \longrightarrow & 0.
\end{array}$$

Let us consider the ϕ-descent sequence more concretely:

$$E'(K)/\phi(E(K)) \xhookrightarrow{\delta_\phi} \mathrm{Sel}^{(\phi)}(K,E) \xrightarrow{\pi} Ш(K,E)[\phi^*].$$

The map δ_ϕ is the connecting homomorphism from Galois cohomology. If $P \in E'(K)$, choose a $Q \in E(\overline{K})$ such that $\phi(Q) = P$. Then $\delta_\phi(P) \in H^1(K, E[\phi])$ is represented by $\xi_Q : G_K \to E[\phi]$, where

$$\xi_Q(\sigma) = \sigma Q - Q, \text{ for all } \sigma \in G_K.$$

A simple diagram chase will tell us that by the definition of $\mathrm{Sel}^{(\phi)}(K,E)$, the image of δ lies inside $\mathrm{Sel}^{(\phi)}(K,E)$. The map π comes from the natural surjection $H^1(K,E[\phi]) \twoheadrightarrow H^1(K,E)[\phi]$. For $[\xi] \in \mathrm{Sel}^{(\phi)}(K,E)$, ξ is a map $G_K \to E[\phi]$ and $\pi([\xi])$ is represented by the composition $G_K \xrightarrow{\xi} E[\phi] \hookrightarrow E$.

Recall that for M a G_K-module, ν a place of K, and $I_\nu \subset G_K$ its inertia group, a cohomology class $\xi \in H^i(K, M) = H^i(G_K, M)$ is said to be *unramified* at ν if it is trivial under the natural map $H^i(G_K, M) \to H^i(I_\nu, M)$. For S a finite set of places of K and M a finite abelian G_K module, we define $H^1(K, M; S)$ to be the set of $\xi \in H^1(K, M)$ such that ξ is unramified outside of S. In fact, this is a finite set [43, ch. X, Lemma 4.3].

Theorem 3.1. *If S is a set of places of K containing infinite places, places at which E has bad reduction, and places dividing* $\deg(\phi)$*, then*

$$\mathrm{Sel}^{(\phi)}(K, E) \subseteq H^1(K, E[\phi]; S).$$

Proof. [43, ch. X, Corollary 4.4] □

Definition. If E/K is an elliptic curve, a *principal homogeneous space* for E/K is a smooth curve C/K together with a simply transitive algebraic group action of E on C defined over K.

For $p \in C$ and $P \in E$, we write the image of P under this action as $p + P$. In this notation, simply transitive means that the equation $p + P = q$ for $p, q \in C$ always has a unique solution P, hence we may also write $P = p - q$. Picking a $p_0 \in C$ gives an isomorphism $\theta : E \to C : P \mapsto p_0 + P$, defined over $K(p_0)$, thus C is a twist of E, and if C has a point defined over K, then C is isomorphic to E over K. Two homogeneous spaces are said to be *equivalent* if they are isomorphic over K such that the isomorphism is compatible with the action of E on each.

Definition. The *Weil-Châtelet* group $WC(E/K)$ is the collection of equivalence classes of homogeneous spaces for E over K.

The set $WC(E/K)$ is a group by the bijection $WC(E/K) \leftrightarrow H^1(K, E)$ defined as follows: for $\{C/K\} \in WC(E/K)$, choose any $p_0 \in C$ and define $\{\sigma \mapsto p_0^\sigma - p_0\}$ to be the corresponding cocycle in $H^1(K, E)$. In fact, C/K is in the trivial class if and only if $C(K)$ is not empty, and $\mathrm{Pic}^0(C)$ can be canonically identified with E via the "summation map," defined by $\mathrm{Div}^0(C) \to E : \sum n_i(p_i) \mapsto \sum [n_i](p_i - p_0)$, which is independent of the choice of

$p_0 \in C$. We identify $WC(E/K) = H^1(K, E)$, and under this identification, one can think of $Ш(E/K)$ as the group of equivalence classes of homogeneous spaces for E/K which have K_ν-rational points for every place ν of K. Under this light, a nontrivial element of $Ш(E/K)$ will correspond to a failure of the Hasse principle for some homogeneous space which has points over each completion K_ν, yet no points over K itself.

3.1 Implementations of descents

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 [5] together with an impressive 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 are called quartic covers of the elliptic curve. It is very well described in [13], as long as one is also aware of the various improvements and clarifications: [14] works out computing equivalence of the involved quartics, [18] completes the classification of minimal models begun in [5] at $p = 2$ and even this was further refined in certain cases by [39] and [42] includes an asymptotic improvement over [5] 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 2) is documented mostly in slides titled "Higher Descents on Elliptic Curves" on Cremona's website[1], as well as some unpublished notes he was kind enough to share.

There is also Denis Simon's `gp` [4] script, which has been incorporated into Sage. It computes the same information as `mwrank`, but via what is called the "number field method." For more of the flavor of this approach, see section 3.2.

The 2-descent methods in Magma [8] were written mostly by Geoff Bailey. Magma's 4-descent routines are based on [32] and [55], 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 [45], and the homogeneous spaces are intersections of three quartics.

---

[1] `http://www.warwick.ac.uk/~masgaj/`

Jeechul Woo, a 2010 Ph.D. student of Noam Elkies, has implemented a `gp` script (which has been ported to Sage [49] but not yet merged as of this writing) for doing 3-isogeny descents when the curve has a rational 3-torsion point, based on [56].

3.2 Schaefer-Stoll

For D an étale algebra over K, define

$$D(S,m) = \{\alpha \in D^\times/(D^\times)^m : \alpha \text{ is unramified outside of } S\},$$

where we say that $\alpha \in D^\times$ is unramified at ν if the extension of étale K-algebras $D(\sqrt[p]{\alpha})/D$ is unramified at all places of D lying above ν.

Note that if $E[m] \subset E(K)$, we have that $\mu_m \subset K^\times$. Then $E[m] \cong (\mu_m)^2$ as trivial G_K-modules, hence $H^1(K, E[m]) \cong H^1(K, (\mu_m)^2) = \mathrm{Hom}(G_K, \mu_m)^2$. Hilbert's theorem 90 implies that $\delta_K : K^\times/(K^\times)^m \to \mathrm{Hom}(G_K, \mu_m)$ is an isomorphism. Then in this case we have

$$H^1(K, E[m]; S) \cong K(S,m) \times K(S,m).$$

We can then use this isomorphism to enumerate elements of $H^1(K, E[m]; S)$, and for each element ξ, determine whether it is in the m-Selmer group. This is done by taking a corresponding principal homogeneous space C/K in the Weil-Châtelet group, and checking whether $C(K_\nu) \neq \varnothing$ for each $\nu \in S$. This demonstrates the effectiveness of the method to compute the m-Selmer group, but often we do not need to extend K so that $E[m] \subset E(K)$, since other similar methods are available.

For the following, assume p is an odd prime, and again that $\phi : E \longrightarrow E'$ is an isogeny over K with kernel $E[\phi]$ of prime exponent p. We have the following improvement to Theorem 3.1:

Theorem 3.2. *If S is a finite set of places of K containing the places above p and the places ν such that at least one of the Tamagawa numbers $c_{E,\nu}$ or $c_{E',\nu}$ is divisible by p, then*

$$\mathrm{Sel}^{(\phi)}(K,E) \subseteq H^1(K, E[\phi]; S).$$

If we consider the following diagram:

$$\begin{array}{ccc} E'(K)/\phi(E(K)) & \xrightarrow{\delta_\phi} & H^1(K, E[\phi]; S) \\ \downarrow{\scriptstyle \prod_{\nu\in S} \mathrm{res}_\nu} & & \downarrow{\scriptstyle \prod_{\nu\in S} \mathrm{res}_\nu} \\ \prod_{\nu\in S} E'(K_\nu)/\phi(E(K_\nu)) & \xrightarrow{\prod_{\nu\in S} \delta_{\phi,\nu}} & \prod_{\nu\in S} H^1(K_\nu, E[\phi_\nu]), \end{array}$$

we may reformulate the definition of the Selmer group as follows:

$$\mathrm{Sel}^{(\phi)}(K, E) = \{\xi \in H^1(K, E[\phi]; S) : \mathrm{res}_\nu(\xi) \in \mathrm{im}\delta_{\phi,\nu} \text{ for all } \nu \in S\}.$$

Proof. [38, Prop. 4.6] □

From now on, let us suppose S satisfies the hypothesis of Theorem 3.2. Following [38], let $\phi' : E' \to E$ be the dual isogeny of ϕ and let X be a Galois-invariant subset of $E'[\phi'] \setminus \{\mathcal{O}\}$ which spans $E'[\phi']$. Considering X as a finite étale subscheme of E', let D be the finite étale K-algebra corresponding to X. The étale algebra $D = \prod_{i=1}^m D_i$ decomposes as a product of finite extensions D_i of K. If $\alpha = (\alpha_1, ..., \alpha_m)$ we say that $D(\sqrt[p]{\alpha})/D$ is unramified at a prime $\mathfrak{p} = (\mathfrak{p}_1, ..., \mathfrak{p}_m)$ if each $D_i(\sqrt[p]{\alpha_i})/D_i$ is unramified at $\mathfrak{p}_i$. Here we say $\mathfrak{p}$ lies above ν if each $\mathfrak{p}_i$ lies above ν.

Note that we can use algorithms for computing S-class groups Cl_S and S-units U_S in the number fields D_i to compute $D(S, n) = \prod_{i=1}^m D_i(S, n)$ via the exact sequences

$$1 \to U_S(D_i)/U_S(D_i)^n \to D_i(S, n) \to \mathrm{Cl}_S(D_i)[n] \to 1.$$

Next, we use the Weil pairing $e_\phi : E[\phi] \times E'[\phi'] \to \mu_p$ together with the Kummer isomorphism $k : H^1(K, \mu_p(\overline{D})) \to D^\times/(D^\times)^p$. The Weil pairing induces an injection $w_\phi : E[\phi] \to \mu_p(\overline{D}) = \{X(\overline{K}) \to \mu_p\}$ taking P to $e_\phi(P, \cdot)$. If the induced map $w_\phi^* : H^1(K, E[\phi]) \to H^1(K, \mu_p(\overline{D}))$ is injective (both globally and locally in S), then we may form the following diagram, and transfer computations in $H^1(K, E[\phi]; S)$ to computations in $D(S, p)$:

$$\begin{array}{ccccc}
E'(K)/\phi(E(K)) & \xrightarrow{\delta_\phi} & H^1(K, E[\phi]; S) & \xrightarrow{k \circ w_\phi^*} & D(S,p) \\
\downarrow{\scriptstyle \prod_{\nu\in S} \mathrm{res}_\nu} & & \downarrow{\scriptstyle \prod_{\nu\in S} \mathrm{res}_\nu} & & \downarrow{\scriptstyle \prod_{\nu\in S} \mathrm{res}_\nu} \\
\prod_{\nu\in S} E'(K_\nu)/\phi(E(K_\nu)) & \xrightarrow{\prod_{\nu\in S} \delta_{\phi,\nu}} & \prod_{\nu\in S} H^1(K_\nu, E[\phi_\nu]) & \xrightarrow{\prod_{\nu\in S} k_\nu \circ w_{\phi,\nu}^*} & \prod_{\nu\in S} D_\nu^\times/(D_\nu^\times)^p
\end{array}$$

Under this new diagram, we have

$$\mathrm{Sel}^{(\phi)}(K,E) \cong \{\alpha \in \mathrm{im}(k \circ w_\phi^*) : \mathrm{res}_\nu(\alpha) \in \mathrm{im}(k_\nu \circ w_{\phi,\nu}^* \circ \delta_{\phi,\nu}) \text{ for all } \nu \in S\}.$$

This description of the ϕ-Selmer group depends on w_ϕ^* being injective globally and locally for $\nu \in S$. If $\phi = [p]$ and $G = \mathrm{Gal}(K(E[p])/K)$, then this is the case if $p \nmid \#G$ or $p \nmid \#X$ [38, Prop. 6.4]. In particular, if we set $X = E[p] \setminus \{\mathcal{O}\}$, then $p \nmid \#X = p^2 - 1$. If we partition X into orbits under the G_K-action, we need only take a union of orbits which spans $E[p]$ such that p does not divide its order.

To make this description of the Selmer group more effective, define $F : E' \to \overline{D}$ as follows. For each $P \in X$, choose a function f_P in $K(P)(E')$ with divisor $\mathrm{div}(f_P) = pP - p\mathcal{O}$ such that for $\sigma \in G_K$ we have $\sigma f_P = f_{\sigma P}$. Then F is the rational function from E' to $\overline{D}$ which sends a point R to the function $P \mapsto f_P(R)$. We call a degree-0 divisor on E' over K *good* if its support avoids $X \cup \{\mathcal{O}\}$. Every point of $E'(K)$ can be represented by a good divisor, and we can evaluate F on a good divisor $\sum_j n_j Q_j$ to find $\prod_j F(Q_j)^{n_j} \in D^\times$. By evaluating on good divisors, F induces a well-defined map from $E'(K)/\phi(E(K))$ to $D(S,p)$ which turns out to be equal to the composition $k \circ w_\phi^* \circ \delta_\phi$. Under this new notation, we have

$$\begin{array}{ccc}
E'(K)/\phi(E(K)) & \xrightarrow{F} & D(S,p) \\
\downarrow{\scriptstyle \prod_{\nu\in S} \mathrm{res}_\nu} & & \downarrow{\scriptstyle \prod_{\nu\in S} \mathrm{res}_\nu} \\
\prod_{\nu\in S} E'(K_\nu)/\phi(E(K_\nu)) & \xrightarrow{\prod_{\nu\in S} F_\nu} & \prod_{\nu\in S} D_\nu^\times/(D_\nu^\times)^p,
\end{array}$$

and

$$\mathrm{Sel}^{(\phi)}(K,E) \cong \{\alpha \in \mathrm{im}(k \circ w_\phi^*) : \mathrm{res}_\nu(\alpha) \in F_\nu(E'(K_\nu)/\phi(E(K_\nu))) \text{ for all } \nu \in S\}.$$

To compute the Selmer group using this description we must be able to find the image of $F_\nu(E'(K_\nu))$ in $D_\nu^\times/(D_\nu^\times)^p$, for $\nu \in S$. Work in [38] allows us to find the size of $E'(K_\nu)/\phi(E(K_\nu))$, which involves computing the norm of the leading coefficient of the power series representation of ϕ on formal groups when $\phi \neq [p]$. Once we know the size, we can search for good divisors defined over K_ν whose classes span the group. Using F_v, it is typically easier to compute independence in $D_\nu^\times/(D_\nu^\times)^p$.

Suppose we have an étale algebra D/K corresponding to a G_K-set X with GL_2-action. Further assume that the stabilizers in $\mathrm{GL}_2(\mathbb{F}_p)$ of points in X meet the center trivially. Then by [38, Lemma 7.2] there is an étale subalgebra D_+ of D corresponding to the orbits in X of the center $\mathbb{F}_p^\times$ of $\mathrm{GL}_2(\mathbb{F}_p)$, and D/D_+ is a cyclic extension of degree $p-1$. Let $\mu_p(\overline{D})^{(1)}$ denote the submodule of $\mu_p(\overline{D})$ consisting of elements for which the action of a central element $\alpha \in \mathbb{F}_p^\times$ is multiplication by α.

The last remaining step is computing $\mathrm{im}(k \circ w_\phi^*)$ in $D(S,p)$. We do so in the generic case $\phi = [p]$, $X = E[p] \setminus \{\mathcal{O}\}$. Let A denote the étale algebra corresponding to $X = E[p] \setminus \{\mathcal{O}\}$ (here we are following the notation of [38], so D will now become A, and D will assume a new role below), and let B denote the étale algebra corresponding to the set of affine lines in $E[p]$ avoiding the origin, i.e., corresponding to $E[p]^\vee \setminus \{\mathcal{O}\}$, where $E[p]^\vee = \mathrm{Hom}(E[p], \mathbb{Z}/p\mathbb{Z})$. We let Y denote the G_K-set of pairs $(P,\ell) \in E[p] \setminus \{\mathcal{O}\} \times E[p]^\vee \setminus \{\mathcal{O}\}$, and let D denote the étale algebra corresponding to Y. Let g be a primitive root mod p and σ_g the automorphism of A/A_+ corresponding to the action of g on X.

Theorem 3.3. *We have the following exact sequence:*

$$0 \longrightarrow E[p] \xrightarrow{w_p} \mu_p(\overline{A})^{(1)} \xrightarrow{u} \mu_p(\overline{B})^{(1)} \xrightarrow{w_p^\vee} E[p]^\vee \otimes \mu_p \longrightarrow 0,$$

where u is defined by

$$\varphi \mapsto \left(\ell \mapsto \prod_{P \in \ell} \varphi(P) \right).$$

Furthermore, the sequence

$$0 \longrightarrow H^1(K, E[p]) \xrightarrow{\overline{w}_p} H^1(K, \mu_p(\overline{A})^{(1)}) \xrightarrow{\overline{u}} H^1(K, \mu_p(\overline{B})^{(1)})$$

is also exact.

$$H^1(K, E[p]) \cong \ker\left(g - \sigma_g : A^\times/(A^\times)^p \to A^\times/(A^\times)^p\right) \cap \ker(\overline{u}),$$

and $\overline{u} : A^\times/(A^\times)^p \to B^\times/(B^\times)^p$ *is induced by the composition*

$$\mathrm{Norm}_{D/B} \circ \iota_{(A \hookrightarrow D)} : A \to B.$$

Proof. [38] □

Corollary 3.4.

$$\mathrm{Sel}^{(p)}(K, E) \cong \{\xi \in A(S, p) : \mathrm{res}_\nu(\xi) \in \mathrm{im} F_\nu \text{ for all } \nu \in S\}.$$

Michael Stoll has kindly provided some unpublished notes regarding the special case of an isogeny of prime degree, which can be useful to prove that $Ш(\mathbb{Q}, E)[\ell] = 0$ when $E[\ell]$ is reducible. These notes consider a degree ℓ isogeny $\phi : E \longrightarrow E'$ over $\mathbb{Q}$ where either $\ell > 3$ or $\ell = 3$ and E has no special fibers of Kodaira type IV or IV* and normalized so that $E[\phi]$ contains real points. In [38], the set of usual primes to consider is restricted to $\{\ell\} \cup \{p : \ell | c_p(E)c_p(E')\}$. If $\ell | c_p(E)c_p(E')$ then both curves have split multiplicative reduction at p, and there are two cases: $c_p(E) = \ell c_p(E')$ or $c_p(E') = \ell c_p(E)$.

Proposition 3.5. *If* $p \neq \ell$ *and* $c_p(E') = \ell c_p(E)$*, then* F_p *has trivial image and the local condition in Corollary 3.4 becomes that* $\mathrm{res}_p(\xi)$ *is trivial.*

If $p \neq \ell$ *and* $c_p(E) = \ell c_p(E')$*, then* F_p *is surjective so the condition is vacuous.*

Proof. (Stoll's notes) □

If $p = \ell$ then either $\Omega(E) = \Omega(E')$ or $\Omega(E) = \ell\Omega(E')$, so let $w \in \{0, 1\}$ be such that $\Omega(E) = \ell^w \Omega(E')$. In the first case, ϕ' is an isomorphism on the kernels of reduction, otherwise ϕ is. Stoll proves that

Proposition 3.6. *If* $E[\phi](\mathbb{Q}_\ell) = 0 = E'[\phi'](\mathbb{Q}_\ell)$*, then*

$$\mathrm{Sel}^{(\phi')}(\mathbb{Q}, E') \cong \ker \alpha \text{ and } \mathrm{Sel}^{(\phi)}(\mathbb{Q}, E) \cong \ker \beta,$$

where if $w = 0$*,*

$$\alpha : K(S_1, \ell)^{(1)} \longrightarrow K(S_2 \cup \{\ell\}, \ell)^* \text{ and } \beta : K'(S_2, \ell)^{(1)} \longrightarrow K'(S_1, \ell)^*$$

are the canonical maps and if $w = 1$*,*

$$\alpha : K(S_1, \ell)^{(1)} \longrightarrow K(S_2, \ell)^* \text{ and } \beta : K'(S_2, \ell)^{(1)} \longrightarrow K'(S_1 \cup \{\ell\}, \ell)^*.$$

Further unraveling of notation is necessary for the above proposition to make sense.

- K is the field of definition of any point in $E[\phi]$ and similarly for K'.
- $S_1 = \{p : c_p(E) = \ell c_p(E')\}$ and $S_2 = \{p : c_p(E') = \ell c_p(E)\}$.
- $K(S,\ell)^{(1)}$ is defined above, and

$$K(S,\ell)^* = \prod_{p\in S} \frac{\mathcal{O}_{K,p}^\times}{(\mathcal{O}_{K,p}^\times)^\ell},$$

  where $\mathcal{O}_{K,p} = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

Corollary 3.7. *With the same hypotheses, assume that the class numbers of K and K' are not divisible by ℓ. Then we have*

$$\#S_1 + w - \#S_2 \leq \dim \ker \alpha \leq \#S_1 + 1$$

and

$$\#S_2 - (\#S_1 + w) \leq \dim \ker \beta \leq \#S_2.$$

Proof. From Stoll's notes, we have $\dim K(S_1,\ell)^{(1)} = \#S_1 + 1$, $(\dim K(S_2,\ell)^*)^{(1)} = \#S_2$, $\dim K'(S_2,\ell)^{(1)} = \#S_2$, and $(\dim K'(S_1,\ell)^*)^{(1)} = \#S_1$. □

On the other hand, if $E'[\phi'](\mathbb{Q}_\ell) \neq 0$ and $w = 1$ then the maps to consider are instead

$$\alpha : K(S_1 \cup \{\ell\},\ell)^{(1)} \longrightarrow K(S_2,\ell)^* \text{ and } \beta : K'(S_2,\ell)^{(1)} \longrightarrow K'(S_1 \cup \{\ell\},\ell)^*.$$

If $w = 0$, then an easy description of β is:

$$\beta : K'(S_2,\ell)^{(1)} \longrightarrow K'(S_1,\ell)^*.$$

We do not have at present a similar description of α in this case, apart from considering the image of F_ℓ explicitly.

In the cases where α and β are defined, we have

$$\max\left\{ \dim Ш(\mathbb{Q},E)[\ell],\ \dim Ш(\mathbb{Q},E')[\ell] \right\} \leq \dim \ker \alpha + \dim \ker \beta - \operatorname{rank}(E(\mathbb{Q})).$$

3.3 The primes $p = 2$ and $p = 3$

Theorem 3.8. *If $E/\mathbb{Q}$ has conductor $N(E) < 5000$, then $\mathrm{BSD}(E/\mathbb{Q}, 2)$ is true.*

Proof. Assume that E is an optimal curve and let $T(E) = \mathrm{ord}_2(\#Ш(\mathbb{Q}, E)_{\mathrm{an}})$. If $T(E) = 0$ then a 2-descent proved $\mathrm{BSD}(E/\mathbb{Q}, 2)$ and if $T(E) > 0$ then a 2-descent proved $Ш(\mathbb{Q}, E)[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If $T(E) = 2$ then a 4-descent proved $\mathrm{BSD}(E/\mathbb{Q}, 2)$ and if $T(E) > 2$ then a 4-descent proved $Ш(\mathbb{Q}, E)[4] \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. For the range of curves considered $T(E)$ was at most 4 and in the case where $T(E) = 4$, an 8-descent proved that $Ш(\mathbb{Q}, E)[8] = Ш(\mathbb{Q}, E)[4]$ and hence proved $\mathrm{BSD}(E/\mathbb{Q}, 2)$. The truth of $\mathrm{BSD}(E/\mathbb{Q}, p)$ is independent of the isogeny class of E and every isogeny class contains an optimal curve. □

Theorem 3.9. *If $E/\mathbb{Q}$ has conductor $N(E) < 5000$, then $\mathrm{BSD}(E/\mathbb{Q}, 3)$ is true.*

Proof. For optimal curves where $\mathrm{ord}_3(\#Ш(\mathbb{Q}, E)_{\mathrm{an}}) = 0$, a 3-descent proved $\mathrm{BSD}(E/\mathbb{Q}, 3)$. For the rest we have $\mathrm{ord}_3(\#Ш(\mathbb{Q}, E)_{\mathrm{an}}) = 2$, and in this case a 3-descent proved that $Ш(\mathbb{Q}, E)[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. These 31 remaining optimal curves are shown in Table A.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 [47] proves the desired upper bound. For the rest of the curves except for 2366d1 and 4914n1, the mod-3 representations are surjective. Table A.4 displays selected Heegner indexes in this case, which together with Kolyvagin (and Jetchev for 4675j1 since $c_{17}(4675\mathrm{j}1) = 3$) 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 $\mathrm{BSD}(F/\mathbb{Q}, 3)$ for both curves. By Theorem B.3, $\mathrm{BSD}(E/\mathbb{Q}, 3)$ only depends on the isogeny class of E, hence the claim is proved. □

Corollary 3.10. *If $\mathrm{rank}(E(\mathbb{Q})) = 0$, E has conductor $N(E) < 5000$ and E has complex multiplication, then the full BSD conjecture is true.*

Chapter 4

CURVES OF CONDUCTOR $N < 5000$

There are 17314 isogeny classes of elliptic curves of conductor up to 5000. There are 7914 of rank 0, 8811 of rank 1 and 589 of rank 2. There are none of higher rank. There are only 116 optimal curves which have complex multiplication in this conductor range. Every rank 2 curve in this range has $\#Ш(\mathbb{Q}, E)_{\text{an}} = 1$. For any curve E in this range, $\text{ord}_p(Ш(\mathbb{Q}, E)_{\text{an}}) \leq 6$ for all primes p. If such an E is optimal then $\text{ord}_p(Ш(\mathbb{Q}, E)_{\text{an}}) \leq 4$ for all primes p. Table A.1 shows how many curves have nontrivial $Ш_{\text{an}}$ at each prime, and what the exponent of that prime is.

4.1 Optimal curves with nontrivial $\#Ш(\mathbb{Q}, E)_{an}$

Theorem 4.1. *If $E/\mathbb{Q}$ is an optimal curve with conductor $N(E) < 5000$ and $\#Ш(\mathbb{Q}, E)_{an} \neq 1$, then for every $p \mid \#Ш(\mathbb{Q}, E)_{an}$, $\text{BSD}(E/\mathbb{Q}, p)$ is true.*

Proof. By table A.1 we have that $p \leq 7$, and by the theorems of the previous section, we may assume that $p \geq 5$.

For $p = 5$, E is one of the twelve curves listed in table A.5. These are all rank 0 curves with $E[5]$ surjective, so if $5 \nmid N(E)$ Kato's theorem 2.16 provides an upper bound of 2 for $\text{ord}_5(\#Ш(\mathbb{Q}, E))$. This leaves just 2900d1 and 3185c1. For 2900d1, Corollary 2.22 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 [47] provides the upper bound of 2. In all twelve cases [17] (and the appendix of [1]) finds visible nontrivial 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 $E = 3364\text{c}1$ and $E[7]$ is surjective. Since $7 \nmid 3364$ and E is a rank 0 curve without complex multiplication, Kato's theorem 2.16 bounds $\text{ord}_7(\#Ш(\mathbb{Q}, E))$ from above by 2. Furthermore, Grigorov's thesis [21, p. 88] shows that

$\mathrm{ord}_7(\#Ш(\mathbb{Q}, E))$ is bounded from below by 2. □

Note: In fact computations show that if E is any (not necessarily optimal) curve with conductor $N(E) < 5000$ and $\mathrm{ord}_p(\#Ш(\mathbb{Q}, E)_{\mathrm{an}}) \neq 0$, then $\mathrm{BSD}(E/\mathbb{Q}, p)$ is true except for the isogeny classes in Table A.6. All of these curve-prime pairs (E, p) have $E[p]$ reducible, and this will be discussed in Section 4.4.

4.2 Rank 0 curves and irreducible mod-p representations

Theorem 4.2. *If $E/\mathbb{Q}$ is an optimal rank 0 curve with conductor $N(E) < 5000$ and p is a prime such that $E[p]$ is surjective and E does not have additive reduction at p, then* $\mathrm{BSD}(E/\mathbb{Q}, p)$ *is true.*

The hypothesis that E does not have additive reduction at p is addressed in Section 4.5.

Proof. By theorems of the previous two sections, we may assume that $p > 3$, E does not have complex multiplication and $\mathrm{ord}_p(\#Ш(\mathbb{Q}, E)_{\mathrm{an}}) = 0$. In this case Kato's theorem applies to E (since the rank part of the conjecture is known for $N(E) < 130000$), and since $E[p]$ is surjective and $p > 3$, we need only consider primes dividing the conductor $N(E)$.

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 $\mathrm{BSD}(E/\mathbb{Q}, p)$ using the first available Heegner discriminant, the algorithm of Stein and Wuthrich [47] 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 a surjective prime of non-additive reduction and E is rank 0. □

For example if E = 1050c1, the first available Heegner index is -311. Bounding the Heegner index is difficult in this case since it involves point searches of prohibitive height. 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.

Theorem 4.3. *If $E/\mathbb{Q}$ is an optimal rank 0 curve with conductor $N(E) < 5000$, $E[p]$ is irreducible and E is not of additive reduction at p, then* $\mathrm{BSD}(E/\mathbb{Q}, p)$ *is true.*

Proof. By the previous theorem we need only consider primes p such that $E[p]$ is not surjective. Similarly we can assume that $p > 3$, $\mathrm{ord}_p(\#Ш(\mathbb{Q}, E)_{\mathrm{an}}) = 0$ and that E does not have complex multiplication. The curve-prime pairs matching these hypotheses can be found in Table A.7 along with selected Heegner indices. The only prime to occur in these pairs is 5, and each chosen Heegner discriminant and index is not divisible by 5 except $E =$ 3468h. Further, 5 does not divide the conductor of any of these curves so by Cha's theorem 2.18, $\mathrm{BSD}(E/\mathbb{Q}, 5)$ is true for these pairs. For $E =$ 3468h note that one of the Tamagawa numbers is 5, so by Theorem 2.20, $\mathrm{BSD}(E/\mathbb{Q}, 5)$ is true for this curve. □

4.3 Rank 1 curves and irreducible mod-p representations

Theorem 4.4. *If $E/\mathbb{Q}$ is a rank 1 curve with conductor $N(E) < 5000$, p is a prime such that $E[p]$ is irreducible, E does not have additive reduction at p and $(E, p) \neq (1155k, 7)$, then* $\mathrm{BSD}(E/\mathbb{Q}, p)$ *is true.*

Note that for $(E, p) = (1155\mathrm{k}, 7)$, we have $c_3(E) = 7, c_5(E) = 7$,

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

by Jetchev's improvement to Kolyvagin's theorem. We may also replace the hypothesis that E does not have additive reduction at p with the hypothesis that E does not have complex multiplication and E does not have additive reduction at p, since .

Proof. We may assume in addition that E is optimal, since reducibility and additive reduction are isogeny-invariant. By Theorems 3.8 and 3.9, if $p < 5$ then $\mathrm{BSD}(E/\mathbb{Q}, p)$ is true. Thus we may assume $p \geq 5$. Computing the Heegner index is much easier when E has rank 1, as noted in Section 2.5. Kolyvagin's theorem then rules out many pairs (E, p) right away. Then some combination of Theorems 2.19, 2.18, 2.20 and the algorithm of Stein and Wuthrich [47] will rule out many more pairs. If no combination of these techniques works for the first Heegner index one usually computes, then another Heegner discriminant must

be used. Table A.8 lists rank 1 curves E for which this is necessary such that $E[p]$ is irreducible, E does not have complex multiplication and $(E,p) \neq (1155\text{k}, 7)$. All these curves have $E[p]$ surjective and p does not divide any Tamagawa numbers so it is sufficient to demonstrate a Heegner index which p does not divide. On the other hand if E has complex multiplication, there are a handful of pairs (E,p) left where E has additive reduction at p, and these are listed in Table A.9. □

4.4 Reducible mod-p representations

Suppose E is an optimal elliptic curve of conductor $N(E) < 5000$ and p is a prime such that $E[p]$ is reducible, i.e., there is a p-isogeny $\phi : E \longrightarrow E'$. If $p < 5$ or E is a rank 0 curve with complex multiplication, results of the previous sections show that $\text{BSD}(E/\mathbb{Q}, p)$ is true. This leaves 464 pairs (E,p). By results in [31], $\text{BSD}(11\text{a}/\mathbb{Q}, 5)$ is true, leaving 463 pairs.[1] Table A.10 illustrates the distribution of primes and ranks of these 463 pairs.

The results of Theorem 2.19 can be applied to 339 of these curve-prime pairs, providing that the Heegner index computation cooperates. This occurs in all but five cases, which are listed in Table A.11. This table also lists the discriminant out of the first ten for which the required point search on the twist is easiest (i.e., for which the corresponding height is smallest). The additional column S is an upper bound for $\text{ord}_p(\#Ш(\mathbb{Q}, E))$ in each case, computed using Corollary 2.24 and the technique immediately preceding it.

This leaves 129 pairs of the original 464: 107 5-isogenies, 17 7-isogenies, 2 11-isogenies, and one isogeny each of degree 19, 43 and 67. The 5-, 7- and 11-isogenies ought to be feasible, since doing an isogeny descent will require computing the class groups of number fields of degree up to 10. The remaining three cases are listed in Table A.12, together with the degrees of the relevant number fields. There are also two cases with rank 2, namely $(E,p) \in \{(2601\text{l}1, 5), (3328\text{d}, 5)\}$. The 119 rank 0 and 1 cases not appearing in Tables A.11 and A.12 are listed in Table A.13 for completeness: if (E,p) does not appear in one of these three tables for $E[p]$ reducible, then $\text{BSD}(E,p)$ is true.

---

[1] In `http://www.math.fsu.edu/~agashe/math/090526-Agashe-v1.pdf`, Agashe explains the consequences of Mazur's article in more detail, in situations like these.

4.5 Additive reduction

Suppose E is an optimal rank 0 or 1 elliptic curve with $N(E) < 5000$, and that p is a prime such that $E[p]$ is irreducible. If we want to prove BSD$(E/\mathbb{Q}, p)$, by Theorems 3.8 and 3.9 we may assume $p > 3$ and by Theorem 4.1 we may assume that $\mathrm{ord}_p(\#Ш(\mathbb{Q}, E)_{\mathrm{an}}) = 0$. By the proof of Theorem 4.4, there are only eighteen rank 1 cases left. There is $(E, p) = (1155\mathrm{k}, 7)$, and E does not have additive reduction at p in this case. There are also the 17 curves listed in Table A.9.

Assume in addition that E has rank 0, noting that we may now assume that E does not have complex multiplication. If E does not have additive reduction at p then Theorem 4.3 proves BSD$(E/\mathbb{Q}, p)$, so we are left to consider pairs (E, p) which are of additive reduction. There are 1964 such pairs.

Suppose that $E[p]$ is not surjective. There are 14 such pairs, and Theorem 2.19 applies to all of them. The Heegner point height calculations listed in Table A.14 prove that BSD$(E/\mathbb{Q}, p)$ is true in these cases. Note that in the cases where p may divide the Heegner index, it must do so of order at most 1, and in these cases it also divides a Tamagawa number, so Jetchev's Theorem 2.20 assists Theorem 2.19.

Now we may also assume that $E[p]$ is surjective. For 1871 of the remaining 1950 pairs, Heegner index computations sufficed to prove BSD$(E/\mathbb{Q}, p)$, using Theorem 2.17 and Theorem 2.20. The remaining 79 cases are listed in Table A.15. Each of these cases have $\mathrm{rank}(E(\mathbb{Q})) = 0$, and $\overline{\rho}_{E,p}$ surjective. The height h listed in the table is such that if we can prove that any point $P \in E^D(\mathbb{Q})$ has height $\hat{h}(P) > h$, then BSD$(E/\mathbb{Q}, p)$ is true.

BIBLIOGRAPHY

[1] Amod Agashe and William Stein. Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero. *Math. Comp.*, 74(249):455–484, 2005.

[2] Emil Artin and George Whaples. Axiomatic characterization of fields by the product formula for valuations. *Bull. Amer. Math. Soc.*, 51:469–492, 1945.

[3] Emil Artin and George Whaples. A note on axiomatic characterization of fields. *Bull. Amer. Math. Soc.*, 52:245–247, 1946.

[4] Karim Belabas, Henri Cohen, et al. *PARI/GP.* The Bordeaux Group, `http://pari.math.u-bordeaux.fr/`.

[5] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. I. *J. Reine Angew. Math.*, 212:7–25, 1963.

[6] 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(4):843–939, 2001.

[7] D. Bump, S. Friedberg, and J. Hoffstein. Nonvanishing theorems for L-functions of modular forms and their derivatives. *Invent. Math.*, 102(3):543–618, 1990.

[8] John Cannon, Alan Steele, et al. *MAGMA Computational Algebra System.* The University of Sydney, `http://magma.maths.usyd.edu.au/magma/`.

[9] J. W. S. Cassels. Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung. *J. Reine Angew. Math.*, 211:95–112, 1962.

[10] J. W. S. Cassels. Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer. *J. Reine Angew. Math.*, 217:180–199, 1965.

[11] B. Cha. *Vanishing of Some Cohomology Groups and Bounds for the Shafarevich-Tate Groups of Elliptic Curves.* PhD thesis, Johns-Hopkins, 2003.

[12] B. Cha. Vanishing of some cohomology goups and bounds for the Shafarevich-Tate groups of elliptic curves. *J. Number Theory*, 111:154–178, 2005.

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

[14] J. E. Cremona and T. A. Fisher. On the equivalence of binary quartics. *J. Symbolic Comput.*, 44(6):673–682, 2009.

[15] J. E. Cremona, M. Prickett, and S. Siksek. Height difference bounds for elliptic curves over number fields. *J. Number Theory*, 116(1):42–68, 2006.

[16] John Cremona and Samir Siksek. Computing a lower bound for the canonical height on elliptic curves over $\mathbb{Q}$. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 275–286. Springer, 2006.

[17] John E. Cremona and Barry Mazur. Visualizing elements in the Shafarevich-Tate group. *Experiment. Math.*, 9(1):13–28, 2000.

[18] John E. Cremona and Michael Stoll. Minimal models for 2-coverings of elliptic curves. *LMS J. Comput. Math.*, 5:220–243 (electronic), 2002.

[19] H. Darmon. *Rational points on modular elliptic curves*, volume 101 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004.

[20] B. Edixhoven. On the Manin constants of modular elliptic curves. In *Arithmetic algebraic geometry (Texel, 1989)*, pages 25–39. Birkhäuser Boston, 1991.

[21] G. Grigorov. *Kato's Euler system and the main conjecture*. PhD thesis, Harvard University, 2005.

[22] G. Grigorov, A. Jorza, S. Patrikis, W. Stein, and C. Tarniţă-Pătraşcu. Computational Verification of the Birch and Swinnerton-Dyer Conjecture for Individual Elliptic Curves. `http://wstein.org/papers/bsdalg`.

[23] B. Gross and D. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[24] B. H. Gross. Kolyvagin's work on modular elliptic curves. In *L-functions and arithmetic (Durhan, 1989)*, volume 153 of *London Math. Soc. Lecture Note Ser.*, pages 235–256. Cambridge Univ. Press, Cambridge, 1991.

[25] A. Grothendieck. Modèles de Néron et monodromie. In *Séminaire de Géométrie Algébrique du Bois Marie, SGA7 I*. Springer Lecture Notes 288, 1967–1969.

[26] James E. Humphreys. *Linear algebraic groups*. Springer-Verlag, 1975.

[27] Dimitar Jetchev. Global divisibility of Heegner points and Tamagawa numbers. *Compos. Math.*, 144(4):811–826, 2008.

[28] K. Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, 295:ix, 117–290, 2004.

[29] V. A. Kolyvagin. Euler systems. In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. Math.*, pages 435–483. Birkhäuser Boston, 1990.

[30] Serge Lang. *Number theory. III*, volume 60. Springer-Verlag, 1991.

[31] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, 47:33–186 (1978), 1977.

[32] J. R. Merriman, S. Siksek, and N. P. Smart. Explicit 4-descents on an elliptic curve. *Acta Arith.*, 77(4):385–404, 1996.

[33] M. R. Murty and V. K. Murty. Mean values of derivatives of modular L-series. *Ann. of Math. (2)*, 133(3), 1991.

[34] André Néron. Arithmétique et classes de diviseurs sur les variétés algébriques. In *Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955*, pages 139–154, Tokyo, 1956. Science Council of Japan.

[35] A. P. Ogg. Elliptic curves and wild ramification. *Amer. J. Math.*, 89:1–21, 1967.

[36] K. Rubin. Congruences for special values of L-functions of elliptic curves with complex multiplication. *Invent. Math.*, 71(2):339–364, 1983.

[37] K. Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.*, 103(1):25–68, 1991.

[38] Edward F. Schaefer and Michael Stoll. How to do a p-descent on an Elliptic Curve. *Trans. Amer. Math. Soc.*, 356:1209–1231, 2004.

[39] Pascale Serf. *The rank of elliptic curves over real quadratic number fields of class number 1.* PhD thesis, Universität des Saarlandes, 1995.

[40] Jean-Pierre Serre. *Algebraic groups and class fields*, volume 117 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1988.

[41] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[42] Samir Siksek. *Descents on curves of genus 1.* PhD thesis, University of Exeter, 1995.

[43] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992.

[44] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[45] Sebastian Stamminger. *Explicit 8-descent On Elliptic Curves*. PhD thesis, International University Bremen, 2005.

[46] W. Stein. *The Birch and Swinnerton-Dyer Conjecture, a Computational Approach*. William Stein, 2007.

[47] W. Stein and C. Wuthrich. Computations about Tate-Shafarevich groups using Iwasawa theory. `http://wstein.org/papers/shark`, February 2008.

[48] William Stein. *Explicit approaches to modular abelian varieties*. PhD thesis, University of California at Berkeley, 2000.

[49] William Stein et al. *Sage: Open Source Mathematical Software*. The Sage Group, `http://www.sagemath.org`, 2010.

[50] J. Tate. Duality theorems in Galois cohomology over number fields. *Proc. Intern. Cong. Math. Stockholm*, pages 288–295, 1962.

[51] John Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki, Vol. 9*, pages Exp. No. 306, 415–440. Soc. Math. France, Paris, 1995.

[52] J.-L. Waldspurger. Sur les valuers de certaines fonctions L automorphes en leur centre de symétrie. *Compositio Math.*, 54(2):173–242, 1985.

[53] A. J. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 2(3):443–551, 1995.

[54] Andrew Wiles. The Birch and Swinnerton-Dyer conjecture. In *The millennium prize problems*, pages 31–41. Clay Math. Inst., Cambridge, MA, 2006.

[55] T. Womack. *Explicit descent on elliptic curves*. PhD thesis, University of Nottingham, 2003.

[56] Jeechul Woo. *Arithmetic of Elliptic Curves and Surfaces: Descents and Quadratic Sections*. PhD thesis, Harvard University, 2010.

[57] S.-W. Zhang. Gross-Zagier formula for GL(2). II. In *Heegner points and Rankin L-series*, volume 49 of *Math. Sci. Res. Inst. Publ.*, pages 191–214. Cambridge Univ. Press, 2004.

Appendix A

THE TABLES

Table A.1: Number of E where $\mathrm{ord}_p(\#Ш(\mathbb{Q}, E)_{\mathrm{an}}) = e > 0$

General E

p	$e = 2$	$e = 4$	$e = 6$
2	743	77	3
3	177	0	0
5	33	0	0
7	5	0	0

Optimal E

p	$e = 2$	$e = 4$	$e = 6$
2	123	8	0
3	31	0	0
5	12	0	0
7	1	0	0

Table A.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 A.3: Optimal E with $\mathrm{ord}_p(\#Ш(\mathbb{Q},E)_{\mathrm{an}}) = 2$ for $p \in \{5,7\}$

1058d1	5	2574d1	5	3384a1	5	3364c1	7
1246b1	5	2834d1	5	3952c1	5		
1664k1	5	2900d1	5	4092a1	5		
2366f1	5	3185c1	5	4592d1	5		

Table A.4: Selected Heegner indexes for certain E with $\mathrm{ord}_3(\#Ш(\mathbb{Q},E)_{\mathrm{an}}) = 2$

E	D	I_K	$\mathrm{ord}_3(I_K)$
2601h1	-8	12	1
2718d1	-119	48	1
2932a1	-31	3	1
3555e1	-56	6	1
3879e1	-35	24	1

E	D	I_K	$\mathrm{ord}_3(I_K)$
3933a1	-56	24	1
4343b1	-19	12	1
4675j1	-19	18	2
4963c1	-19	3	1

Table A.5: 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

Table A.6: Non-optimal (E,p) with $\mathrm{ord}_p(\#Ш(\mathbb{Q},E)_{\mathrm{an}}) > 0$ where $\mathrm{BSD}(E/\mathbb{Q},p)$ was not proved

546f2	7	870i3	5	1342c3	5	2370m2	5
570l3	5	870i4	5	1922c2	7	2550be2	5
570l4	5	1050o2	5	1938j2	5	3270h2	5
858k2	7	1230k2	7	1950y2	5		

Table A.7: Non-additive reduction, irreducible but not surjective

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

Table A.8: Some Heegner indexes using larger discriminants

E	p	D	I_K	E	p	D	I_K	E	p	D	I_K
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 A.9: Some rank 1 curves with complex multiplication

225a	5	3136v	7
675a	5	3267d	11
900c	5	3600bd	5
1568g	7	3600be	5
2700h	5	3872a	11
2700l	5	4356a	11
2700p	5	4356c	11
3136t	7	4356b	11
3136u	7		

Table A.10: Ranks of certain E for reducible $E[p]$, $p > 3$

p	$r = 0$	$r = 1$	$r = 2$
5	176	156	2
7	50	44	
11	4	6	
13	10	8	
19		1	
37	2	2	
43		1	
67		1	

Table A.11: Heegner index challenge curves, reducible case

E	p	D_1	h	D_2	S
1950b1	5	-911	62.3	-191	6
2574d1	7	-263	268.9	-95	4
3042o1	5	-23	35.4	-23	4
4950bo1	5	-1151	28.4	-239	4
4950bq1	5	-479	42.7	-479	2

Let z_i be a generator of $E^{D_i}(\mathbb{Q})_{/\text{tors}}$ for $i = 1, 2$. For each line in the table, If $h(z_1) > h$ then BSD$(E/\mathbb{Q}, p)$ is true. Further, since $\hat{h}(z_2) \geq H(E^{D_2})$, Corollary 2.24 shows that $\text{ord}_p(\#Ш(\mathbb{Q}, E)) \leq S$ unconditionally.

Table A.12: Large degree isogenies for $N(E) < 5000$

E	p	d
361a1	19	9
1849a1	43	21
4489a1	67	33

Table A.13: Small degree isogenies for $N(E) < 5000$

26b1	7	286d1	5	784h1	7	1586d1	5	2290d1	5	3542r1	5
38b1	5	294b1	7	786m1	5	1650r1	5	2318e1	5	3786g1	5
50b1	5	302a1	5	806f1	5	1650s1	5	2350n1	5	3806k1	5
57c1	5	325e1	5	834g1	5	1686c1	5	2370m1	5	3850t1	5
58b1	5	366b1	5	858k1	7	1717c1	5	2550be1	5	4010e1	5
66c1	5	395c1	5	862e1	5	1745e1	5	2651c1	5	4011d1	5
75c1	5	426a1	5	870i1	5	1790d1	5	2715c1	5	4043a1	5
110a1	5	441d1	7	874e1	5	1866i1	5	2766i1	5	4389k1	5
118b1	5	490k1	7	885d1	5	1870h1	5	2786d1	5	4450k1	5
121b1	11	537e1	5	890g1	5	1914o1	5	2850w1	5	4495d1	5
123a1	5	546f1	7	1050o1	5	1914p1	5	2869b1	5	4650bl1	5
150a1	5	550k1	5	1147b1	5	1938j1	5	3025a1	11	4650bp1	5
155a1	5	570l1	5	1155n1	5	1950y1	5	3026d1	5	4730k1	7
158c1	5	574i1	7	1230k1	7	1986g1	5	3075l1	5	4774j1	5
174b1	7	574j1	5	1254k1	5	2090n1	5	3126c1	5	4774k1	5
175a1	5	606f1	5	1293e1	5	2110e1	5	3135h1	5	4790c1	5
186b1	5	665d1	5	1310c1	5	2110h1	7	3136r1	7	4854c1	5
203a1	5	678d1	7	1342c1	5	2170q1	5	3206e1	5	4886f1	5
246b1	5	710d1	5	1479f1	5	2175j1	5	3270h1	5	4910g1	5
258f1	7	762g1	7	1526e1	5	2235f1	5	3333g1	5		

Table A.14: Additive reduction, irreducible but not surjective

E	p	D	I_K	$\prod_q c_q$	E	p	D	I_K	$\prod_q c_q$
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

Table A.15: Heegner index challenge curves, surjective additive case

E	p	D_1	h	D_2	S	E	p	D_1	h	D_2	S
1050l1	5	-311	27.2	-311	4	3850m1	5	-2351	38.8	-271	2
1050n1	5	-2399	63.4	-311	8	3850y1	5	-1399	596.4	-271	8
1050q1	5	-311	53.8	-311	6	3900k1	5	-1199	106.1	-191	4
1350o1	5	-239	30.8	-71	4	3900l1	5	-191	23.5	-191	6
1470q1	7	-479	223.6	-311	6	4050bi1	5	-71	32.7	-71	2
1764h1	7	-167	21.5	-47	4	4050s1	5	-551	37.0	-119	4
1850d1	5	-471	57.0	-71	4	4050x1	5	-119	25.6	-71	4
2100o1	5	-311	94.7	-311	4	4200bd1	5	-479	888.7	-311	8
2352x1	7	-551	25.9	-47	4	4200m1	5	-719	309.8	-311	8
2450bd1	5	-559	63.2	-31	6	4350q1	5	-719	104.5	-719	6
2450k1	5	-159	22.5	-31	4	4350w1	5	-719	141.5	-71	8
2550bc1	5	-191	37.0	-191	6	4410b1	7	-671	49.4	-671	2
2550j1	5	-239	46.3	-191	8	4410bi1	7	-1319	177.1	-1319	4
2550z1	5	-1511	30.4	-671	6	4410bj1	7	-311	36.1	-311	4
2646ba1	7	-47	99.7	-47	6	4410q1	7	-839	49.2	-551	2
2646bd1	7	-143	143.4	-47	6	4410u1	7	-2231	70.5	-671	4
2650k1	5	-679	516.8	-439	6	4550p1	5	-1119	647.4	-1119	6
3038m1	7	-55	40.7	-55	4	4606b1	7	-31	54.2	-31	4
3150bc1	5	-1511	40.7	-311	4	4650bo1	5	-119	166.1	-119	8
3150bd1	5	-1991	3250.0	-839	8	4650bs1	5	-239	1154.9	-119	10
3150bj1	5	-311	24.2	-311	2	4650bt1	5	-1511	22.1	-119	2
3150bn1	5	-1991	252.7	-311	8	4650bu1	5	-1199	175.8	-119	10
3150t1	5	-1151	183.5	-311	6	4650q1	5	-119	75.8	-119	4
3185c1	7	-199	69.0	-131	4	4650w1	5	-719	2343.8	-119	10
3225b1	5	-119	23.0	-71	2	4725q1	5	-59	47.1	-59	4
3234c1	7	-503	172.9	-503	4	4800ba1	5	-71	24.2	-71	4
3350d1	5	-79	43.4	-31	6	4850h1	5	-31	131.5	-31	6
3450p1	5	-479	56.8	-479	6	4900w1	5	-311	22.0	-31	4
3450v1	5	-191	827.5	-191	10	4950bj1	5	-239	57.4	-239	6
3630c1	11	-1559	57.9	-239	2	4950bk1	5	-239	99.9	-239	6
3630l1	11	-239	286.2	-239	6	4950bm1	5	-479	7759.1	-239	10
3630r1	11	-239	37.7	-239	4	4950bp1	5	-431	144.8	-239	8
3630u1	11	-1319	30.9	-239	2	4950w1	5	-1151	50.3	-239	4
3650j1	5	-79	62.9	-71	6	4950x1	5	-359	370.8	-359	6
3822bc1	7	-647	27.4	-311	4	4998bg1	7	-47	50.0	-47	6
3822e1	7	-1511	21.9	-335	2	4998bk1	7	-47	509.1	-47	8
3822u1	7	-503	27.6	-503	4	4998k1	7	-47	178.2	-47	6
3822w1	7	-503	152.5	-335	4	4998t1	7	-1487	27.4	-47	4
3822z1	7	-1823	80.6	-311	6	4998u1	7	-47	31.9	-47	4
3850e1	5	-1399	60.1	-271	4						

Let z_i be a generator of $E^{D_i}(\mathbb{Q})_{/\text{tors}}$ for $i = 1, 2$. For each line in the table, If $h(z_1) > h$ then $\text{BSD}(E/\mathbb{Q}, p)$ is true. Further, since $\hat{h}(z_2) \geq H(E^{D_2})$, Corollary 2.24 shows that $\text{ord}_p(\#Ш(\mathbb{Q}, E)) \leq S$ unconditionally.

Appendix B

ABELIAN VARIETIES OVER GLOBAL FIELDS

This chapter will review the characterization of global fields, the Tamagawa measure on the Néron model of an abelian variety, the Birch and Swinnerton-Dyer (BSD) conjecture as generalized by Tate and classical results which support the conjecture.

A global field K is a finite separable extension of either $\mathbb{Q}$ or $\mathbb{F}_q(t)$, where $\mathbb{F}_q$ is a finite field and t is transcendental over it (called *number fields* and *function fields,* respectively—the term function field will always be meant in this sense, with $X(Y)$ denoting the field of X-valued functions on Y). Global fields are the natural setting for class field theory, and Artin and Whaples (in [2] and [3]) characterized these fields axiomatically in terms of the following properties:

- Every valuation of K is either archimedean or discrete with finite residue class field.

- The normalized absolute values $|\cdot|_v$ representing the set of places M_K satisfy a product formula

$$\prod_{v \in M_K} |\alpha|_v = 1 \text{ for all } \alpha \in K^*.$$

  For this to make sense, one can assume that $|\alpha|_v = 1$ for all but finitely many places, or that the product rule is in the sense of absolute convergence.

To define the normalized valuation, let v be a valuation of K and let K_v be the completion with respect to v. Then for $\alpha \in K_v$, the map $x \mapsto \alpha x$ will scale any Haar measure on K_v by a number which does not depend on the choice of Haar measure. This number is the normalized valuation $|\alpha|_v$ of α.

Let A be an abelian variety defined over a global field K, and let G_K be the absolute Galois group of K. It is helpful to consider A as a scheme over K, because this allows us to phrase some definitions in a natural way. Let $\mathfrak{p}$ be a nonzero prime ideal of K and fix

the notation $\mathcal{O}_\mathfrak{p} = \{\alpha \in K : |\alpha|_\mathfrak{p} \leq 1\}$ for the valuation ring, $\mathfrak{m}_\mathfrak{p} = \{\alpha \in K : |\alpha|_\mathfrak{p} < 1\}$ for its maximal ideal and $k_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ for the residue class field. In addition, define $\mathcal{O}_K$ to be the ring of integers of K. The abelian variety A is said to have good reduction at $\mathfrak{p}$ if there exists a smooth proper scheme X over $\mathcal{O}_\mathfrak{p}$ whose generic fiber is A. For example if $K = \mathbb{Q}$ then $\mathfrak{p} = (p)$ for a prime number p and we have $\mathcal{O}_\mathfrak{p} = \mathbb{Z}_{(p)}$, $\mathfrak{m}_\mathfrak{p} = p\mathbb{Z}_{(p)}$ and $k_\mathfrak{p} = \mathbb{F}_p$. In this case A has good reduction at p if there is a smooth proper scheme defined over $\mathbb{Z}_{(p)}$ (i.e., the coefficients of the defining equation all have denominators that are not divisible by p) whose generic fiber is A, and the fiber product then gives a scheme over $\mathbb{F}_p$. In general, we have the following diagram:

$$\begin{array}{ccccc} A & \longrightarrow & X & \longleftarrow & X \times_{\mathcal{O}_\mathfrak{p}} k_\mathfrak{p} \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Spec}(K) & \longrightarrow & \mathrm{Spec}(\mathcal{O}_\mathfrak{p}) & \longleftarrow & \mathrm{Spec}(k_\mathfrak{p}). \end{array}$$

The Néron model of A over $\mathcal{O}_K$ is a smooth group scheme $\mathcal{A}$ over $\mathcal{O}_K$ whose generic fiber is A, such that the following universal property is satisfied. For any smooth scheme X over $\mathcal{O}_K$, morphisms $X_K \longrightarrow \mathcal{A}_K = A$ extend uniquely to morphisms $X \longrightarrow \mathcal{A}$. That is, there is an isomorphism of morphism groups as illustrated in the following diagram:

$$\begin{array}{ccccc} & & \mathcal{A}_K & \longrightarrow & \mathcal{A} \\ & \nearrow & \downarrow & \nearrow & \downarrow \\ X_K & \longrightarrow & X & & \\ & \searrow & & \searrow & \\ & & \mathrm{Spec}(K) & \longrightarrow & \mathrm{Spec}(\mathcal{O}_K). \end{array}$$

The existence of Néron models is highly nontrivial and is due to Néron [34]. For a prime $\mathfrak{p}$ of K, let $\mathcal{A}_\mathfrak{p}$ denote the special fiber of $\mathcal{A}$ over the residue class field $k_\mathfrak{p}$. As an algebraic group over $k_\mathfrak{p}$, $\mathcal{A}_\mathfrak{p}$ is not necessarily connected so denote the connected component containing the identity by $\mathcal{A}_\mathfrak{p}^0$. Since $\mathcal{A}_\mathfrak{p}^0$ is a group variety over $k_\mathfrak{p}$ it is an extension of an abelian variety by a linear group. This linear group is an extension of a torus by a unipotent group, so we define $u(\mathcal{A}, \mathfrak{p})$ to be the dimension of the unipotent part and $t(\mathcal{A}, \mathfrak{p})$ to be the dimension of the torus (see [40, Chapter VII] and [26, Part VI] for details).

Let ℓ be a rational prime such that $\mathfrak{p} \nmid \ell$, let L/K be the finite extension $L = K(\mathcal{A}[\ell])$

and let $G = \mathrm{Gal}(L/K)$. The higher ramification groups are defined by

$$G_i = \{\sigma \in G : \mathrm{ord}_{\mathfrak{p}}(\mathfrak{p}^\sigma - \mathfrak{p}) \geq i+1\},$$

which form a decreasing sequence of subgroups of G. The wild ramification index can be defined via the Hilbert formula

$$\delta(\mathcal{A}, \mathfrak{p}) = \sum_{i=1}^{\infty} \frac{\#G_i}{\#G} \dim_{\mathbb{Z}/\ell\mathbb{Z}} \mathcal{A}[\ell]/\mathcal{A}[\ell]^{G_i}.$$

Grothendieck proved in [25] that this is independent not only of the field L but also of the prime ℓ. (Note that Ogg proved this first for elliptic curves in [35]). For example, if $A = E$ is an elliptic curve over $\mathbb{Q}$ and if all of its two torsion is rational, then $\mathcal{A}[\ell] = \mathcal{A}[\ell]^{G_i}$ for all $i \geq 1$, i.e., $\delta(E, p) = 0$ for all odd primes p.

Finally, define the conductor of $\mathcal{A}$ (and of A) to be

$$N(\mathcal{A}) = \prod_{\mathfrak{p}} \mathfrak{p}^{2u(\mathcal{A},\mathfrak{p})+t(\mathcal{A},\mathfrak{p})+\delta(\mathcal{A},\mathfrak{p})}.$$

By [41], if $\mathcal{A}$ has good reduction at $\mathfrak{p}$ then $u(\mathcal{A}, \mathfrak{p}) = t(\mathcal{A}, \mathfrak{p}) = \delta(\mathcal{A}, \mathfrak{p}) = 0$, and if $\mathcal{A}$ has good reduction at $\mathfrak{p}$ over an extension of K of degree prime to $\mathrm{Norm}(\mathfrak{p})$ then $\delta(\mathcal{A}, \mathfrak{p}) = 0$. In particular this is the case if $\mathrm{char}(k_{\mathfrak{p}}) > 2\dim(\mathcal{A}) + 1$. For elliptic curves over $\mathbb{Q}$, this implies that wild ramification only happens for $p = 2, 3$ and in particular if $p \geq 5$ then $\mathrm{ord}_p(N(E)) = 2u(E, p) + t(E, p) \leq 2$.

The connected Néron model, denoted $\mathcal{A}^0$, is the open subgroup scheme of $\mathcal{A}$ consisting of $\mathcal{A}^0_\nu$ at each fiber of $\mathcal{A} \longrightarrow \mathrm{Spec}(\mathcal{O}_K)$. For each prime $\mathfrak{p}$ of K, define the Tamagawa number $c_{\mathfrak{p}}(\mathcal{A})$ to be the number of connected components in the fiber over $\mathfrak{p}$. It is possible to use Galois cohomology to show that this is equivalent to

$$c_{\mathfrak{p}}(\mathcal{A}) = [\mathcal{A}_{k_{\mathfrak{p}}}(k_{\mathfrak{p}}) : \mathcal{A}^0_{k_{\mathfrak{p}}}(k_{\mathfrak{p}})],$$

starting with $0 \to \mathcal{A}^0 \to \mathcal{A} \to \Phi \to 0$ and using Lang's theorem.

Following [30, III §5] let $W_{\mathcal{A}}$ be the projective $\mathcal{O}_K$-module of invariant differentials on $\mathcal{A}$. Then $d := \mathrm{rank}(W_{\mathcal{A}}) = \dim(\mathcal{A}) = \dim(H^0(\mathcal{A}_K, \Omega^d))$ and $\wedge^d W_{\mathcal{A}}$ is a submodule of $H^0(\mathcal{A}_K, \Omega^d)$ of rank 1 where $\wedge^d$ represents the d-fold exterior power (the elements of $\wedge^d W_{\mathcal{A}}$ are invariant d-forms) and Ω^d represents the space of d-forms. Choose a K-basis $\{\omega_1, ..., \omega_d\}$

for $H^0(\mathcal{A}_K, \Omega^d)$ and let $\eta = \wedge_i \omega_i$. Then $\wedge^d W_{\mathcal{A}} \cong \eta \mathfrak{a}_\eta$ where $\mathfrak{a}_\eta$ is a fractional ideal of K. A complex embedding σ of K represents a scheme morphism $\mathrm{Spec}(\mathbb{C}) \to \mathrm{Spec}(K)$. Taking the fiber product gives a morphism $\mathcal{A}_{\mathbb{C}} \to \mathcal{A}_K$, and we define η_σ to be the pullback of η by this morphism.

If σ is a complex embedding of K (whose image is not contained in $\mathbb{R}$, of course) define

$$c_{\sigma,\eta}(\mathcal{A}) = \int_{\mathcal{A}_\sigma(\mathbb{C})} i \ \eta_\sigma \wedge \overline{\eta_\sigma},$$

and if σ is a real embedding of K define

$$c_{\sigma,\eta}(\mathcal{A}) = \int_{\mathcal{A}_\sigma(\mathbb{R})} |\eta_\sigma|.$$

Finally define

$$c_\infty(\mathcal{A}) = \frac{\mathrm{Norm}(\mathfrak{a}_\eta)}{|\Delta(K)|^{d/2}} \prod_\sigma c_{\sigma,\eta}(\mathcal{A}),$$

where σ ranges over embeddings corresponding to the archimedean places of K and $\Delta(K)$ denotes the discriminant. This quantity does not depend on the choice of η: If $\eta' = s\eta$ for $s \in K^*$, then $\eta \mathfrak{a}_\eta = \eta' \mathfrak{a}_{\eta'} = s\eta \mathfrak{a}_{\eta'}$ gives $\mathfrak{a}_\eta = s\mathfrak{a}_{\eta'}$. For a complex embedding σ, $\eta'_\sigma \wedge \overline{\eta'_\sigma} = \sigma(s)\overline{\sigma(s)}\eta_\sigma \wedge \overline{\eta_\sigma} = |\sigma(s)|^2 \eta_\sigma \wedge \overline{\eta_\sigma}$ and for a real embedding σ, $|\eta'_\sigma| = |\sigma(s)||\eta_\sigma|$. Because $\mathrm{Norm}(\mathfrak{a}_\eta) = \mathrm{Norm}(s)\mathrm{Norm}(\mathfrak{a}_{\eta'})$ one sees that $c_\infty(\mathcal{A})$ is independent of η, by the product rule for global fields and since $\mathrm{Norm}(s) = \prod_{\mathfrak{p}} |s|_{\mathfrak{p}}$.

If $A^\vee$ is the dual abelian variety it will have the same dimension as A and the rank of $A(K)$ will agree with that of $A^\vee(K)$. It is proven in [34] that there is a canonical choice of height function on $A(K) \times A^\vee(K)$. This height is denoted $\hat{h}$ and called the Néron-Tate canonical height. A good discussion of the general theory of heights can be found in [30, ch. II & III].[1] The Néron-Tate height is a nondegenerate pairing of $A(K)$ with $A^\vee(K)$, and if $\{P_1, ..., P_r\}$ is a basis for $A(K)$, and $\{Q_1, ..., Q_r\}$ is a basis for $A^\vee(K)$, then the regulator is $\mathrm{Reg}(A(K)) := |\det(\langle P_i, Q_j \rangle)_{i,j=1}^r|$, where $\langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$.

The L-function of an abelian variety A is defined as follows. Suppose $\mathfrak{p}$ is a non-archimedean prime of K and let $\mathrm{Frob}_{\mathfrak{p}}$ denote the arithmetic Frobenius element of $D_{\mathfrak{p}}/I_{\mathfrak{p}}$, where $D_{\mathfrak{p}}$ is the decomposition group and $I_{\mathfrak{p}}$ is the inertia group. If ℓ is a prime not equal

[1] The reader unfamiliar with these topics should know that details regarding divisors are being suppressed—see *Ibid.* for more details.

to the characteristic of $k_\mathfrak{p}$ then we define the ℓ-adic Tate module $T_\ell(A) = \varprojlim A(\overline{\mathbb{Q}})[\ell^n]$. Let $P_\mathfrak{p}(T)$ denote the characteristic polynomial of $\mathrm{Frob}_\mathfrak{p}$ restricted to the $I_\mathfrak{p}$-invariant piece $T_\ell(A)^{I_\mathfrak{p}}$. Then, the local L-factor at $\mathfrak{p}$ is defined to be

$$L(A/K, \mathfrak{p}, s) = P_\mathfrak{p}(\mathrm{Norm}(\mathfrak{p})^{-s})^{-1}.$$

The global L-function is defined as the Euler product over local L-factors:

$$L(A/K, s) = \prod_\mathfrak{p} L(A/K, \mathfrak{p}, s).$$

This L-function converges for $\Re(s) > 3/2$. By the deep results of [53] and [6], if $\dim A = 1$ and $K = \mathbb{Q}$ then this function has analytic continuation to the entire complex plane, and this is also denoted $L(A/K, s)$. This is also true if $\dim A = 1$, A has complex multiplication, and K is a number field—see [44, II, §10] for details. In both of these cases there is also a functional equation.

The Shafarevich-Tate group is the kernel of the map $H^1(K, A) \longrightarrow \prod_\mathfrak{p} H^1(K_\mathfrak{p}, A)$, which is the product of the restriction maps coming from $K \hookrightarrow K_\mathfrak{p}$ over all $\mathfrak{p}$ (not just the non-archimedean places). We have the alternating, bilinear Cassels-Tate pairing, originally defined for elliptic curves in [9] and extended to abelian varieties in [50]:

$$Ш(K, A) \times Ш(K, A^\vee) \to \mathbb{Q}/\mathbb{Z}.$$

The Birch and Swinnerton-Dyer conjecture comes in two pieces.

Conjecture B.1. *The order of vanishing of $L(A/K, s)$ at $s = 1$ is equal to the rank of the Mordell-Weil group $A(K)$.*

We define $r_{\mathrm{an}}(A/K) = \mathrm{ord}_{s=1} L(A/K, s)$ to be the analytic rank.

Conjecture B.2. *We have*

$$\mathrm{rank}(A(K)) = r_{\mathrm{an}}(A/K),$$

the Shafarevich-Tate group is finite, and the leading term of the Taylor series expansion for $L(A/K, s)$ about $s = 1$ is given by

$$\frac{L^{(r)}(A/K, 1)}{r!} = \frac{c_\infty(\mathcal{A}) \cdot \prod_\mathfrak{p} c_\mathfrak{p}(\mathcal{A}) \cdot R_{A(K)} \cdot \#Ш(K, A)}{\#A(K)_{\mathrm{tors}} \cdot \#A^\vee(K)_{\mathrm{tors}}}.$$

Tate has characterized the unique flavor of this conjecture by describing it as relating the order of vanishing of a function at a point at which it is not known to be defined to the order of a group that is not known to be finite. There is an analogue to the Birch and Swinnerton-Dyer conjecture in which all the quantities are known to be defined and finite: the analytic class number formula for a number field K. Here the object is $\mathcal{O}_K^\times$, and the analogy with the Néron model comes from taking it to be the integral model of $\mathbb{G}_m$. Its rank is $n = r + s - 1$, where r is the number of real embeddings and s is the number of conjugate pairs of complex embeddings and this is also the order of vanishing of the Dedekind zeta function $\zeta_K(s)$ at $s = 0$. The class group $Ш(K, \mathbb{G}_m) = \ker\left(H^1(K, \mathbb{G}_m) \to \prod_{\mathfrak{p}} H^1(K_{\mathfrak{p}}, \mathbb{G}_m)\right)$ plays the role of the Shafarevich-Tate group, and there is a formula for the leading coefficient of the Taylor expansion:

$$\frac{\zeta_K^{(n)}(0)}{n!} = \frac{-1 \cdot R_K \cdot \#Ш(K)}{\#(\mathcal{O}_K^\times)_{\text{tors}}}.$$

Andrei Jorza has written up a proof of the fact that the class group can be defined in this way, and the notes are available on his website[2]. Many similar conjectures have been made for groups of algebraic cycles by Tate, Lichtenbaum, Deligne, Beilinson, Bloch and Kato.

Originally proven by Cassels for elliptic curves over number fields [10], the following theorem was proven in full generality by Tate [51]:

Theorem B.3. *If K is a number field, the truth of the full BSD conjecture depends only on the K-isogeny class of A. If K is a function field, then the truth of the full BSD conjecture is preserved by isogenies of degree prime to the characteristic of K.*

The following is due to Artin, Milne, Tate and others:

Theorem B.4. *If K is a function field, then $r_{\text{an}}(A/K) \geq \text{rank}(A(K))$. Furthermore, the full BSD conjecture is equivalent to the statement that the Shafarevich-Tate group is finite.*

[2] `http://www.ajorza.org/`