OXFORD UNIVERSITY PRESS LTD JOURNAL **00** (0000), 1–17
doi:10.1093/OUP Journal/XXX000

Toward a Generalization of the Gross-Zagier Conjecture

William Stein[1]*
[1] *Department of Mathematics, University of Washington, Web:* `http://wstein.org`, *Email:* `wstein@uw.edu`

Abstract: We review some of Kolyvagin's results and conjectures about elliptic curves, then make a new conjecture that slightly refines Kolyvagin's conjectures. We introduce a definition of finite index subgroups $W_p \subset E(K)$, one for each prime p that is inert in a fixed imaginary quadratic field K. These subgroups generalize the group $\mathbb{Z}y_K$ generated by the Heegner point $y_K \in E(K)$ in the case $r_{\mathrm{an}} = 1$. For any curve with $r_{\mathrm{an}} \geq 1$, we give a description of W_p, which is conditional on truth of the Birch and Swinnerton-Dyer conjecture and our conjectural refinement of Kolyvagin's conjecture. We then deduce the following conditional theorem, up to an explicit finite set of primes: (a) the set of indexes $[E(K) : W_p]$ is finite, and (b) the subgroups W_p with $[E(K) : W_p]$ maximal satisfy a higher-rank generalization of the Gross-Zagier formula. We also investigate a higher-rank generalization of a conjecture of Gross-Zagier.

KEY WORDS number theory; Birch and Swinnerton-Dyer Conjecture; Euler systems; Heegner points; Kolyvagin's conjecture; computational number theory; Gross-Zagier theorem

Received

1 Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$. The order of vanishing r_{an} at $s = 1$ of the Hasse-Weil L-series $L(E/\mathbb{Q}, s)$ of E is defined because E is modular (see [BCDT01, Wil95]). The Birch and Swinnerton-Dyer (BSD) rank conjecture [Bir65] asserts that r_{an} is equal to the algebraic rank r_{alg} of $E(\mathbb{Q})$. The BSD formula then gives a conjectural formula for the leading coefficient of the Taylor expansion about $s = 1$ of $L(E/\mathbb{Q}, s)$; this formula resembles the analytic class number formula. The BSD rank conjecture is known for curves with $r_{\mathrm{an}} \leq 1$, but there has been relatively little progress toward the BSD rank conjecture when $r_{\mathrm{an}} \geq 2$.

In the late 1980s, Kolyvagin wrote several landmark papers that combined the Gross-Zagier theorem [GZ86] about heights of Heegner points over quadratic imaginary fields K, a theorem [BFH90] about nonvanishing of special values of twists of L-functions, and relations involving Hecke operators between Heegner points over ring class fields of K to prove that if $r_{\mathrm{an}} \leq 1$, then the BSD rank conjecture is true for E. Kolyvagin wrote [Kol91a] on the case of general rank, in which he computes the elementary invariants of the Selmer groups of any elliptic curve E of any rank in terms of properties of Heegner points, assuming a certain nontriviality hypothesis. It was until recently unclear whether or not this hypothesis was ever satisfied for any curve with $r_{\mathrm{an}} \geq 2$. Fortunately, this hypothesis has now been confirmed numerically (with high probability) in one case of a rank 2 curve [JLS08].

We review some of Kolyvagin's results and conjectures from [Kol91a], then make a new conjecture that refines Kolyvagin's conjectures. Using reduction modulo p of Heegner points, we introduce a definition of finite index subgroups $W_p \subset E(K)$, one for each prime p that is inert in K. Let $y_K \in E(K)$ be the associated Heegner point as in Equation (1) below. Then these subgroups W_p generalize the group $\mathbb{Z}y_K$ in the case $r_{\mathrm{an}} = 1$. For any $r_{\mathrm{an}} \geq 1$, we give a description of W_p, which is conditional on truth of the BSD conjecture and our conjectural refinement of Kolyvagin's conjecture. We then deduce the following conditional theorem (see Theorems 7.5 and 7.7), up to an explicit finite set of primes: (a) the set of indexes $[E(K) : W_p]$ is finite, and (b) the subgroups W_p with $[E(K) : W_p]$ maximal satisfy a higher-rank generalization of the Gross-Zagier formula (see (5) below). We also give numerical data and a new conjecture about the existence of Gross-Zagier subgroups.

We leave open far more questions than we answer, and we intend to follow up on these questions in subsequent papers. For example, perhaps the definition of the groups W_p can be refined and generalized in various ways, and results similar to those in this paper proved about them. It would be interesting to find a practical algorithm that can provably compute the groups W_p for a particular p, assuming that $E(K)$ has already been computed. We also hope to find a higher-rank analogue of the Gross-Zagier formula over the Hilbert class field of K, involving the Petersson inner product, modular forms, and Rankin-Selberg convolutions $L_{\mathcal{A}}(f, s)$, as in [GZ86], which is consistent with the results we prove about the groups W_p in this paper. It would also be

*Supported by NSF grant 0555776.

valuable to give proofs of the results of [Kol91a] building on [McC91] instead of [Kol91b], possibly using results from the present paper.

We briefly outline the structure of this paper. In the first few sections, we state the BSD conjecture and Gross-Zagier formula, define Kolyvagin points, state Kolyvagin's conjectures, and then define certain finite index subgroups W_p of $E(K)$. In the rest of the paper, we study reduction mod p, conditionally deduce the structure of W_p, and give some numerical examples.

More precisely, we do the following. In Section 2 we state the full Birch and Swinnerton-Dyer conjecture over an imaginary quadratic field K, and state a generalized Gross-Zagier formula for elliptic curves of any rank. In Section 3, we introduce the Kolyvagin points P_λ on E over ring class fields of K, and deduce some key properities of these points. We state Kolvagin's conjectures from [Kol91a] along with some of their consequences in Section 4. We also state a conjecture that refines Kolyvagin's conjectures and also refines a conjecture of Gross-Zagier. In Section 5 we use reductions of Kolyvagin points to define, for every prime p that is inert in K, a finite index subgroup W_p of $E(K)$. Section 6 lays some general foundations for our later determination of the structure of W_p by studying the image of a fixed $Q \in E(K)$ in $E(\mathbb{F}_{p^2})/(p+1)$. Section 7 presents a conditional proof that (up to primes not in the set $B(E)$) maximal index subgroups exist and that they satisfy our generalized Gross-Zagier formula. Finally, in Section 8 we numerically investigate the existence of Gross-Zagier subgroups of $E(K)$, and give evidence for a higher-rank generalization of a conjecture of Gross-Zagier.

Acknowledgement: We thank R. Bradshaw, K. Buzzard, C. Citro, J. Coates, C. Cornut, M. Flach, R. Greenberg, B. Gross, D. Jetchev, K. Lauter, B. Mazur, R. Miller, and Tonghai Yang for helpful conversations. We thank Amod Agashe and Andrei Jorza for carefully reading a draft of the paper and providing many helpful comments, and we thank the anonymous referee for much helpful feedback.

> "It is always good to try to prove true theorems."
>
> – Bryan Birch

1.1 Notation and Conventions

Let A be an abelian group. Let A_{tor} be the subgroup of elements of A of finite order and let $A_{/\,\mathrm{tor}} = A/A_{\mathrm{tor}}$ denote the quotient of A by its torsion subgroup. Let $A[n]$ be the subgroup of elements of A of order n, and for any prime ℓ, let $A(\ell)$ be the subgroup of elements of ℓ-power order. For $z \in A$, let $e = \mathrm{ord}_\ell(z)$ be the largest integer e such that $z = \ell^e y$ for some $y \in A$, or $\mathrm{ord}_\ell(z) = \infty$ if the set of e is unbounded. If $a_1, \ldots, a_n$ are elements of an additive or multiplicative group A, we let $\langle a_1, \ldots, a_n\rangle$ denote the subgroup of A generated by the a_i.

Throughout this paper, E denotes an elliptic curve defined over $\mathbb{Q}$ of conductor N, and K is a quadratic imaginary field with $D = \mathrm{disc}(K)$ coprime to N that satisfies the *Heegner hypothesis*—each prime dividing N splits in K. We fix an ideal $\mathcal{N}$ in $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N}$ is cyclic of order N. Let H be the Hilbert class field of K, let $\pi : X_0(N) \to E$ be a fixed choice of modular parametrization (see Section 3 below), and let

$$y_K = \mathrm{Tr}_{H/K}(\pi((\mathbb{C}/\mathcal{O}_K, \mathcal{N}^{-1}/\mathcal{O}_K))) \in E(K) \tag{1}$$

be the Heegner point associated to K.

Let c denote the Manin constant of E (see Section 2), and c_q the Tamagawa numbers of E at primes $q \mid N$. Unless otherwise stated, everywhere in this paper p denotes a prime that is inert in K.

2 Gross-Zagier Subgroups

In this section, we fix our notation and conventions, and define the Manin constant. Then we recall the statement of the full Birch and Swinnerton-Dyer conjecture over an imaginary quadratic field K. We give a new definition of *Gross-Zagier subgroups* of $E(K)$ and prove that they all satisfy a Gross-Zagier style formula. When $r_{\mathrm{an}} = 1$, we prove that $\mathbb{Z}y_K$ is the unique Gross-Zagier subgroup, up to torsion.

Let E be an elliptic curve over $\mathbb{Q}$ and let K be a quadratic imaginary field that satisfies the Heegner hypothesis – so K has discriminant $D < -4$, each prime dividing the conductor N of E splits in K, and $\gcd(D, N) = 1$. Let $\mathcal{O}_K$ be the ring of integers of K. Let E^D denote the quadratic twist of E by D. Throughout this paper, except briefly in Section 8, we *always* assume that

$$r_{\mathrm{an}}(E/\mathbb{Q}) > r_{\mathrm{an}}(E^D/\mathbb{Q}) \leq 1 \tag{2}$$

Recall that under the Heegner hypothesis the sign of the functional equation of

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

is -1, so the sign in the functional equations for $L(E/\mathbb{Q}, s)$ and $L(E^D/\mathbb{Q}, s)$ are different, hence

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

Proposition 2.1. *Suppose E is an elliptic curve with $r_{\mathrm{an}}(E/\mathbb{Q}) > 0$. Then there exist infinitely many D satisfying the Heegner hypothesis with*

$$r_{\mathrm{an}}(E/\mathbb{Q}) > r_{\mathrm{an}}(E^D/\mathbb{Q}) \leq 1.$$

Proof. The main theorem of [BFH90] implies the existence of infinitely many D with $r_{\mathrm{an}}(E^D/\mathbb{Q}) \leq 1$. Since $r_{\mathrm{an}}(E/\mathbb{Q}) > 0$ and $r_{\mathrm{an}}(E/\mathbb{Q}) \not\equiv r_{\mathrm{an}}(E^D/\mathbb{Q}) \pmod 2$, the inequality $r_{\mathrm{an}}(E/\mathbb{Q}) > r_{\mathrm{an}}(E^D/\mathbb{Q})$ also holds.

Let $\omega = 2\pi i c f(z) dz$ be the pullback of a minimal invariant differential on E, where $f(z) \in S_2(\Gamma_0(N))$ is a cuspidal newform, and c is the Manin constant of E (see [ARS06]). For each prime $q \mid N$, let c_q be the Tamagawa number of E at q. Set $r = r_{\mathrm{an}}(E/K) = \mathrm{ord}_{s=1} L(E/K, s)$, which is defined since every elliptic curve over $\mathbb{Q}$ is modular. Let $\|\omega\|^2 = \int_{E(\mathbb{C})} \omega \wedge \overline{i\omega} = 2 \cdot \mathrm{Vol}(\mathbb{C}/\Lambda)$. The Shafarevich-Tate group of E over a number field M is

$$Ш(E/M) = \ker\left(\mathrm{H}^1(M, E) \to \bigoplus_v H^1(M_v, E)\right).$$

The following is a formulation of the Birch and Swinnerton-Dyer conjecture [GZ86, pg. 311] over K.

Conjecture 2.2 (Birch and Swinnerton-Dyer)**.** *The Mordell-Weil group $E(K)$ has rank $r = \mathrm{ord}_{s=1} L(E/K, s)$, the Shafarevich-Tate group $Ш(E/K)$ is finite, and*

$$\frac{L^{(r)}(E/K, 1)}{r!} = \frac{\#Ш(E/K) \cdot \|\omega\|^2 \cdot \mathrm{Reg}(E/K) \cdot \left(\prod_{q|N} c_q\right)^2}{\#E(K)_{\mathrm{tor}}^2 \cdot \sqrt{|D|}}. \tag{3}$$

Let $Ш_{\mathrm{an}}$ be the order of $Ш(E/K)$ that is predicted by Conjecture 2.2. The existence of the Cassels-Tate pairing implies that if $Ш(E/K)$ is finite, then $\#Ш(E/K)$ is a perfect square, so Conjecture 2.2 implies that $\sqrt{Ш_{\mathrm{an}}}$ is an integer. Recall from Section 1.1 that $A_{/\mathrm{tor}} = A/A_{\mathrm{tor}}$.

Definition 2.3 (Gross-Zagier subgroup)**.** *A* Gross-Zagier subgroup *$W \subset E(K)$ is a torsion-free subgroup such that $E^D(\mathbb{Q}) \subset W + E(K)_{\mathrm{tor}}$, the quotient $E(K)_{/\mathrm{tor}}/W$ is cyclic, and*

$$[E(K) : W] = c \cdot \prod c_q \cdot \sqrt{Ш_{\mathrm{an}}}. \tag{4}$$

For any set S of primes, we say that a subgroup $W \subset E(K)$ is a *Gross-Zagier subgroup up to primes not in S* if W has no p-torsion for $p \notin S$ and all the conditions of Definition 2.3 holds up to primes not in S.

We will numerically investigate the existence of Gross-Zagier subgroups in Section 8, assuming that Conjecture 2.2 is true. Even the existence of Gross-Zagier subgroups of every $E(K)$ is far from clear, since if they exist, then $\#E(K)_{\mathrm{tor}}$ divides $c \prod c_q \cdot \sqrt{Ш_{\mathrm{an}}}$. In fact, we will give an example of an $E(K)$ that does not have any Gross-Zagier subgroups (this example does not satisfy (2)).

In the following proposition we do not assume the Conjecture 2.2. Thus $Ш_{\mathrm{an}}$ *a priori* could just be some meaningless transcendental number. Also, for any subgroup $H \subset E(K)$, we write $\mathrm{Reg}(H)$ for the absolute value of the determinant of the height pairing matrix on any basis for H modulo torsion.

Proposition 2.4. *If W is a Gross-Zagier subgroup, then W satisfies the* generalized Gross-Zagier formula*:*

$$\frac{L^{(r)}(E/K, 1)}{r!} = \frac{\|\omega\|^2}{c^2 \cdot \sqrt{|D|}} \cdot \mathrm{Reg}(W). \tag{5}$$

More generally, a torsion-free subgroup $W \subset E(K)$ satisfies the generalized Gross-Zagier formula if and only if it has index $c \cdot \prod c_q \cdot \sqrt{Ш_{\mathrm{an}}}$ in $E(K)$.

Proof. The BSD formula (3) with $\#Ш(E/K)$ replaced by $Ш_{\mathrm{an}}$ implies that (5) holds if and only if

$$\frac{\|\omega\|^2}{c^2 \cdot \sqrt{|D|}} \cdot \mathrm{Reg}(W) = \frac{Ш_{\mathrm{an}} \cdot \|\omega\|^2 \cdot \mathrm{Reg}(E/K) \cdot \left(\prod_{p|N} c_q\right)^2}{\#E(K)_{\mathrm{tor}}^2 \cdot \sqrt{|D|}}. \tag{6}$$

Our hypotheses that $[E(K) : W]$ is finite and that W is torsion free imply that

$$[E(K) : W]^2 = \frac{\mathrm{Reg}(W) \cdot \#E(K)_{\mathrm{tor}}^2}{\mathrm{Reg}(E/K)} \tag{7}$$

Manipulate (6) by cancelling everything in common on both sides and putting the regulators and torsion on the left, and everything else on the right. The substitution (7) then shows that $[E(K) : W]^2 = c^2 \cdot \left(\prod_{q|N} c_q\right)^2 \cdot Ш_{\mathrm{an}}$ if and only if (5) holds. Taking square roots proves the proposition. □

Corollary 2.5. *Let $y_K \in E(K)$ be the Heegner point after fixing a choice of ideal $\mathcal{N}$ as in Equation* (1)*, and assume that E has analytic rank* 1*. Then the Gross-Zagier subgroups of $E(K)$ are the cyclic groups $\langle y_K + P\rangle$, for all $P \in E(K)_{\mathrm{tor}}$.*

Proof. By [Kol88], $E(K)$ is of rank 1, and by Proposition 2.4 the Gross-Zagier formula [GZ86, Thm. 2.1, pg. 311] implies that $[E(K) : \langle y_K\rangle] = c \prod c_q \sqrt{Ш_{\mathrm{an}}}$ (see also, [GZ86, Conj. 2.2, pg. 311]). Since $E(K)_{/\,\mathrm{tor}}$ is free of rank 1 and $\langle y_K\rangle$ is torsion free, $E(K)_{/\,\mathrm{tor}}/\langle y_K\rangle$ is cyclic, so $\langle y_K\rangle$ is a Gross-Zagier subgroup. The same argument proves this with y_K replaced by $y_K + P$ for any $P \in E(K)_{\mathrm{tor}}$, since y_K and $y_K + P$ have the same height. If W is any Gross-Zagier subgroup, then since $E(K)$ has rank one we must have $W \equiv \langle y_K\rangle \pmod{E(K)_{\mathrm{tor}}}$, so $W = \langle y_K + P\rangle$ for some $P \in E(K)_{\mathrm{tor}}$.

3 Heegner and Kolyvagin Points

In this section, we define certain subsets $\Lambda^k_{\ell^n} \subset \mathbb{Z}$ of positive square-free integers. For each integer $\lambda \in \Lambda^k_{\ell^n}$, we consider the corresponding ring class field K_λ, and we define elements $I_\lambda, J_\lambda \in \mathbb{Z}[\mathrm{Gal}(K_\lambda/K)]$. We then apply these group ring elements to the Heegner points $y_\lambda \in E(K_\lambda)$ to obtain the Kolyvagin points $P_\lambda \in E(K_\lambda)$. Finally, we prove the $\mathrm{Gal}(K_\lambda/K)$-equivariance of the equivalence class $P_\lambda + \ell^n E(K)$ in $E(K)/\ell^n E(K)$.

For any integer m, let $a_m = a_m(E)$ be the mth coefficient of the L-series $\sum a_m/m^s$ attached to E. Let ℓ be any prime and n any positive integer. For any nonnegative integer k, let $\Lambda^k_{\ell^n}$ be the set of squarefree positive integers $\lambda = p_1 \ldots p_k$ coprime to N, where each p_i is inert in K and

$$a_{p_i} \equiv p_i + 1 \equiv 0 \pmod{\ell^n}.$$

When $k = 0$, we set $\Lambda^0_{\ell^n} = \{1\}$. The Chebotarev density theorem implies that $\Lambda^k_{\ell^n}$ is infinite for any $k \geq 1$.

Recall from Section 1.1 that we fixed an ideal $\mathcal{N}$ in $\mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N}$ is cyclic of order N, and let $\mathcal{O}_\lambda = \mathbb{Z} + \lambda\mathcal{O}_K$ be the order in $\mathcal{O}_K$ of conductor λ. Let $X_0(N)$ be the compact modular curve defined over $\mathbb{Q}$ that classifies isomorphism classes of elliptic curves equipped with a cyclic subgroup of order N. Fix a choice of minimal modular parametrization $\pi : X_0(N) \to E$, which exists by the modularity theorem [BCDT01, Wil95]. For each $\lambda \in \Lambda^k_{\ell^n}$, the *Heegner point*

$$x_\lambda = [(\mathbb{C}/\mathcal{O}_\lambda, (\mathcal{N} \cap \mathcal{O}_\lambda)^{-1}/\mathcal{O}_\lambda)] \in X_0(N)(K_\lambda)$$

is defined over the ring class field K_λ of K of conductor λ.

Definition 3.1 (Heegner point)**.** *The Heegner point y_λ associated to $\lambda \in \Lambda^k_{\ell^n}$ is*

$$y_\lambda = \pi(x_\lambda) \in E(K_\lambda).$$

We emphasize that that y_λ depends on the choice of modular parametrization π_E and the ideal $\mathcal{N}$ in $\mathcal{O}_K$ with $\mathcal{O}_K/\mathcal{N} = \mathbb{Z}/N\mathbb{Z}$. However, once we fix that data, the Heegner points for all λ are defined.

For $\lambda \in \Lambda^k_{\ell^n}$, let $G_\lambda = \mathrm{Gal}(K_\lambda/K_1)$ and note that we have a canonical isomorphism

$$G_\lambda \cong \prod_{p|\lambda} G_p,$$

where the group $G_p = \mathrm{Gal}(K_p/K_1) = \langle t_p\rangle$ is cyclic of order $p+1$, with some (non-canonical) choice t_p of generator. Let

$$I_p = \sum_{i=1}^{p} i t_p^i \in \mathbb{Z}[G_p] \quad \text{and} \quad I_\lambda = \prod_{p|\lambda} I_p \in \mathbb{Z}[G_\lambda].$$

Let R be a set of representatives in $\mathrm{Gal}(K_\lambda/K)$ for the quotient group $\mathrm{Gal}(K_\lambda/K)/\mathrm{Gal}(K_\lambda/K_1) \cong \mathrm{Gal}(K_1/K)$, and let

$$J_\lambda = \sum_{g \in R} g \in \mathbb{Z}[G_\lambda].$$

Definition 3.2 (Kolyvagin Point)**.** *The Kolyvagin point P_λ associated to $\lambda \in \Lambda^k_{\ell_n}$ is*

$$P_\lambda = J_\lambda I_\lambda y_\lambda \in E(K_\lambda).$$

Note that $P_1 = y_K \in E(K)$.

Let $R = \mathrm{End}(E/\mathbb{C})$ and let $B(E)$ be the set of *odd* primes ℓ that do not divide $\mathrm{disc}(R)$ and such that the ℓ-adic representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_R(\mathrm{Tate}_\ell(E))$ is surjective. By a theorem of Serre [Ser72], the set $B(E)$ contains all but finitely many primes (see [GJP+09] for algorithms to bound $B(E)$). Let T_p be the pth Hecke operator on the Jacobian $J_0(N)$ of $X_0(N)$, and for each prime $p \mid \lambda$, let Tr_p be the trace $J_0(N)(K_\lambda) \to J_0(N)(K_{\lambda/p})$.

Proposition 3.3. *The points y_λ form an Euler system, in the sense that if $\lambda = p\lambda'$ for a prime p and $\lambda \in \Lambda_\ell$, then $y_\lambda = \mathrm{Frob}_\wp(y_{\lambda'}) \pmod{\wp}$ for all primes $\wp$ of K_λ over p, and $\mathrm{Tr}_p(x_\lambda) = T_p(x_{\lambda'})$ in $J_0(N)$.*

Proof. See [Gro91, Prop. 3.7].

Proposition 3.4. *We have*

$$[I_\lambda y_\lambda] \in (E(K_\lambda)/\ell^n E(K_\lambda))^{G_\lambda} \qquad \text{and} \qquad [P_\lambda] \in (E(K_\lambda)/\ell^n E(K_\lambda))^{\mathrm{Gal}(K_\lambda/K)}$$

Proof. Though standard (see, e.g., [Gro91, Prop. 3.6]) this proposition plays a key role in Section 5, so we give a proof here for the convenience of the reader. The first statement implies the second, since $[P_\lambda]$ is the $\mathrm{Gal}(K_1/K)$ trace of $[I_\lambda y_\lambda]$. It remains to prove the first inclusion. For this, it suffices to show that $[I_\lambda y_\lambda]$ is fixed by t_p for all primes $p \mid \lambda$, as these elements generate G_λ. We will prove this by showing that $(t_p - 1)I_\lambda y_\lambda$ lies in $\ell^n E(K_\lambda)$.

Write $\lambda = p\lambda'$. We have

$$(t_p - 1)I_p = (t_p - 1) \cdot \left(\sum_{i=1}^{p} i t_p^i\right) = p + 1 - \mathrm{Tr}_p, \tag{8}$$

where as above $\mathrm{Tr}_p = \mathrm{Tr}_{K_\lambda/K_{\lambda'}}$. Note that this is the only place in the proof where we use the explicit definition of I_p as $\sum_{i=1}^{p} i t_p^i$, and in fact we could instead replace I_p by any element I of $\mathbb{Z}[G_\lambda]$ such that

$$(t_p - 1)I = p + 1 - \mathrm{Tr}_p,$$

but doing so does not seem to lead to anything interesting. Note that the Euler system relation (see Proposition 3.3) and our hypothesis that $a_p \equiv 0 \pmod{\ell^n}$ together imply that

$$\mathrm{Tr}_p I_{\lambda'} y_\lambda = I_{\lambda'} \mathrm{Tr}_p y_\lambda = I_{\lambda'} a_p y_{\lambda'} \in \ell^n E(K_\lambda).$$

We have

$$(t_p - 1)I_\lambda = (t_p - 1)I_p I_{\lambda'} = (p + 1 - \mathrm{Tr}_p)I_{\lambda'}$$

in $\mathbb{Z}[G_\lambda]$, so since $p + 1 \equiv 0 \pmod{\ell^n}$

$$(t_p - 1)I_\lambda y_\lambda = (p + 1)I_{\lambda'} y_\lambda - \mathrm{Tr}_p I_{\lambda'} y_\lambda \in \ell^n E(K_\lambda).$$

□

4 Kolyvagin's Conjectures and their Consequences

For any prime ℓ and positive integer n, let

$$\Lambda_{\ell^n} = \bigcup_{\text{all } k \geq 0} \Lambda_{\ell^n}^k$$

be the set of square-free positive integers λ such that $\ell^n \mid \gcd(a_p, p + 1)$ for each $p \mid \lambda$. In this section, we define maps $n, m : \Lambda_\ell \to \mathbb{Z} \cup \{\infty\}$ that measure ℓ-divisibility properties of λ and P_λ for all $\lambda \in \Lambda_\ell$. We state Kolyvagin's "Conjecture A" that there exists λ with $m(\lambda) \neq \infty$, then state Kolyvagin's structure theorem, which describes the structure of $\mathrm{Sel}^{(\ell^b)}(E/K)$, for b sufficiently large, in terms of the maps n and m. Finally, we state Kolyvagin's stronger "Conjecture D", which basically asserts that if f is the smallest nonnegative integer such that $m(\lambda) \neq \infty$ for some $\lambda \in \Lambda_\ell^f$, then for sufficiently large k the cohomology classes τ_{λ,ℓ^n} with $\lambda \in \Lambda_{\ell^n+k}^f$ generate a subgroup of $\mathrm{Sel}^{(\ell^n)}(E/K)$ that equals the image of a subgroup V of $E(K)$. To motivate Conjecture 4.9, we prove that it implies that $\mathrm{rank}(E(\mathbb{Q})) = f + 1$ and $Ш(E/K)(\ell)$ is finite for each $\ell \in B(E)$ and determine the structure of V (see Proposition 4.11).

Recall that we defined ord_ℓ in Section 1.1. Define two set-theoretic maps

$$n, m : \Lambda_\ell \to \mathbb{Z} \cup \{\infty\}$$

by

$$n(\lambda) = \max\{e : \lambda \in \Lambda_{\ell^e}\} \qquad \text{and} \qquad m(\lambda) = \mathrm{ord}_\ell([P_\lambda]),$$

where $[P_\lambda]$ denotes the equivalence class of P_λ in $E(K_\lambda)/\ell^{n(\lambda)}E(K_\lambda)$. For each integer $k \geq 0$, let

$$m_{\ell,k} = \min(m(\Lambda_\ell^k)) \qquad \text{and} \qquad m_\ell = \min(m(\Lambda_\ell)) = \min(\{m_{\ell,k} : k \geq 0\}).$$

Also, let

$$f_\ell = \min\{k : m_{\ell,k} < \infty\} \leq \infty, \tag{9}$$

where we let $f_\ell = \infty$ if $m_\ell = \infty$.

Kolyvagin proves [Kol91b, Thm. C] that $m_{\ell,0} \geq m_{\ell,1} \geq m_{\ell,2} \geq \ldots$.

Conjecture 4.1 (Kolyvagin's Conjecture A_ℓ)**.** *$m_\ell < \infty$. Equivalently, there exists $\lambda \in \Lambda_\ell$ such that $[P_\lambda] \neq 0$.*

See [JLS08] for the first computational evidence for Conjecture 4.1. For example, for a specific rank 2 elliptic curve, that paper shows that $m_3 = m_{3,1} = 0$ and $f_3 = 1$, assuming that the numerical computation of a certain Heegner point y_λ was done to sufficient precision. (If the computation were not done to sufficient precision it is highly likely that we would haved detected this.)

Conjecture 4.1 is quite powerful, as the following theorem shows. For an abelian group A of odd order with an action of complex conjugation, let A^+ denote the $+1$ eigenspace for conjugation and A^- the minus eigenspace, so $A = A^+ \oplus A^-$. As always, we continue to assume our minimality hypothesis that

$$r_{\mathrm{an}}(E/\mathbb{Q}) > r_{\mathrm{an}}(E^D/\mathbb{Q}) \leq 1.$$

Theorem 4.2 (Kolyvagin)**.** *Let $\ell \in B(E)$, suppose Conjecture 4.1 is true for ℓ, and let $f = f_\ell$. For every k, let $b_k = \ell^{m_{\ell,k} - m_{\ell,k+1}}$. Then for every $n \geq m_{\ell,f}$, we have*

$$\mathrm{Sel}^{(\ell^n)}(E/\mathbb{Q}) = \mathrm{Sel}^{(\ell^n)}(E/K)^+ \approx (\mathbb{Z}/\ell^n\mathbb{Z})^{f+1} \oplus (\mathbb{Z}/b_{f+1}\mathbb{Z})^2 \oplus (\mathbb{Z}/b_{f+3}\mathbb{Z})^2 \oplus \cdots$$

and

$$\mathrm{Sel}^{(\ell^n)}(E^D/\mathbb{Q}) = \mathrm{Sel}^{(\ell^n)}(E/K)^- \approx (\mathbb{Z}/\ell^n\mathbb{Z})^h \oplus (\mathbb{Z}/b_f\mathbb{Z})^2 \oplus (\mathbb{Z}/b_{f+2}\mathbb{Z})^2 \oplus \cdots$$

where $h = \mathrm{rank}(E^D(\mathbb{Q})) \leq 1$.

Proof. The leftmost equality in the above two equations is true because ℓ is odd, and Theorem 1 of [Kol91a] implies both of the rightmost equalities, but possibly with $\mathrm{Sel}^{(\ell^n)}(E/K)^+$ and $\mathrm{Sel}^{(\ell^n)}(E/K)^-$ swapped and a different value for h. Theorem 1 of [Kol91a] is proved by inductively constructing cohomology classes with good properties with respect to certain localization homomorphisms. To finish the proof, we establish that these two Selmer groups are not swapped and that $h = \mathrm{rank}(E^D(\mathbb{Q}))$.

First note that by [Kol88, BFH90], our hypothesis that $r_{\mathrm{an}}(E^D/\mathbb{Q}) \leq 1$ implies that $r_{\mathrm{an}}(E^D/\mathbb{Q}) = \mathrm{rank}(E^D(\mathbb{Q}))$ and $Ш(E^D/\mathbb{Q})$ is finite.

If $f = 0$, then the Heegner point y_K has infinite order, so by [GZ86] we have $r_{\mathrm{an}}(E/K) = 1$ and by [Kol88], $E(K)$ has rank 1 and $Ш(E/K)$ is finite. By our minimality hypothesis, we have $r_{\mathrm{an}}(E/\mathbb{Q}) > r_{\mathrm{an}}(E^D/\mathbb{Q})$, so $r_{\mathrm{an}}(E/\mathbb{Q}) = \mathrm{rank}(E(\mathbb{Q})) = 1$ and $r_{\mathrm{an}}(E^D/\mathbb{Q}) = \mathrm{rank}(E^D(\mathbb{Q})) = 0$. Thus the two displayed Selmer groups $\mathrm{Sel}^{(\ell^n)}(E/K)^\pm$ are in the claimed order. Moreover, $h = 0 = \mathrm{rank}(E^D(\mathbb{Q}))$.

Next assume $f > 0$. Then one of the two Selmer groups contained $(\mathbb{Z}/\ell^n\mathbb{Z})^{f+1}$ for arbitrarily large n. Since we know that $Ш(E^D/\mathbb{Q})$ is finite and $\mathrm{rank}(E^D(\mathbb{Q})) \leq 1$ but $f + 1 \geq 2$, the Selmer group that contains $(\mathbb{Z}/\ell^n\mathbb{Z})^{f+1}$ must be $\mathrm{Sel}^{(\ell^n)}(E/K)^+$. Thus again we see that the two displayed Selmer groups are in the claimed order. Also, again $h = \mathrm{rank}(E^D(\mathbb{Q}))$ follows.

□

Remark 4.3. *Suppose the hypotheses of Theorem 4.2 are satisfied. Then comparing the conclusion about the choice of signs in Theorem 4.2 with the statement of Theorem 1 in [Kol91a] shows that $f + 1 \equiv r_{\mathrm{an}}(E/\mathbb{Q}) \pmod 2$, which implies the parity conjecture for the Selmer group of E at ℓ.*

Proposition 4.4. *Let $\ell \in B(E)$. Then $f_\ell = \mathrm{rank}(E(\mathbb{Q})) - 1$ if and only if $Ш(E/\mathbb{Q})(\ell)$ is finite and Conjecture 4.1 holds for ℓ.*

Proof. First suppose $f_\ell = \mathrm{rank}(E(\mathbb{Q})) - 1$. Then $f_\ell \neq \infty$, so Conjecture 4.1 holds. To prove that $Ш(E/\mathbb{Q})(\ell)$ is finite, use Theorem 4.2 and that by our rank hypothesis the image of $E(\mathbb{Q})$ in $\mathrm{Sel}^{(\ell^n)}(E/\mathbb{Q})$ is $(\mathbb{Z}/\ell^n\mathbb{Z})^{f+1}$. Thus $Ш(E/\mathbb{Q})[\ell^n]$ is a quotient of the ℓ^n-torsion subgroup of the finite group $(\mathbb{Z}/b_{f+1}\mathbb{Z})^2 \oplus (\mathbb{Z}/b_{f+3}\mathbb{Z})^2 \oplus \cdots$, so $Ш(E/\mathbb{Q})(\ell)$ is finite.

Conversely, suppose the ℓ-primary group $Ш(E/\mathbb{Q})(\ell)$ is finite and that Conjecture 4.1 holds. Let b be a positive integer such that $\ell^b Ш(E/\mathbb{Q})(\ell) = 0$. Then the map $\mathrm{Sel}^{(\ell^b)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})(\ell)$ is surjective, and for every integer $n \geq b$, the map $\mathrm{Sel}^{(\ell^n)}(E/\mathbb{Q})[\ell^b] \to Ш(E/\mathbb{Q})(\ell)$ is also surjective, since $\mathrm{Sel}^{(\ell^b)}(E/\mathbb{Q}) \to \mathrm{Sel}^{(\ell^n)}(E/\mathbb{Q})[\ell^b]$. The image of $\ell^b\,\mathrm{Sel}^{(\ell^n)}(E/\mathbb{Q})$ in $Ш(E/\mathbb{Q})(\ell)$ is trivial. Since $\ell \in B(E)$ we have $E(\mathbb{Q})_{\mathrm{tor}}[\ell] = 0$, so exactness of the sequence

$$0 \to E(\mathbb{Q})/\ell^n E(\mathbb{Q}) \to \mathrm{Sel}^{(\ell^n)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})(\ell) \to 0$$

implies that $\ell^b\,\mathrm{Sel}^{(\ell^n)}(E/\mathbb{Q}) \approx \ell^b(\mathbb{Z}/\ell^n\mathbb{Z})^r$, where $r = \mathrm{rank}(E(\mathbb{Q}))$. On the other hand, if we also choose $\ell^b \geq b_{f+1}$, then Theorem 4.2 implies that $\ell^b\,\mathrm{Sel}^{(\ell^n)}(E/\mathbb{Q}) \approx \ell^b(\mathbb{Z}/\ell^n\mathbb{Z})^{f+1}$. We conclude that $r = f + 1$.

□

Kolyvagin's other conjectures involve $\mathrm{H}^1(K, E[\ell^\infty]) = \varinjlim_m \mathrm{H}^1(K, E[\ell^m])$.

Lemma 4.5. *Suppose $E(K)[\ell] = 0$. Then for every $m \geq 1$, the natural map $\mathrm{H}^1(K, E[\ell^m]) \to \mathrm{H}^1(K, E[\ell^\infty])$ is injective.*

Proof. This lemma is of course very well known, but we give a proof for completeness. It suffices to show that for any pair a, b of nonnegative integers that the map

$$\mathrm{H}^1(K, E[\ell^a]) \to \mathrm{H}^1(K, E[\ell^{a+b}]) \tag{10}$$

is injective. Taking Galois cohomology of $0 \to E[\ell^a] \to E[\ell^{a+b}] \to E[\ell^{a+b}]/E[\ell^a] \to 0$ we see that $\mathrm{H}^0(K, E[\ell^{a+b}]/E[\ell^a])$ surjects onto the kernel of (10). We have an exact sequence of Galois modules

$$0 \to E[\ell^a] \to E[\ell^{a+b}] \xrightarrow{\ell^a} E[\ell^b] \to 0,$$

so $\mathrm{H}^0(K, E[\ell^{a+b}]/E[\ell^a]) \cong \mathrm{H}^0(K, E[\ell^b]) = E(K)[\ell^b] = 0$, since $E(K)[\ell] = 0$.

□

We now define Galois cohomology classes associated to the Kolyvagin points P_λ. For $\lambda \in \Lambda_{\ell^n}$ with $\ell \in B(E)$, let $\tau_{\lambda,\ell^n} \in \mathrm{H}^1(K, E[\ell^n])$ be the image of P_λ under the map

$$(E(K_\lambda)/\ell^n E(K_\lambda))^{\mathrm{Gal}(K_\lambda/K)} \hookrightarrow \mathrm{H}^1(K_\lambda, E[\ell^n])^{\mathrm{Gal}(K_\lambda/K)} \cong \mathrm{H}^1(K, E[\ell^n]),$$

where the last map is an isomorphism because $\ell \in B(E)$ (see, e.g., [Gro91, §4]). Kolyvagin also remarks that one can define Galois cohomology classes τ_{λ,ℓ^n} for $\ell \notin B(E)$ and all $\lambda \in \Lambda_{\ell^{k_0+n}}$, where k_0 is the smallest nonnegative even integer such that $\ell^{k_0/2}E(\mathbf{K})(\ell) = 0$ and $\mathbf{K}$ is the compositum of all K_λ for $\lambda \in \Lambda$. Of course, for all $\ell \in B(E)$ we have $k_0 = 0$.

Let τ'_{λ,ℓ^n} be the image in $H^1(K, E[\ell^\infty])$ of τ_{λ,ℓ^n} (note that for the moment we are not assuming that $\ell \in B(E)$, so the natural map $\mathrm{H}^1(K, E[\ell^m]) \to \mathrm{H}^1(K, E[\ell^\infty])$ need not be injective). For any integers $a \geq 0$, $k \geq k_0$ and $n \geq 1$, let

$$V^a_{k,\ell^n} = \langle \tau'_{\lambda,\ell^n} : \lambda \in \Lambda^a_{\ell^{n+k}} \rangle \subset H^1(K, E[\ell^\infty])$$

Since $\Lambda^a_{\ell^{n+k+1}} \subset \Lambda^a_{\ell^{n+k}}$, we have

$$V^a_{0,\ell^n} \supset V^a_{1,\ell^n} \supset V^a_{2,\ell^n} \supset \cdots.$$

We have $\ell\tau_{\lambda,\ell^{n+1}} = \tau_{\lambda,\ell^n}$, because the following diagram commutes, with $G = \mathrm{Gal}(K_\lambda/K)$:

$$\begin{tikzcd}
(E(K_\lambda)/\ell^{k+n+1}E(K_\lambda))^G \arrow[r, hook] & \mathrm{H}^1(K_\lambda, E[\ell^{k+n+1}])^G \\
(E(K_\lambda)/\ell^{k+n}E(K_\lambda))^G \arrow[r, hook] \arrow[u, "{[\ell]}"] & \mathrm{H}^1(K_\lambda, E[\ell^{k+n}])^G \arrow[u]
\end{tikzcd}$$

Thus $\ell V^a_{k,\ell^{n+1}} \subset V^a_{k,\ell^n}$.

We say $\{\tau_{\lambda,\ell^n}\}$ is a *strong nonzero system* if there exists $a \geq 0$ such that for all $k \geq k_0$ there exists n such that $V^a_{k,\ell^n} \neq 0$. In other words, if one continues the grid of subgroups of $\mathrm{H}^1(K, E[\ell^\infty])$ below infinitely far to the right and up in the obvious way, then it is *not* the case that sufficiently far to the right every single group is 0.

$$\begin{tikzcd}
\vdots & \vdots & \vdots & \\
V^a_{0,\ell^3} & V^a_{1,\ell^3} \arrow[l] & V^a_{2,\ell^3} \arrow[l] & \cdots \arrow[l] \\
V^a_{0,\ell^2} & V^a_{1,\ell^2} \arrow[l] & V^a_{2,\ell^2} \arrow[l] & \cdots \arrow[l] \\
V^a_{0,\ell} & V^a_{1,\ell} \arrow[l] & V^a_{2,\ell} \arrow[l] & \cdots \arrow[l]
\end{tikzcd}$$

Conjecture 4.6 (Kolyvagin's Conjecture B_ℓ)**.** *$\{\tau_{\lambda,\ell^n}\}$ is a strong nonzero system.*

Remark 4.7. *Kolyvagin remarks [Kol91a, pg. 258] that if $\ell \in B(E)$, then $\{\tau_{\lambda,\ell^n}\}$ is a strong nonzero system if and only if there exists n such that $V^a_{0,\ell^n} \neq 0$. By Lemma 4.5, this is the case if and only if some τ is nonzero. So for $\ell \in B(E)$, Conjectures 4.1 is true if and only if Conjecture 4.6 is true.*

The following conjecture is motivated by Theorem 4.2 and the conjecture that $\text{Ш}(E/K)$ is finite.

Conjecture 4.8 (Kolyvagin's Conjecture C)**.** *The set of primes ℓ such that $m_\ell \neq 0$ is finite.*

Let $r_{\mathrm{an}} = \mathrm{ord}_{s=1} L(E,s)$, and let $\varepsilon = (-1)^{r_{\mathrm{an}}-1}$. For any module A with an action of complex conjugation σ, and $\nu \in \{0,1\}$, let $A^\nu = (1-(-1)^\nu \varepsilon\sigma)A$.

Conjecture 4.9 (Kolyvagin's Conjecture D_ℓ)**.** *There exists $\nu \in \{0,1\}$ and a subgroup $V \subset (E(K)/E(K)_{\mathrm{tor}})^\nu$ such that $1 \leq \mathrm{rank}(V) \equiv \nu \pmod 2$ and for all $n \geq 1$ and all sufficiently large k, one has*

$$V^a_{k,\ell^n} \equiv V \pmod{\ell^n(E(K)_{/\,\mathrm{tor}})},$$

where $a = \mathrm{rank}(V) - 1$.

The following conjecture is the natural generalization to higher rank of the hypothesis when $r_{\mathrm{an}}(E/\mathbb{Q}) = 1$ that the Hegner point y_K has infinite order.

Conjecture 4.10 (Kolyvagin's Conjecture D)**.** *There exists a single subgroup V of $E(K)$ such that Conjecture 4.9 holds simultaneously for all ℓ with that V.*

Conjecture 4.9 has numerous consequences. Much of the following proposition is implicitly stated without any proofs in [Kol91a, pg. 258–259], so we give complete proofs below.

Proposition 4.11. *Assume our running minimality hypothesis that $r_{\mathrm{an}}(E/\mathbb{Q}) > r_{\mathrm{an}}(E^D/\mathbb{Q}) \leq 1$. Suppose Conjecture 4.9 is true for $\ell \in B(E)$ and let $f = f_\ell$. Then*

1. $(E(K)/E(K)_{\mathrm{tor}})^\nu = (E(K)/E(K)_{\mathrm{tor}})^+$,
2. $a = f$,
3. $\mathrm{rank}(E(\mathbb{Q})) = f + 1$,
4. $\text{Ш}(E/K)(\ell)$ *is finite,*
5. $r_{\mathrm{an}}(E/\mathbb{Q}) \equiv \mathrm{rank}(E(\mathbb{Q})) \pmod 2$, *and*
6. $V \otimes \mathbb{Z}_\ell = \ell^{m_f} E(\mathbb{Q}) \otimes \mathbb{Z}_\ell$.

Proof. By Conjecture 4.9, there exists $\nu \in \{0,1\}$ and a subgroup $V \subset (E(K)/E(K)_{\mathrm{tor}})^\nu$ such that $1 \leq \mathrm{rank}(V) \equiv \nu \pmod 2$ and for all $n > 0$ and all sufficiently large k we have

$$V^a_{k,\ell^n} \equiv V \pmod{\ell^n E(K)_{\mathrm{tor}}},$$

where $a = \mathrm{rank}(V) - 1$.

If $\mathrm{rank}(V) = 1$, then $a = 0$, so $V^0_{k,\ell^n} \neq 0$ for some k, so since f is the smallest integer such that $V^f_{k,\ell^n} \neq 0$, this implies that $f = 0$ giving Part 2; thus the Heegner point y_K has infinite order and $r_{\mathrm{an}}(E/K) = 1$. Since $r_{\mathrm{an}}(E/\mathbb{Q}) > r_{\mathrm{an}}(E^D/\mathbb{Q})$, we have $r_{\mathrm{an}}(E/\mathbb{Q}) = 1$ and $r_{\mathrm{an}}(E^D/\mathbb{Q}) = 0$, so Parts 1,3,4, 5 follows. Finally, Part 6 follows since V^0_{k,ℓ^n} is just the image of the Heegner point y_K under the connecting homomorphism, and $\mathrm{ord}_\ell(y_K) = m_f$.

Next assume that $\mathrm{rank}(V) > 1$. By our minimality hypothesis, $r_{\mathrm{an}}(E^D/\mathbb{Q}) \leq 1$, so $\mathrm{rank}(E^D(\mathbb{Q})) \leq 1$, hence $V \not\subset (E(K)/E(K)_{\mathrm{tor}})^-$, so $V \subset (E(K)/E(K)_{\mathrm{tor}})^+$, which proves Part 1. We have $f \leq a$ since $V^a_{k,\ell^n} \neq 0$ for some $k \geq 0$. Also, since $f < \infty$, Theorem 4.2 implies that $\mathrm{rank}(E(\mathbb{Q})) \leq f+1$. Since $\mathrm{rank}((E(K)/E(K)_{\mathrm{tor}})^+) = \mathrm{rank}(E(\mathbb{Q}))$, we have

$$a+1 = \mathrm{rank}(V) \leq \mathrm{rank}(E(\mathbb{Q})) \leq f+1 \leq a+1.$$

We conclude that the above inequalities are equalities, so $a = f$ which proves Part 2, and $\mathrm{rank}(E(\mathbb{Q})) = f+1$, which proves Part 3. Also because $\mathrm{rank}(E(\mathbb{Q})) = f+1$, Theorem 4.2 implies that $\text{Ш}(E/\mathbb{Q})(\ell)$ is finite, so since $\text{Ш}(E^D/\mathbb{Q}))$ is also finite, Part 4 is true. Considering the definition of the A^ν before the statement of Conjecture 4.9, we see that $1-(-1)^\nu(-1)^{r_{\mathrm{an}}-1}\sigma = 1+\sigma$, so $\nu \equiv r_{\mathrm{an}} \pmod 2$. Since part of Conjecture 4.9 is that $\mathrm{rank}(V) \equiv \nu \pmod 2$, and we proved that $\mathrm{rank}(V) = \mathrm{rank}(E(\mathbb{Q}))$, we conclude that $r_{\mathrm{an}} \equiv \mathrm{rank}(E(\mathbb{Q})) \pmod 2$, which is Part 5. By [Kol91a, Thm. 3], for all $k \geq m_f$ the subgroup $V^f_{k,\ell^n} \subset \mathrm{H}^1(K, E[\ell^\infty])$ contains $(\ell^{m_f}\mathbb{Z}/\ell^n\mathbb{Z})^{f+1} = \delta(\ell^{m_f}E(\mathbb{Q}))$, so $\ell^{m_f}E(\mathbb{Q}) \otimes \mathbb{Z}_\ell \subset V \otimes \mathbb{Z}_\ell$. On the other hand, by definition of m_f, every cohomology class τ_{λ,ℓ^n} is contained in $\ell^{m_f}\,\mathrm{H}^1(K, E[\ell^n])$. Thus $\delta(V) \subset \ell^{m_f}\,\mathrm{H}^1(K, E[\ell^\infty])$, so $V \subset \ell^{m_f}E(\mathbb{Q})$. This proves Part 6.

□

Recall from Section 2 that c is the Manin constant of E and the c_q are the Tamagawa numbers of E. We make the following new refinement of Kolyvagin's Conjecture 4.8.

Conjecture 4.12. *We have* $m_\ell = \mathrm{ord}_\ell(c \cdot \prod_{q|N} c_q)$.

Theorem 7.5 and Theorem 7.7 below serve as our motivation to make Conjecture 4.12. In particular, Kolyvagin proved that at primes $\ell \in B(E)$, Conjecture 4.12 is equivalent to [GZ86, Conj 2.2, pg 311] in the special case when E has analytic rank 1 over K.

5 Mod p Kolyvagin Points and Kolyvagin Subgroups

As always, we assume E is an elliptic curve over $\mathbb{Q}$, that K is a quadratic imaginary field satisfying the Heegner hypothesis, and p is a prime that is inert in K. The Heegner hypothesis implies that the primes of bad reduction for E split in K, so p must be a prime of good reduction. For each such prime, we define a finite-index subgroup W_p of $E(K)$. We do this by extending Kolyvagin's construction of points P_λ to obtain a new well-defined construction of elements of the quotient group

$$E(\mathbb{F}_p)/(p+1) = E(\mathbb{F}_p)/(p+1)E(\mathbb{F}_p)$$

for any inert prime p. Thus this section takes Kolyvagin's definition of points P_λ one step further to define elements of $E(\mathbb{F}_p)/(p+1)$. We first compute the structure of the odd part of the group $E(\mathbb{F}_p)/(p+1)$ for any good prime p. We then use properties of splitting of primes in certain ring class fields to define the canonical reduction $R_{p,\lambda} \in E(\mathbb{F}_p)/(p+1)$ of the Kolyvagin points P_λ, and consider the subgroup X_p of $E(\mathbb{F}_p)/(p+1)$ generated by the $R_{p,\lambda}$ for certain λ. We then define W_p to be the inverse image of X_p and finish with some results about the structure of W_p.

If A is a finite abelian group, the *odd part* of A is the subgroup of A of all elements of odd order, and if n is an integer, the odd part of n is $n/2^{\mathrm{ord}_2(n)}$.

Lemma 5.1. *The odd part of* $E(\mathbb{F}_p)/(p+1)$ *is cyclic of order the odd part of* $\gcd(p+1, a_p)$.

Proof. Suppose ℓ is an odd prime divisor of $\#(E(\mathbb{F}_p)/(p+1))$. If the ℓ-primary subgroup of $E(\mathbb{F}_p)/(p+1)$ is not cyclic, then since $\ell \neq p$ we have $E(\mathbb{F}_p)[\ell] \approx (\mathbb{Z}/\ell\mathbb{Z})^2$. The Weil pairing induces an isomorphism of Galois modules $\bigwedge^2 E[\ell] \cong \mu_\ell$ and $E[\ell] \subset E(\mathbb{F}_p)$, so $\mu_\ell \subset \mathbb{F}_p^*$, hence $\ell \mid (p-1)$. Since ℓ divides $\#(E(\mathbb{F}_p)/(p+1))$ and ℓ is prime, we have $\ell \mid (p+1)$, so $\ell \mid \gcd(p-1, p+1) = 2$, a contradiction, since ℓ is odd.

The group $E(\mathbb{F}_p)$ has order $p+1-a_p$, and we just proved above that $E(\mathbb{F}_p)(\ell)$ is cyclic for any odd prime divisor ℓ of $p+1$. Thus the quotient ℓ-primary group $(E(\mathbb{F}_p)/(p+1))(\ell) = (E(\mathbb{F}_p)(\ell))/(p+1)$ has order ℓ^m, where

$$m = \mathrm{ord}_\ell(\gcd(p+1, \#E(\mathbb{F}_p))) = \mathrm{ord}_\ell(\gcd(p+1, p+1-a_p)) = \mathrm{ord}_\ell(\gcd(p+1, a_p)).$$

Taking the product over all odd primes ℓ, shows that the odd part of $E(\mathbb{F}_p)/(p+1)$ has order the odd part of $\gcd(p+1, a_p)$. □

Remark 5.2. *1. Lemma 5.1 is true even if p is a good prime that is not inert in K (in fact, the lemma and proof have nothing to do with K).*

2. Lemma 5.1 is false if we do not restrict to odd parts. For example, if E is $y^2 = x^3 - x$ and $p = 3$, then $E(\mathbb{F}_3) \approx (\mathbb{Z}/2\mathbb{Z})^2$, so $E(\mathbb{F}_3)/4 \approx (\mathbb{Z}/2\mathbb{Z})^2$ is not cyclic.

3. For every prime ℓ, there exists infinitely many primes p such that $E(\mathbb{F}_p)(\ell)$ is not cyclic. Indeed, by the Chebotarev density theorem there are infinitely many p that split completely in the field $\mathbb{Q}(E[\ell])$, and for these p we have $(\mathbb{Z}/\ell\mathbb{Z})^2 \subset E(\mathbb{F}_p)$.

Lemma 5.3. *If p is inert in K and does not divide λ, then the prime ideal $p\mathcal{O}_K$ of K splits completely in K_λ. In particular, if $p \in \Lambda^1_{\ell^n}$ and $\lambda \in \Lambda_{\ell^n}$ with $p \nmid \lambda$, then $p\mathcal{O}_K$ splits completely in K_λ.*

Proof. (Compare line -3 on page 103 of [Kol91b].) Since p is inert, the ideal $p\mathcal{O}_K$ is a prime principal ideal of $\mathcal{O}_K$, hence splits completely in the Hilbert class field K_1. As explained in [Gro91, pg. 238], class field theory identifies $\mathrm{Gal}(K_\lambda/K_1)$ with $C = (\mathcal{O}_K/\lambda\mathcal{O}_K)^*/(\mathbb{Z}/\lambda\mathbb{Z})^*$. The image of p is trivial in C, so the Frobenius element attached to $p\mathcal{O}_K$ is trivial, hence $p\mathcal{O}_K$ splits completely in the ring of integers of K_λ, as claimed. □

Define the reduction map $E(K) \to E(\mathbb{F}_{p^2})$ by reducing the Néron model $\mathcal{E}$ of E over $\mathcal{O}_K$ modulo $p\mathcal{O}_K$, and using the natural maps $E(K) \cong \mathcal{E}(\mathcal{O}_K) \to \mathcal{E}_{\mathbb{F}_{p^2}}(\mathbb{F}_{p^2}) \cong E(\mathbb{F}_{p^2})$. Let $\pi_p : E(K) \to E(\mathbb{F}_p)/(p+1)$ be the composition of reduction modulo the prime ideal $p\mathcal{O}_K$ with $\mathrm{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p} : E(\mathbb{F}_{p^2}) \to E(\mathbb{F}_p)$ followed by quotienting out by the subgroup $(p+1)E(\mathbb{F}_p)$. Fix a *choice* $\wp$ of prime ideal of K_λ over $p\mathcal{O}_K$. Extend π_p to a map $\pi_\wp : E(K_\lambda) \to E(\mathbb{F}_p)/(p+1)$ by quotienting out by $\wp$, as illustrated in the following diagram:

$$\begin{tikzcd}
E(K_\lambda) \arrow[drr, "\mathrm{mod}\ \wp"] & & \\
E(K) \arrow[u] \arrow[r, "\cong"] \arrow[dddrr, dotted, "\pi_p"'] & \mathcal{E}(\mathcal{O}_K) \arrow[r] & E(\mathbb{F}_{p^2}) \arrow[d, "\text{trace}"] \\
& & E(\mathbb{F}_p) \arrow[dd] \\
& & \\
& & E(\mathbb{F}_p)/(p+1)
\end{tikzcd}$$

For each $\ell \mid (p+1)$, let $v_\ell = \mathrm{ord}_\ell(\gcd(a_p, p+1))$, and define $\pi_{\wp,\ell} : E(K_\lambda) \to (E(\mathbb{F}_p)/(p+1))(\ell)$ by

$$\pi_{\wp,\ell}(S) = \pi_\wp\left(\frac{p+1}{\ell^{v_\ell}} S\right).$$

We now study how the homomorphism $\pi_{\wp,\ell}$ depends on our choice of prime of $\wp$ over $p\mathcal{O}_K$.

Proposition 5.4. *The map $\pi_{\wp,\ell}$ induces a well-defined (independent of choice of $\wp$) homomorphism*

$$\vartheta : (E(K_\lambda)/\ell^{v_\ell}E(K_\lambda))^{\mathrm{Gal}(K_\lambda/K)} \to E(\mathbb{F}_p)/(p+1).$$

Proof. Let $[S] \in (E(K_\lambda)/\ell^{v_\ell}E(K_\lambda))^{\mathrm{Gal}(K_\lambda/K)}$ with $S \in E(K_\lambda)$. If $\wp'$ is another prime of K_λ over $p\mathcal{O}_K$, then because the Galois group acts transitively on the primes over a given prime, there is $\sigma \in \mathrm{Gal}(K_\lambda/K)$ such that $\pi_{\wp',\ell}(S) = \pi_{\wp,\ell}(\sigma(S))$. Since $[S]$ is $\mathrm{Gal}(K_\lambda/K)$-equivariant, we have $\sigma(S) = S + \ell^{v_\ell} \cdot Q$, for some $Q \in E(K_\lambda)$, so

$$\begin{aligned}
\vartheta([\sigma(S)]) &= \pi_{\wp,\ell}(\sigma(S)) \\
&= \pi_\wp\left(\frac{p+1}{\ell^{v_\ell}}\sigma(S)\right) \\
&= \pi_\wp\left(\frac{p+1}{\ell^{v_\ell}} S\right) + \pi_\wp((p+1)Q) \\
&= \pi_{\wp,\ell}(S) + 0 = \vartheta([S]),
\end{aligned}$$

where $\pi_\wp((p+1)Q) = (p+1)\pi_\wp(Q)$ is 0, since the group $E(\mathbb{F}_p)/(p+1)$ is killed by $p+1$. □

By Proposition 3.4, $[P_\lambda]$ is in the domain of the homomorphism ϑ of Proposition 5.4.

Definition 5.5 (Mod p Kolyvagin Point)**.** *The* mod p Kolyvagin point *associated to $p \in \Lambda^1_{\ell^n}$ and $\lambda \in \Lambda_{\ell^n}$ is*

$$R_{p,\lambda} = \vartheta([P_\lambda]) \in E(\mathbb{F}_p)/(p+1),$$

where ϑ is as in Proposition 5.4.

As above, let $v_\ell = \mathrm{ord}_\ell(\gcd(a_p, p+1))$. For each $k \geq 0$, let

$$X_{k,p} = \left\langle R_{p,\lambda} : \lambda \in \bigcup_{\ell} \Lambda^{f_\ell}_{\ell^{v_\ell+k}} \right\rangle \subset E(\mathbb{F}_p)/(p+1) \tag{11}$$

be the subgroup generated by all mod p Kolyvagin points associated to λ that are a product of f_ℓ primes, where f_ℓ is from Equation (9). Note that the subscript of Λ in (11) is $\ell^{v_\ell+k}$, and we take the union over *all* ℓ thus obtaining a subgroup $X_{k,p}$ that need not be ℓ-primary for any ℓ, despite $R_{p,\lambda}$ being ℓ-primary. Let

$$X_p = \bigcap_{k \geq 0} X_{k,p}.$$

Let $W_{k,p}$ be the inverse image of $X_{k,p}$ under the map π_p:

$$W_{k,p} = \pi_p^{-1}(X_{k,p}) \subset E(K),$$

and

$$W_p = \pi_p^{-1}(X_p) \subset E(K).$$

Since $E(\mathbb{F}_p)/(p+1)$ is finite, $W_{k,p}$ and W_p have finite index in $E(K)$; also, by Lemma 5.1, the odd part of this index divides $\gcd(p+1, a_p)$.

Remark 5.6. *Note that $E^D(\mathbb{Q})$ is in the kernel of the trace map, hence in the kernel of π_p, so $E^D(\mathbb{Q}) \subset W_p$. Thus it is possible that W_p contains torsion, hence W_p in general need not be a Gross-Zagier subgroup as in Definition 2.3. In a future paper, we intend to give a more refined definition of a sequence of groups W_p^a, for each $a \geq 0$, which better accounts for torsion. We would then search for a Gross-Zagier style formula for each group W_p^a for $a \leq f+1$, in order to more closely relate $r_{\mathrm{an}}(E/\mathbb{Q})$ to $f+1$.*

6 Controlling the Reduction Map

The main result of this section is a proof that under certain hypothesis, if a point Q has infinite order and n is a positive integer, then there are infinitely many primes p such that the image of Q in $E(\mathbb{F}_{p^2})/(p+1)$ has order divisible by n. We prove this using Galois cohomology and by converting a condition on ℓ-divisibility of points into a Chebotarev condition. We will use this result later to study the maximum index $[E(K) : W_p]$ that can occur and prove a generalized Gross-Zagier formula for such W_p.

Let E, K, etc., be as above, and let $\ell \in B(E)$, where $B(E)$ is the set of primes defined on page 5. Suppose $Q \in E(K)$ has infinite order, and let n be an odd positive integer. Suppose that for each prime $\ell \mid n$, the set of cardinalities $\{\# \mathrm{H}^1(K(E[\ell^j])/K, E[\ell^j]) : j \geq 1\}$ is bounded. This hypothesis is satisfied if $\ell \in B(E)$, since then $\mathrm{H}^1(K(E[\ell^j])/K, E[\ell^j]) = 0$ for all j (see [Gro91, pg. 241] and [GJP+09, Prop. 5.2]).

Proposition 6.1. *Let Q and n be as above. Let S be the set of primes p such that p is inert in K, p splits completely in $K(E[n])/K$, and the image of Q in $E(\mathbb{F}_{p^2})/(p+1)E(\mathbb{F}_{p^2})$ has order divisible by n. Then S has positive (Dirichlet) density.*

Proof. Let $m = \prod \ell_i^{e_i}$ with ℓ_i the distinct primes that divide n, and e_i any positive integers, which we will fix later in the argument. Fix any i, and let $L = K(E[\prod_{j \neq i} \ell_j])$, which is a Galois extension of K. Define homomorphisms Ψ_i, f, g, and h as in the following commutative diagram:

$$\begin{tikzcd}
E(K(E[m]))/\ell_i^{e_i} E(K(E[m])) \arrow[r, hook] & \mathrm{H}^1(K(E[m]), E[\ell_i^{e_i}]) \\
 & \mathrm{H}^1(L(E[\ell_i^{e_i}]), E[\ell_i^{e_i}]) \arrow[u, "f"] \\
 & \mathrm{H}^1(K(E[\ell_i^{e_i}]), E[\ell_i^{e_i}]) \arrow[u, "h"] \\
E(K)/\ell_i^{e_i} E(K) \arrow[uuu] \arrow[r, hook] \arrow[uuur, dotted, "\psi_i"] & \mathrm{H}^1(K, E[\ell_i^{e_i}]) \arrow[u, "g"]
\end{tikzcd}$$

The horizontal maps above are induced by the short exact sequence coming from multiplication by $\ell_i^{e_i}$, and the vertical maps on the right are the restriction maps. The diagram commutes so the order of the image of Q in $E(K(E[m]))/\ell_i^{e_i}E(K(E[m]))$ is the same as the order of $\Psi_i(Q)$.

By hypothesis and the inflation restriction sequence the cardinality of $\ker(g)$ is bounded independently of i and e_i. Also, $[L:K]$ depends only on the set of prime divisors ℓ_i of n, not their exponents, so

$$\#\ker(h) = \#\,\mathrm{H}^1(L(E[\ell_i^{e_i}])/K(E[\ell_i^{e_i}]), E[\ell_i^{e_i}]) = \#\,\mathrm{Hom}(\mathrm{Gal}(L(E[\ell_i^{e_i}])/K(E[\ell_i^{e_i}])), E[\ell_i^{e_i}])$$

is also bounded independent of e_i, because every homomorphism has image in the fixed subset $E[\ell_i^d]$, where d is the exponent of the group $\mathrm{Gal}(L/K)$. Finally, the map f is injective, since

$$\ker(f) \cong \mathrm{H}^1(K(E[m])/L(E[\ell_i^{e_i}]), E[\ell_i^{e_i}])$$

and $\#\,\mathrm{Gal}(K(E[m])/L(E[\ell_i^{e_i}]))$ is divisible only by the primes ℓ_j for $j \neq i$ and these are all coprime to $\#E[\ell_i^{e_i}] = \ell_i^{2e_i}$. We conclude that there is an integer b such that $\#\ker(\Psi_i) \leq \ell_i^b$, and this bound holds no matter how we increase the numbers e_i and e_j (for all j).

The above proof that $\ker(\Psi_i)$ is uniformly bounded is completely general. See Remark 6.3 for a sketch of an alternative proof of this bound in the special case when $\ell \in B(E)$ for all $\ell \mid n$, which is the only case we will use in this paper.

Because $\ker(\Psi_i)$ is uniformly bounded independent of our choice of e_i, for each i, we can choose e_i large enough so that $\Psi_i(Q)$ has order divisible by $\ell_i^{\mathrm{ord}_{\ell_i}(n)}$. Then for each i, let d_i be maximal such that $\ell_i^{d_i}$ divides Q in $E(K(E[m]))$. Note that $d_i < e_i$ for each i, since $\Psi_i(Q) \neq 0$ and $\Psi(Q)$ is an element of a group that is killed by $\ell_i^{e_i}$. Since $m = \prod \ell_i^{e_i}$, we have $\ell_i^{d_i+1} \mid m$, so

$$M_i = K\left(E[m],\ \frac{1}{\ell_i^{d_i+1}}Q\right)$$

does not depend on the choice of $\ell_i^{d_i+1}$th root of Q, is a Galois extension of $K(E[m])$, and $[M_i : K(E[m])]$ is a nontrivial power of ℓ_i. Thus the M_i for all i are linearly disjoint as extensions of $K(E[m])$.

Let M be the compositum of the fields M_i defined above. Since the M_i are linearly disjoint nontrivial extensions of $K(E[m])$, there exists an automorphism $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$ such that $\sigma|_{K(E([m]))}$ is complex conjugation, and $\sigma|_{M_i}$ has order divisible by ℓ_i for each i. By the Chebotarev density theorem, there is a positive density of primes $p \in \mathbb{Z}$ that are unramified in M and have Frobenius the class of σ. Such primes are inert in K since complex conjugation acts nontrivially on K, split completely in $K(E[m])/K$ since complex conjugation has order 2, and each prime over p in $K(E[m])$ does not split completely in any of the extensions $M_i/K(E[m])$ since $[\mathrm{Frob}_p]|_{M_i} = \sigma|_{M_i}$ has order divisible by $\ell_i > 2$. Note that this is the only place in the argument where we use that n is odd.

Let p be any prime as in the previous paragraph. We have

$$E(\mathbb{F}_{p^2})/\ell_i^{e_i}E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/\ell_i^{e_i}\mathbb{Z})^2$$

since $p\mathcal{O}_K$ splits completely in $K(E[m])$ and $\ell_i^{e_i} \mid m$. Also, the Frobenius condition implies that the primes of M_i over $p\mathcal{O}_K$ do not have residue class degree 1, so since M_i is generated by any choice of $\frac{1}{\ell^{d_i+1}}Q$, the reduction $\overline{Q}$ of Q modulo any prime over $p\mathcal{O}_K$ is not divisible by $\ell_i^{d_i+1}$ in $E(\mathbb{F}_{p^2})$. Note that $\ell_i^{d_i}$ divides $\overline{Q}$, because the prime $p\mathcal{O}_K$ splits completely in $K(E[m])/K$ and $\ell_i^{d_i}$ divides Q in $K(E[m])$, so d_i is the largest integer such that $\ell_i^{d_i}$ divides the image of $\overline{Q}$ in $E(\mathbb{F}_{p^2})$. We conclude that for each i the image of Q in $E(\mathbb{F}_{p^2})/\ell_i^{e_i}E(\mathbb{F}_{p^2})$ has order the same as the order of $\Psi_i(Q)$.

By hypothesis, $e_i \geq \mathrm{ord}_{\ell_i}(n)$ and $\Psi_i(Q)$ has order divisible by $\ell_i^{\mathrm{ord}_{\ell_i}(n)}$ for each i, so the image of Q in $E(\mathbb{F}_{p^2})/mE(\mathbb{F}_{p^2})$ has order divisible by n. For any such p, we also have that the characteristic polynomial of the class of Frob_p in $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ acting on $E[m]$ is $x^2 - a_px + p \pmod{m}$. On the other hand, since $[\mathrm{Frob}_p]$ on $E[m]$ is the class of complex conjugation and complex conjugation acts nontrivially (since m is odd) hence has characteristic polynomial $x^2 - 1$, we have $x^2 - a_px + p \equiv x^2 - 1 \pmod{m}$. Thus $m \mid (p+1)$, so the image of Q in $E(\mathbb{F}_{p^2})/(p+1)E(\mathbb{F}_{p^2})$ also has order divisible by n, which completes the proof. □

Remark 6.2. *Proposition 6.1 is analogous to the statement that if $x, n \in \mathbb{Z}$ with $\gcd(n,x) = 1$ and $\mathbb{Q}(\zeta_n, \sqrt[n]{x})$ is an extension of $\mathbb{Q}(\zeta_n)$ of degree n, then there exist a positive density of primes p such that the multiplicative order of x modulo p is divisible by n. The proof of this statement resembles the proof of Proposition 6.1, except we work with the field $\mathbb{Q}(\zeta_n, \sqrt[n]{x})$. The idea of the proof of Proposition 6.1 is well-known to experts who study questions such as the Lang-Trotter conjecture about reduction of points on elliptic curves.*

Remark 6.3. *If for every prime $\ell \mid n$ we have $\ell \in B(E)$, we can alternatively use that $K(E[\ell_1^\infty])$ and $K(E[\ell_2^\infty])$ are linearly disjoint for distinct odd primes ℓ_1 and ℓ_2 in $B(E)$ to give a different proof that the maps Ψ_i have uniformly bounded kernel in Proposition 6.1. In that case we have that $\mathrm{Gal}(K(E[n])/K) \approx \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, so*

$$\ker\Big(\mathrm{H}^1(K, E[n]) \to \mathrm{H}^1(K(E[n]), E[n])\Big) \cong \mathrm{H}^1(K(E[n])/K, E[n]) = \mathrm{H}^1(\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}), (\mathbb{Z}/n\mathbb{Z})^2) = 0,$$

where the last group is 0 by a standard group cohomology argument (see, e.g., [Ste02, §5.1]). This implies that the maps Ψ_i are all injective. The linear disjointness of $K(E[\ell_1^\infty])$ and $K(E[\ell_2^\infty])$ for the distinct odd *primes ℓ_1 and ℓ_2 follows by a Galois theory argument using the structure of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. We thank R. Greenberg for this observation.*

7 Maximal Index Subgroups W_p

As above, we assume that E is an elliptic curve over $\mathbb{Q}$ with positive analytic rank and that $K = \mathbb{Q}(\sqrt{D})$ is a quadratic imaginary field that satisfies the Heegner hypothesis and the minimality hypothesis that $r_{\mathrm{an}}(E/\mathbb{Q}) > r_{\mathrm{an}}(E^D/\mathbb{Q}) \leq 1$.

Recall that for each inert prime p of K we defined a subgroup $X_p \subset E(\mathbb{F}_p)/(p+1)$ in Equation (11) of Section 5. This was a group got by reducing Kolyvagin points associated to all primes ℓ modulo a choice of prime over p. In this section, for all $\ell \in B(E)$ we conditionally compute, in terms of $m_{\ell,f}$, the ℓ-primary part $X_p(\ell)$ of this subgroup $X_p \subset E(\mathbb{F}_p)/(p+1)$. We relate our refinement of Kolyvagin's conjectures to the generalized Gross-Zagier formula (5). We also conditionally compute X_p in terms of $c \cdot \prod c_q \cdot \sqrt{\#Ш(E/K)}$ using Theorem 4.2. We apply our description of X_p to prove that, up to primes not in $B(E)$, the subgroups W_p with $[E(K) : W_p]$ maximal are all Gross-Zagier subgroups of $E(K)$.

Proposition 7.1. *Conjecture 4.9 implies that for every $\ell \in B(E)$,*

$$X_p(\ell) = \frac{p+1}{\ell^{v_\ell}} \cdot \pi_p(\ell^{m_{\ell,f}} E(\mathbb{Q})),$$

where $v_\ell = \mathrm{ord}_\ell(p+1)$.

Proof. Let Φ be the composite homomorphism

$$(E(K_\lambda)/\ell^{v_\ell} E(K_\lambda))^{\mathrm{Gal}(K_\lambda/K)} \hookrightarrow \mathrm{H}^1(K_\lambda, E[\ell^{v_\ell}])^{\mathrm{Gal}(K_\lambda/K)} \cong \mathrm{H}^1(K, E[\ell^{v_\ell}]),$$

and let $\delta : E(K) \to \mathrm{H}^1(K, E[\ell^{v_\ell}])$. We are assuming Conjecture 4.9, so we may apply Proposition 4.11 Part 6 (taking into account Lemma 4.5), to see that for all k sufficiently large we have $\delta(\ell^{m_{\ell,f}} E(\mathbb{Q})) = V^f_{k,\ell^{v_\ell}}$. Thus

$$\delta(\ell^{m_{\ell,f}} E(\mathbb{Q})) = \langle \Phi([P_\lambda]) : \lambda \in \Lambda^f_{\ell^{v_\ell + k}} \rangle.$$

Let $i : E(K) \to (E(K_\lambda)/\ell^{v_\ell} E(K_\lambda))^{\mathrm{Gal}(K_\lambda/K)}$. For any $Q \in E(K)$ we have $\frac{p+1}{\ell^{v_\ell}} \cdot \pi_p(Q) = \vartheta(i(Q))$ where ϑ is as in Proposition 5.4. Since $\delta = \Phi \circ i$ and Φ is injective, the group $X_{k,p}(\ell)$ generated by all $\vartheta([P_\lambda])$ is equal to $\vartheta(i(\ell^{m_{\ell,f}} E(\mathbb{Q})))$. Since this is true for all sufficiently large k, the proposition follows for X_p. □

Theorem 7.5 below generalizes [Kol91b, Thm. E] to arbitrary rank. To prove it we first prove some lemmas and make a definition.

Lemma 7.2. *Suppose A is a nonzero finitely generated free abelian group and $\varphi : A \to \mathbb{Z}/d\mathbb{Z}$ is a surjective homomorphism. For every nonzero integer c we have $[A : \varphi^{-1}(\varphi(cA))] = \gcd(c, d)$.*

Proof. Let $B = \varphi^{-1}(\varphi(cA))$. We have $\varphi(\ker(\varphi)) = 0 \subset \varphi(cA)$, so $\ker(\varphi) \subset B$. Since $\ker(\varphi) \subset B$, the isomorphism $A/\ker(\varphi) \cong \mathbb{Z}/d\mathbb{Z}$ induces an isomorphism $A/B \cong (\mathbb{Z}/d\mathbb{Z})/\varphi(B)$. But φ is surjective, so $\varphi(B) = \varphi(\varphi^{-1}(\varphi(cA))) = \varphi(cA) = c\varphi(A) = c(\mathbb{Z}/d\mathbb{Z})$, so $A/B \cong (\mathbb{Z}/d\mathbb{Z})/(c(\mathbb{Z}/d\mathbb{Z})) \cong \mathbb{Z}/\gcd(d,c)\mathbb{Z}$. □

Recall (see page 5) that $B(E)$ is a set of primes that have certain good properties for E. Below, for any integer n we either let $n' = \ell^{\mathrm{ord}_\ell(n)}$ be the ℓ-part of n or the maximal divisor of n divisible only by primes in $B(E)$, depending on whether we are considering the first or second part of the following lemma.

Lemma 7.3. *Assume $E(\mathbb{Q})$ has positive rank and let t be a positive integer.*

1. *If $\ell \in B(E)$ is such that $X_p(\ell) = \frac{p+1}{\ell^{v_\ell}} \cdot \pi_p(tE(\mathbb{Q}))$ for all inert primes p, then*

$$\max\{\mathrm{ord}_\ell([E(K) : W_p]) : \text{ all inert } p\} = \mathrm{ord}_\ell(t).$$

2. If for all $\ell \in B(E)$ we have $X_p(\ell) = \frac{p+1}{\ell^{v_\ell}} \cdot \pi_p(tE(\mathbb{Q}))$ for all inert primes p, then

$$\max\{[E(K) : W_p]' : \text{ all inert } p\} = t'.$$

Proof. Let p be any inert prime, and recall that p is a prime of good reduction, since all bad primes split in K. By Lemma 5.1, the odd part of the image of $\pi_p : E(K) \to E(\mathbb{F}_p)/(p+1)$ is a cyclic group $\mathbb{Z}/n\mathbb{Z}$ for some integer n. Since $\pi_p(E^D(\mathbb{Q})) = 0$ (see Remark 5.6), we have

$$\pi_p(tE(\mathbb{Q}))' = \pi_p(tE(\mathbb{Q}) + tE^D(\mathbb{Q}))' = \pi_p(tE(K))',$$

so by Proposition 7.6, $W_p' = \pi_p^{-1}(X_p)' = \pi_p^{-1}(\pi_p(tE(K))')$. Thus Lemma 7.2 implies that $[E(K)' : W_p']$ is $\gcd(t,n)'$. This proves that set of indexes $[E(K)' : W_p']$ all divide t'.

We show the maximum equals t' by proving that there is a positive density of primes p such that the n above is divisible by t'. By hypothesis, there is a point $P \in E(\mathbb{Q})$ of infinite order. By Proposition 6.1, there exists a positive density of primes p that are inert in K such that $\pi_p(P) \in E(\mathbb{F}_p)/(p+1)$ has order divisible by t'. For such p, the n above is thus divisible by t', so $\gcd(t,n)' = t'$, which completes the proof. □

Let

$$w_\ell = \sup(\{\mathrm{ord}_\ell([E(K) : W_p]) : \text{ all inert } p\}) \leq \infty. \tag{12}$$

Lemma 7.4. *Suppose $\ell \in B(E)$, that Conjecture 4.9 is true for E, and assume that p is an inert prime such that $\mathrm{ord}_\ell([E(K) : W_p])$ is maximal in the sense that it equals w_ℓ. Then $m_{\ell,f} = \mathrm{ord}_\ell([E(K) : W_p])$.*

Proof. We are assuming that Conjecture 4.9 is true, so Proposition 7.1 applies and gives an explicit formula for $X_p(\ell)$. Namely, we may take $t = m_{\ell,f}$ in Lemma 7.3. Also, by Conjecture 4.9 (and Proposition 4.11) we have $E(\mathbb{Q})$ has rank at least 1. The lemma then follows from Lemma 7.3. □

Theorem 7.5. *Suppose $\ell \in B(E)$, that Conjectures 2.2 and 4.9 are true for E, and that p is an inert prime such that $w_\ell = \mathrm{ord}_\ell([E(K) : W_p])$, where w_ℓ is as in* (12) *above. Then W_p satisfies the generalized Gross-Zagier formula* (5) *up to a rational factor that is coprime to ℓ if and only if Conjecture 4.12 is true for ℓ.*

Proof. We are assuming Conjecture 4.9, which implies Conjecture 4.1, so we may apply Theorem 4.2, which has Conjecture 4.1 as a hypothesis. Let b_k be as in Theorem 4.2 for our given prime ℓ. Theorem 4.2 implies that

$$\begin{aligned}\#\text{Ш}(E/K)(\ell) &= \#((\mathbb{Z}/b_f\mathbb{Z})^2 \oplus (\mathbb{Z}/b_{f+1}\mathbb{Z})^2 \oplus (\mathbb{Z}/b_{f+2}\mathbb{Z})^2 \oplus \cdots) \\ &= (b_f \cdot b_{f+1} \cdots)^2 \\ &= \ell^{2(m_{\ell,f} - m_{\ell,f+1} + m_{\ell,f+1} - m_{\ell,f+2} + m_{\ell,f+2} - \cdots)} \cdots \\ &= \ell^{2(m_{\ell,f} - m_\ell)},\end{aligned}$$

so $m_{\ell,f} - m_\ell = \mathrm{ord}_\ell(\sqrt{\#\text{Ш}(E/K)(\ell)})$.

We will now show that the generalized Gross-Zagier formula (5) holds up to a rational factor that is coprime to ℓ if and only if Conjecture 4.12 that $m_\ell = \mathrm{ord}_\ell(c\prod c_q)$ is true for ℓ. We will repeatedly use Lemma 7.4 that $m_{\ell,f} = \mathrm{ord}_\ell([E(K) : W_p])$.

First, suppose that the generalized Gross-Zagier formula (5) holds up to a rational factor that is coprime to ℓ. Proposition 2.4 combined with Conjecture 2.2 (that $\text{Ш}_{\mathrm{an}} = \#\text{Ш}$), implies that this hypothesis means that $\mathrm{ord}_\ell([E(K) : W_p]) = \mathrm{ord}_\ell\left(c\prod c_q \cdot \sqrt{\#\text{Ш}(E/K)(\ell)}\right)$. Thus:

$$\begin{aligned}m_{\ell,f} &= \mathrm{ord}_\ell([E(K) : W_p]) \\ &= \mathrm{ord}_\ell\left(c\prod c_q \cdot \sqrt{\#\text{Ш}(E/K)(\ell)}\right) \\ &= \mathrm{ord}_\ell\left(c\prod c_q\right) + \mathrm{ord}_\ell(\sqrt{\#\text{Ш}(E/K)(\ell)}) \\ &= \mathrm{ord}_\ell\left(c\prod c_q\right) + m_{\ell,f} - m_\ell,\end{aligned}$$

where in the last equality we use the formula for $\#\text{Ш}(E/K)(\ell)$ that we derived above using Theorem 4.2. Subtracting $m_{\ell,f}$ from both sides shows that $m_\ell = \mathrm{ord}_\ell(c\prod c_q)$.

Conversely, suppose that $m_\ell = \mathrm{ord}_\ell(c\prod c_q)$. From Theorem 4.2 we have

$$m_{\ell,f} - m_\ell = \mathrm{ord}_\ell(\sqrt{\#\text{Ш}(E/K)(\ell)}),$$

so

$$\mathrm{ord}_\ell([E(K) : W_p]) = m_{\ell,f} = \mathrm{ord}_\ell\left(c\prod c_q\right) + m_{\ell,f} - m_\ell = \mathrm{ord}_\ell\left(c\prod c_q \cdot \sqrt{\#\text{Ш}(E/K)(\ell)}\right).$$

Proposition 2.4 then implies that W_p satisfies the generalized Gross-Zagier formula up to a rational factor coprime to ℓ. □

For any integer n, let n' denote the maximal divisor of n that is divisible only by primes in $B(E)$, and for any abelian group A, let $A' = A \otimes \mathbb{Z}[1/b]$, where b is the product of the finitely many primes not in $B(E)$. Let

$$T = c \cdot \prod_{q|N} c_q \cdot \sqrt{\#\text{Ш}(E/K)}.$$

Proposition 7.6. *Conjectures 4.9 and 4.12 together imply that* $X_p' = \pi_p(TE(\mathbb{Q}))'$.

Proof. Using the calculation in the first paragraph of the proof of Theorem 7.5 along with Conjecture 4.12 combined with Theorem 4.2, shows that for every $\ell \in B(E)$, we have

$$m_{\ell,f} = \text{ord}_\ell(T).$$

Since the integers $T/\ell^{m_{\ell,f}}$ and $(p+1)/\ell^{v_\ell}$, for $v_\ell = \text{ord}_\ell(p+1)$, both act as automorphisms on any ℓ-primary group,

$$\begin{aligned}\pi_p(TE(\mathbb{Q}))(\ell) &= \left(\frac{T}{\ell^{m_{\ell,f}}} \cdot \pi_p(\ell^{m_{\ell,f}}E(\mathbb{Q}))\right)(\ell)\\ &= \pi_p(\ell^{m_{\ell,f}}E(\mathbb{Q}))(\ell)\\ &= \frac{p+1}{\ell^{v_\ell}} \cdot \pi_p(\ell^{m_{\ell,f}}E(\mathbb{Q})) = X_p(\ell),\end{aligned}$$

where the last equality uses Proposition 7.1 (which assumes that Conjecture 4.9 is true). We conclude that $X_p' = \pi(TE(\mathbb{Q}))'$.

Theorem 7.7 is a partial converse to Theorem 7.5.

Theorem 7.7. *Assume that* $E(\mathbb{Q})$ *has positive rank. Then Conjectures 4.9 and 4.12 together imply that the maximum index* $[E(K)' : W_p']$ *over all inert* p *is* $(c \cdot \prod c_q \cdot \sqrt{\#\text{Ш}(E/K)})'$.

Proof. The conjectures we're assuming allow us to use Proposition 7.6 and hence take $t = T$ in Lemma 7.3. This proves the theorem. □

Conclusion: By Proposition 2.4, if W_p' has maximal index in $E(K)'$, then imply that we have an equality

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\|\omega\|^2}{c \cdot \sqrt{|D|}} \cdot \text{Reg}(W_p),$$

up to powers of primes not in $B(E)$. Thus the W_p' of maximal index satisfy this generalized Gross-Zagier formula.

Conjecture 7.8. *If* $W \subset E(K)$ *is* any *Gross-Zagier subgroup of index* ℓ^{w_ℓ}, *then there exists an inert prime* p *such that* W_p' *equals* W'.

8 Existence of Gross-Zagier Subgroups

Let E, K, etc., be as in Section 1.1, and let

$$t = c \cdot \prod_{q|N} c_q \cdot \sqrt{\#\text{Ш}(E/K)_{\text{an}}}.$$

In this section we investigate the analogue of the conjectures on pages 311–312 of [GZ86]. In particular, the existence of any Gross-Zagier subgroup for $E(K)$ combined with the BSD conjecture implies that $\#E(K)_{\text{tor}} \mid t$. The main theorem of [GZ86] thus led Gross-Zagier to make the following conjecture.

Conjecture 8.1 (Gross-Zagier)**.** *If* $E(K)$ *has rank* 1, *then the integer* t *is divisible by* $\#E(\mathbb{Q})_{\text{tor}}$.

Proposition 8.2. *Assume the BSD formula. If there exists any subgroup* W *of* $E(K)$ *such that the generalized Gross-Zagier formula* (5) *holds for* W, *then* $\#E(K)_{\text{tor}} \mid t$. *Note that we do not assume* W *is torsion free.*

Proof. Let W be such a subgroup. Arguing as in the proof of Proposition 2.4, we see that

$$\#E(K)^2_{\text{tor}} \cdot (\text{Reg}(W)/\text{Reg}(E/K)) = c^2 \cdot \left(\prod_{q|N} c_q\right)^2 \cdot \text{Ш}_{\text{an}} = t^2.$$

The quotient $\text{Reg}(W)/\text{Reg}(E/K)$ is a square integer, so taking square roots of both sides yields the claim.

□

Because of Proposition 8.2, we view the divisibility $\#E(K)_{\rm tor} \mid t$ as a sort of *"litmus test"* for whether there could be a generalization of the Gross-Zagier formula in general. First, we observe that the most naive generalization of Conjecture 8.1 to higher rank is *false* (!), as the following example shows.

Example 8.3. *Let E be the curve 65a of rank 1 over $\mathbb{Q}$ given by $y^2+xy=x^3-x$ and let $D=-56$. Then $\#\text{Ш}_{\rm an}(E/K)=\prod c_q = c = 1$, so $t=1$, but $\#E(\mathbb{Q})_{\rm tor}=2$. Here $E^D(\mathbb{Q})$ has rank 2, so $\operatorname{rank}(E(K))=3$, and the rank hypothesis of Conjecture 8.1 is not satisfied.*

Proposition 8.4. *Suppose $\operatorname{rank}(E(\mathbb{Q}))>0$ and that t is a positive integer. Then there exists a Gross-Zagier subgroup $W\subset E(K)$ if and only if $\#E(K)_{\rm tor}\mid t$.*

Proof. Suppose $W\subset E(K)$ is a Gross-Zagier subgroup. Then $[E(K):W]=t$. By hypothesis W is torsion free, so $E(K)_{\rm tor}\hookrightarrow E(K)/W$, so $\#E(K)_{\rm tor}\mid \#(E(K)/W)=t$.

Conversely, suppose that $\#E(K)_{\rm tor}\mid t$, and note that by hypothesis $E(\mathbb{Q})$ has positive rank. The group $E(K)/(E^D(\mathbb{Q})+E(K)_{\rm tor})$ is thus a finitely generated infinite abelian group, so has subgroups of all index. In particular, it has a subgroup W' such that the quotient by W' is cyclic of order $t/\#E(K)_{\rm tor}$. Let $\tilde{W}$ be the inverse image of W' in $E(K)$, so $E(K)_{\rm tor}, E^D(\mathbb{Q})\subset\tilde{W}$, and $[E(K):\tilde{W}]=t/\#E(K)_{\rm tor}$. Since $\tilde{W}$ is finitely generated, there exists a torsion free subgroup $W\subset\tilde{W}$ such that $W\oplus E(K)_{\rm tor}=\tilde{W}$. Then

$$[E(K):W]=\#E(K)_{\rm tor}\cdot[E(K):\tilde{W}]=\#E(K)_{\rm tor}\cdot\frac{t}{\#E(K)_{\rm tor}}=t.$$

□

Elsewehere in this paper, for technical reasons in order to apply Kolyvagin's theorems, we made a minimality hypothesis on $r_{\rm an}(E^D/\mathbb{Q})$, and based on extensive numerical data, we conjecture that this is the right hypothesis to guarantee the existence of Gross-Zagier subgroups $W\subset E(K)$.

Conjecture 8.5. *If $r_{\rm an}(E/\mathbb{Q})>r_{\rm an}(E^D/\mathbb{Q})\le 1$, then $\#E(K)_{\rm tor}\mid t$. In particular, there exists a Gross-Zagier subgroup $W\subset E(K)$.*

We obtain evidence for Conjecture 8.5 using Sage[†] [S$^+$09, Creb, PAR], Cremona's tables [Crea], Proposition 8.4, and assuming the Birch and Swinnerton-Dyer conjecture. More precisely, we check that Conjecture 8.5 is "probably true" for every elliptic curve of rank ≥ 2 and conductor $\le 130,000$ and the first three D that satisfy the Heegner hypothesis, except possibly for the triples $(E, D, \#E(K)_{\rm tor})$ in Table 1 where the computation of the conjectural order of $\#\text{Ш}(E/K)$ took too long.

Table 1: All triples up to conductor 130,000 where we did not yet verify Conjecture 8.5

$(8320e1,-191,2),(9842d1,-223,3),(9842d1,-255,3),(9842d1,-447,3),(74655j1,-251,3),$
$(87680a1,-119,2),(87680a1,-151,2),(87680b1,-119,2),(87680b1,-151,2),(89465a1,-51,2),$
$(89465a1,-59,2),(89465a1,-71,2),(95545b1,-191,2),(95545b1,-219,2),(104585b1,-139,2),$
$(104585b1,-179,2),(104585b1,-191,2),(114260a1,-231,2),(114260a1,-239,2),(114260a1,-431,2),$
$(122486a1,-103,3),(122486a1,-55,3),(122486a1,-87,3),(126672r1,-335,2),(126672r1,-647,2),$
$(126672r1,-719,2),(129940a1,-111,2),(129940a1,-71,2),(129940a1,-79,2)$

In our computations, we considered the first three Heegner D, *without* making the condition $r_{\rm an}(E^D/\mathbb{Q})\le 1$. The conjecture is *false* without the hypothesis that $r_{\rm an}(E^D/\mathbb{Q})\le 1$, as Example 8.3 above shows. Moreover, we found two further similar examples in which, however, E has rank 2 and E^D has rank 3. First, for the curve E with Cremona label 20672m1, equation $y^2=x^3-431x-3444$ and $D=-127$, we have $\operatorname{rank}(E(\mathbb{Q}))=2$, $\operatorname{rank}(E^D(\mathbb{Q}))=3$, and $\#E(K)_{\rm tor}=2$, but $t=1$. A second example is E given by 18560c1 and $D=-151$, in which again $\operatorname{rank}(E(\mathbb{Q}))=2$, $\operatorname{rank}(E^D(\mathbb{Q}))=3$, $\#E(K)_{\rm tor}=2$, but $t=1$.

This was a large computation that relies on a range of nontrivial computer code, which we carried out as follows. First we computed $\#E(K)_{\rm tor}$ for each of the 78,420 elliptic curve of conductor $\le$130,000 with rank ≥ 2 and the first three Heegner D. We then determined whether $\#E(K)_{\rm tor}$ divides $c\cdot\prod c_q$. Since we are verifying that something divides $c\cdot\prod c_q$, there is no loss at all in assuming Manin's conjecture that $c=1$ for the optimal quotient of $X_0(N)$. We then computed the Manin constant c for non-optimal curves by finding a shortest isogeny path from the optimal curve in the isogeny graph of E (there is unfortunately a small possibility of error in computation of the isogeny graph, due to numerical precision used in the implementation). We found only 37 remaining curves E of rank ≥ 2 such that $\#E(K)_{\rm tor}\nmid c\cdot\prod c_q$, and $37\cdot 3=111$ corresponding pairs (E,D). It

[†] Running on hardware purchased using National Science Foundation Grant No. DMS-0821725.

turns out that all of these curves are optimal hence have $c = 1$. For each of these pairs (E, D) we attempted to compute $\#\text{Ш}(E/K)_{\text{an}}$ using Conjecture 2.2 and some results of [GJP$^+$09], and the computation finished in all but 29 cases. The main difficulty was computing $\text{Reg}(E/K)$ in terms of $\text{Reg}(E/\mathbb{Q})$ and $\text{Reg}(E^D/\mathbb{Q})$ by saturating the sum of $E(\mathbb{Q})$ and $E^D(\mathbb{Q})$ in $E(K)$. Computing $E^D(\mathbb{Q})$ was sometimes very difficult, since E^D has huge conductor and rank 1, and this sometimes took as long as a day when it completed. For more details, the reader is urged to read the source code of the Sage command `heegner_sha_an` in Sage-3.4.1 and later.

References

[ARS06] A. Agashe, K. A. Ribet, and W. A. Stein, *The Manin Constant*, JPAM Coates Volume (2006), `http://wstein.org/papers/ars-manin/`.

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

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

[Bir65] B. J. Birch, *Conjectures concerning elliptic curves*, Proceedings of Symposia in Pure Mathematics, VIII, Amer. Math. Soc., Providence, R.I., 1965, pp. 106–112. MR 30 #4759

[Crea] J. E. Cremona, *Elliptic Curves Data*, `http://www.warwick.ac.uk/~masgaj/ftp/data/`.

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

[GJP$^+$09] G. Grigorov, A. Jorza, S. Patrikis, C. Patrascu, and W. Stein, *Verification of the Birch and Swinnerton-Dyer Conjecture for Specific Elliptic Curves*, To appear in Mathematics of Computation (2009).

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

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

[JLS08] D. Jetchev, K. Lauter, and W. Stein, *Explicit heegner points: Kolyvagin's conjecture and nontrivial elements in the Shafarevich-Tate group.*

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

[Kol91a] V. A. Kolyvagin, *On the structure of Selmer groups*, Math. Ann. **291** (1991), no. 2, 253–259. MR 93e:11073

[Kol91b] ———, *On the structure of Shafarevich-Tate groups*, Algebraic geometry (Chicago, IL, 1989), Springer, Berlin, 1991, pp. 94–121.

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

[PAR] PARI, *A computer algebra system designed for fast computations in number theory*, `http://pari.math.u-bordeaux.fr/`.

[S$^+$09] W. A. Stein et al., *Sage Mathematics Software (Version 3.3)*, The Sage Development Team, 2009, `http://www.sagemath.org`.

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

[Ste02] W. A. Stein, *There are genus one curves over* **Q** *of every odd index*, J. Reine Angew. Math. **547** (2002), 139–147. MR 2003c:11059

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