Explicit Heegner points: Kolyvagin's conjecture and non-trivial elements in the Shafarevich-Tate group

Dimitar Jetchev, Kristin Lauter and William Stein

ABSTRACT

Kolyvagin used Heegner points to associate a system of cohomology classes to an elliptic curve over $\mathbb{Q}$ and conjectured that the system contains a nontrivial class. His conjecture has profound implications on the structure of Selmer groups. We provide new computational and theoretical evidence for Kolyvagin's conjecture. More precisely, we apply results of Zhang and others to deduce that Kolyvagin classes are computable, then explicitly study Heegner points over ring class fields and Kolyvagin's conjecture for specific elliptic curves of rank two. We explain how Kolyvagin's conjecture implies that if the analytic rank of an elliptic curve is at least two then the $\mathbb{Z}_p$-corank of the corresponding Selmer group is at least two as well. We also use explicitly computed Heegner points to produce non-trivial classes in the Shafarevich-Tate group.

1. Introduction

Let $E_{/F}$ be an elliptic curve over a number field F. The analytic rank $r_{\mathrm{an}}(E/F)$ of E is the order of vanishing of the L-function $L(E_{/F}, s)$ at $s = 1$. The Mordell-Weil rank $r_{\mathrm{MW}}(E/F)$ is the rank of the Mordell-Weil group $E(F)$. The conjecture of Birch and Swinnerton-Dyer asserts that $r_{\mathrm{an}}(E/F) = r_{\mathrm{MW}}(E/F)$.

Kolyvagin constructed explicit cohomology classes from Heegner points over certain abelian extensions of quadratic imaginary fields and used these classes to bound the size of the Selmer groups for elliptic curves over $\mathbb{Q}$ of analytic rank at most one (see [Kol90], [Kol91b] and [Gro91]). His results, together with the Gross-Zagier formula (see [GZ86]), imply the following theorem:

THEOREM 1.1 (Gross-Zagier, Kolyvagin). *Let $E_{/\mathbb{Q}}$ be an elliptic curve which satisfies $r_{\mathrm{an}}(E/\mathbb{Q}) \leqslant 1$. Then the Shafarevich-Tate group $\text{Ш}(E/\mathbb{Q})$ is finite and $r_{\mathrm{an}}(E/\mathbb{Q}) = r_{\mathrm{MW}}(E/\mathbb{Q})$.*

Unfortunately, very little is known about the Birch and Swinnerton-Dyer conjecture for elliptic curves $E_{/\mathbb{Q}}$ with $r_{\mathrm{an}}(E/\mathbb{Q}) \geqslant 2$. Still, it implies the following conjecture:

Conjecture 1. If $r_{\mathrm{an}}(E/\mathbb{Q}) \geqslant 2$ then $r_{\mathrm{MW}}(E/\mathbb{Q}) \geqslant 2$.

As far as we know, nothing has been proved towards the above assertion. A weaker conjecture can be formulated in the language of Selmer coranks. The Selmer corank $r_p(E/F)$ of $E_{/F}$ is the $\mathbb{Z}_p$-corank of the Selmer group $\mathrm{Sel}_{p^\infty}(E/F)$. Using Kummer theory, one shows that $r_p(E/\mathbb{Q}) \geqslant r_{\mathrm{MW}}(E/\mathbb{Q})$ with an equality occuring if and only if the p-primary part of the Shafarevich-Tate group $\text{Ш}(E/\mathbb{Q})$ is finite. Thus, one obtains the following weaker conjecture:

Conjecture 2. If $r_{\mathrm{an}}(E/\mathbb{Q}) \geqslant 2$ then $r_p(E/\mathbb{Q}) \geqslant 2$.

For elliptic curves E of arbitrary analytic rank, Kolyvagin was able to explain the exact structure of the Selmer group $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ in terms of Heegner points and the associated cohomology classes under a conjecture about the non-triviality of these classes (see [Kol91a, Conj.A]). Unfortunately, Kolyvagin's conjecture appears to be extremely difficult to prove. Until the present paper, there has been no example of an elliptic curve over $\mathbb{Q}$ of rank at least two for which the conjecture has been verified.

In this paper, we present a complete algorithm to compute Kolyvagin's cohomology classes by explicitly computing the corresponding Heegner points over ring class fields. We use this algorithm to verify Kolyvagin's conjecture for the first time for elliptic curves of analytic rank two. We also explain (see Corollary 3.3) how Kolyvagin's conjecture implies Conjecture 2. In addition, we use methods of Cornut (see [Cor02]) to provide theoretical evidence for Kolyvagin's conjecture. As a separate application of the explicit computation of Heegner points, we construct nontrivial cohomology classes in the Shafarevich-Tate group $\Sha(E/K)$ of elliptic curves E over certain quadratic imaginary fields. One of the main contributions of this paper is that by establishing certain height bounds, we prove that there exists an algorithm which *provably* computes the correct Heegner points over ring class fields.

The paper is organized as follows. Section 2 introduces Heegner points over ring class fields and Kolyvagin cohomology classes. We explain the methods of computation and illustrate them with several examples. In Section 3 we state Kolyvagin's conjecture, discuss Kolyvagin's work on Selmer groups and establish Conjecture 2 as a corollary. Moreover, we present a proof of the theoretical evidence following closely Cornut's arguments. Section 3.6 contains the essential examples for which we manage to explicitly verify the conjecture. Finally, in Section 4 we apply our computational techniques to produce explicit non-trivial elements in the Shafarevich-Tate groups for specific elliptic curves. Finally, the appendix establishes certain bounds on the logarithmic heights of the Heegner points over ring class fields.

2. Heegner points over ring class fields

We discuss Heegner points over ring class fields in Section 2.1 and describe a method for computing them in Section 2.2. Height estimates for these points are given in the appendix. We illustrate the method with some examples in Section 2.3. The standard references are [Gro91], [Kol90] and [McC91].

2.1 Heegner points over ring class fields

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and let $K = \mathbb{Q}(\sqrt{-D})$ for some fundamental discriminant $D > 0$, $D \neq 3, 4$, such that all prime factors of N are split in K. We refer to such a discriminant as a *Heegner discriminant* for $E/\mathbb{Q}$. Let $\mathcal{O}_K$ be the ring of integers of K. It follows that $N\mathcal{O}_K = \mathcal{N}\bar{\mathcal{N}}$ for an ideal $\mathcal{N}$ of $\mathcal{O}_K$ with $\mathcal{O}_K/\mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}$.

By the modularity theorem (see [BCDT01]), there exists an optimal (having minimal degree) modular parameterization $\varphi : X_0(N) \to E$. Let $\mathcal{N}^{-1}$ be the fractional ideal of $\mathcal{O}_K$ for which $\mathcal{N}\mathcal{N}^{-1} = \mathcal{O}_K$. We view $\mathcal{O}_K$ and $\mathcal{N}$ as $\mathbb{Z}$-lattices of rank two in $\mathbb{C}$ and observe that $\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}^{-1}$ is a cyclic isogeny of degree N between the elliptic curves $\mathbb{C}/\mathcal{O}_K$ and $\mathbb{C}/\mathcal{N}^{-1}$. This isogeny corresponds to a complex point $x_1 \in X_0(N)(\mathbb{C})$. According to the theory of complex multiplication [Sil94, Ch.II], the point x_1 is defined over the Hilbert class field H_K of K.

More generally, for an integer c, let $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$ be the order of conductor c in $\mathcal{O}_K$ and let $\mathcal{N}_c = \mathcal{N} \cap \mathcal{O}_c$, which is an invertible ideal of $\mathcal{O}_c$. Then $\mathcal{O}_c/\mathcal{N}_c \simeq \mathbb{Z}/N\mathbb{Z}$ and the map $\mathbb{C}/\mathcal{O}_c \to \mathbb{C}/\mathcal{N}_c^{-1}$

is a cyclic isogeny of degree N. Thus, it defines a point $x_c \in X_0(N)(\mathbb{C})$. By the theory of complex multiplication, this point is defined over the ring class field $K[c]$ of conductor c over K (that is, the unique abelian extension of K corresponding to the norm subgroup $\widehat{\mathcal{O}_c}^\times K^\times \subset \widehat{K}^\times$; e.g., if $c = 1$ then $K[1] = H_K$).

We use the parameterization $\varphi : X_0(N) \to E$ to obtain points

$$y_c = \varphi(x_c) \in E(K[c]).$$

Let $y_K = \mathrm{Tr}_{H_K/K}(y_1)$. We refer to y_K as the *Heegner point* for the discriminant D, even though it is only well defined up to sign and torsion (if $\mathcal{N}'$ is another ideal with $\mathcal{O}/\mathcal{N}' \simeq \mathbb{Z}/N\mathbb{Z}$ then the new Heegner point differs from y_K by at most a sign change and a rational torsion point).

2.2 Explicit computation of the points y_c

Significant work has been done on explicit calculations of Heegner points on elliptic curves (see [Coh07], [Del02], [Elk94], [Wat04]). Yet, all of these only compute the points y_1 and y_K. In [EJL06] explicit computations of the points y_c were considered in several examples and some difficulties were outlined. However, there has been no algorithm which provably computes the points y_c. One of the main contributions of this paper is the description of such an algorithm.

To compute the point $y_c = [\mathbb{C}/\mathcal{O}_c \to \mathbb{C}/\mathcal{N}_c^{-1}] \in E(K[c])$ we let $f \in S_2(\Gamma_0(N))$ be the newform corresponding to the elliptic curve E and Λ be the complex lattice (defined up to homothety), such that $E \cong \mathbb{C}/\Lambda$. Let $\mathfrak{h}^\times = \mathfrak{h} \cup \mathbb{P}^1(\mathbb{Q}) \cup \{i\infty\}$, where $\mathfrak{h} = \{z \in \mathbb{C} : \Im(z) > 0\}$ is the upper-half plane equipped with the action of $\Gamma_0(N)$ by linear fractional transformations. The modular parametrization $\varphi : X_0(N) \to E$ is then given by the function $\varphi : \mathfrak{h}^\times \to \mathbb{C}/\Lambda$

$$\varphi(\tau) = \int_\tau^{i\infty} f(z)dz = \sum_{n \geqslant 1} \frac{a_n}{n} e^{2\pi i n \tau}, \tag{1}$$

where $f = \sum_{n=1}^\infty a_n q^n$ is the Fourier expansion of the modular form f.

We first compute ideal class representatives $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_{h_c}$ for the Picard group $\mathrm{Pic}(\mathcal{O}_c) \cong \mathrm{Gal}(K[c]/K)$, where $h_c = \#\mathrm{Pic}(\mathcal{O}_c)$. Let $\sigma_i \in \mathrm{Gal}(K[c]/K)$ be the image of the ideal class of $\mathfrak{a}_i$ under the Artin map. We use the ideal $\mathfrak{a}_i$ to compute a complex number (a *quadratic surd*)$\tau_i \in \mathfrak{h}$ representing the CM point $\sigma_i(x_c)$ for each $i = 1, \ldots, h_c$ (since $X_0(N) = \Gamma_0(N) \backslash \mathfrak{h}^\times$). Explicitly, the Galois conjugates of x_c are

$$\sigma_i(x_c) = [\mathbb{C}/\mathfrak{a}_i^{-1} \to \mathbb{C}/\mathfrak{a}_i^{-1}\mathcal{N}_c^{-1}], \ i = 1, \ldots, h_c.$$

Next, we use (1) to approximate $\varphi(\sigma_i(x_c))$ as an element of $\mathbb{C}/\Lambda$ by truncating the infinite series up to sufficiently many terms whose number is determined precisely by the results of the appendix. Finally, the image of $\varphi(\tau_i) + \Lambda$ under the Weierstrass $\wp$-function gives us an approximation of the x-coordinate of the point y_c on the Weierstrass model of the elliptic curve E. On the other hand, this coordinate is $K[c]$-rational. Thus, if we compute the map (1) with sufficiently many terms and up to high enough floating point accuracy, we must be able to recognize the correct x-coordinate of y_c on the Weierstrass model as an element of $K[c]$.

To implement the last step, we use the upper bound established in the appendix on the logarithmic height of the Heegner point y_c. The bound on the logarithmic height comes from a bound on the canonical height combined with bounds on the height difference (see the appendix for complete details). Once we have a height bound, we estimate the floating point accuracy required for the computation. Finally, we estimate the number of terms of (1) necessary to compute the point y_c up to the corresponding accuracy (see [Coh07, p.591] for more details).

Remark 1. In practice, there are two ways to implement the above algorithm. The first approach is to compute an approximation x_i of the x-coordinates of $y_c^{\sigma_i}$ for every $i = 1, \ldots, c$ and form the polynomial $F(z) = \prod_{i=1}^{h_c}(z - x_i)$. The coefficients of this polynomial are very close to the rational coefficients of the minimal polynomial of the actual x-coordinate of y_c. Thus, one can try to recognize the coefficients of $F(z)$ by using the continued fractions method. The second approach is to search for the τ_i with the largest imaginary part (which will make the convergence of the corresponding series (1) defining the modular parametrization fast) and then try to search for an algebraic dependence of degree $[K[c] : K]$ using standard algorithms implemented in PARI/GP. Indeed, computing a conjugate with a smaller imaginary part might be significantly harder since the infinite series in (1) will converge slower and one will need more terms to compute the image up to the required accuracy.

Remark 2. We did *not* actually implement an algorithm for computing bounds on heights of Heegner points as described in the appendix of this paper. Thus, the computations in the specific examples below are not provably correct, though we did many consistency checks and we are convinced that our computational observations are correct. The primary goal of the examples and practical implementation of our algorithm is to provide tools and data for improving our theoretical understanding of Kolyvagin's conjecture, and not making the computations below provably correct does not detract from either of these goals.

2.3 Examples
We compute the Heegner points y_c for specific elliptic curves and choices of quadratic imaginary fields.

53a1: Let $E_{/\mathbb{Q}}$ be the elliptic curve with label **53a1** in Cremona's database (see [Cre]). Explicitly, E is the curve $y^2 + xy + y = x^3 - x^2$. Let $D = 43$ and $c = 5$. The conductor of E is 53 which is split in $K = \mathbb{Q}(\sqrt{-D})$, so D is a Heegner discriminant for E. The modular form associated to E is $f_E(q) = q - q^2 - 3q^3 - q^4 + 3q^6 - 4q^7 + 3q^8 + 6q^9 + \cdots$. One applies the methods from Section 2.2 to compute the minimal polynomial of the x-coordinate of y_5 for the above model

$$F(x) = x^6 - 12x^5 + 1980x^4 - 5855x^3 + 6930x^2 - 3852x + 864.$$

Since $F(x)$ is an irreducible polynomial over K, it generates the ring class field $K[5]/K$, i.e., $K[5] = K[\alpha] \cong K[x]/\langle F(x)\rangle$, where α is one of the roots. To find the y-coordinate of y_5 we substitute α into the equation of E and factor the resulting quadratic polynomial over $K[5]$ to obtain that the point y_5 is equal to

$$\left(\alpha, -4/315\alpha^5 + 43/315\alpha^4 - 7897/315\alpha^3 + 2167/35\alpha^2 - 372/7\alpha + 544/35\right) \in E(K[5]).$$

389a1: The elliptic curve with label **389a1** is $y^2 + y = x^3 + x^2 - 2x$ and the associated modular form is $f_E(q) = q - 2q^2 - 2q^3 + 2q^4 - 3q^5 + 4q^6 - 5q^7 + q^9 + 6q^{10} + \cdots$. Let $D = 7$ (which is a Heegner discriminant for E) and $c = 5$. As above, we compute the minimal polynomial of the x-coordinate of y_5:

$$F(x) = x^6 + \frac{10}{7}x^5 - \frac{867}{49}x^4 - \frac{76}{245}x^3 + \frac{3148}{35}x^2 - \frac{25944}{245}x + \frac{48771}{1225}.$$

If α is a root of $F(x)$ then $y_5 = (\alpha, \beta)$ where

$$\begin{aligned}
\beta = {} & \frac{280}{7761}\sqrt{-7}\alpha^5 + \frac{1030}{7761}\sqrt{-7}\alpha^4 - \frac{12305}{36218}\sqrt{-7}\alpha^3 - \frac{10099}{15522}\sqrt{-7}\alpha^2 \\
& + \frac{70565}{54327}\sqrt{-7}\alpha + \frac{-18109 - 33814\sqrt{-7}}{36218}.
\end{aligned}$$

709a1: The elliptic curve **709a1** with equation $y^2 + y = x^3 - x^2 - 2x$ has an associated modular

form $f_E(q) = q - 2q^2 - q^3 + 2q^4 - 3q^5 + 2q^6 - 4q^7 - 2q^9 + \cdots$. Let $D = 7$ (a Heegner discriminant for E) and $c = 5$. The minimal polynomial of the x-coordinate of y_5 is

$$F(x) = \frac{1}{5^2 \cdot 7^2 \cdot 19^2} \left(442225x^6 - 161350x^5 - 2082625x^4 - 387380x^3 + 2627410x^2 + 18136030x + 339921\right),$$

and if α is a root of x then $y_5 = (\alpha, \beta)$ for

$$\beta = \frac{341145}{62822}\sqrt{-7}\alpha^5 - \frac{138045}{31411}\sqrt{-7}\alpha^4 - \frac{31161685}{1319262}\sqrt{-7}\alpha^3 + \frac{7109897}{1319262}\sqrt{-7}\alpha^2 +$$

$$+ \frac{39756589}{1319262}\sqrt{-7}\alpha + \frac{-219877 + 4423733\sqrt{-7}}{439754}.$$

718b1: The curve **718b1** has equation $y^2 + xy + y = x^3 - 5x$ with associated modular form $f_E(q) = q - q^2 - 2q^3 + q^4 - 3q^5 + 2q^6 - 5q^7 - q^8 + q^9 + 3q^{10} + \dots$. Again, for $D = 7$ and $c = 5$ we find $F(x) = \frac{1}{3^4 \cdot 5^2} \left(2025x^6 + 12400x^5 + 32200x^4 + 78960x^3 + 289120x^2 + 622560x + 472896\right)$ and $y_5 = (\alpha, \beta)$ with

$$\beta = \frac{16335}{12271}\sqrt{-7}\alpha^5 + \frac{206525}{36813}\sqrt{-7}\alpha^4 + \frac{54995}{5259}\sqrt{-7}\alpha^3 + \frac{390532}{12271}\sqrt{-7}\alpha^2 +$$

$$+ \frac{-36813 + 9538687\sqrt{-7}}{73626}\alpha + \frac{-12271 + 4018835\sqrt{-7}}{24542}.$$

3. Kolyvagin's conjecture: consequences and evidence

We recall Kolyvagin's construction of the cohomology classes in Section 3.2 and state Kolyvagin's conjecture in Section 3.3. Section 3.4 is devoted to the proof of the promised consequence regarding the $\mathbb{Z}_p$-corank of the Selmer group of an elliptic curve with large analytic rank. In Section 3.5 we provide Cornut's arguments for the theoretical evidence for Kolyvagin's conjecture and finally, in Section 3.6 we verify Kolyvagin's conjecture for particular elliptic curves. Throughout the entire section we assume that $E_{/\mathbb{Q}}$ is an elliptic curve of conductor N, D is a Heegner discriminant for E and $p \nmid ND$ is a prime such that the mod p Galois representation $\overline{\rho}_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p])$ is surjective.

3.1 Preliminaries

Most of this section follows the exposition in [Gro91], [McC91] and [Kol91c].

1. Kolyvagin primes. We refer to a prime number ℓ as a *Kolyvagin prime* if ℓ is inert in K and p divides both a_ℓ and $\ell + 1$). For a Kolyvagin prime ℓ let

$$M(\ell) = \mathrm{ord}_p(\gcd(a_\ell, \ell + 1)).$$

We denote by Λ^r the set of all square-free products of exactly r Kolyvagin primes and let $\Lambda = \bigcup_r \Lambda^r$. For any $c \in \Lambda$, let $M(c) = \min_{\ell | c} M(\ell)$. Finally, let

$$\Lambda_m^r = \{c \in \Lambda^r : M(c) \geqslant m\}$$

and let $\Lambda_m = \bigcup_r \Lambda_m^r$.

2. Kolyvagin derivative operators. Let $\mathcal{G}_c = \mathrm{Gal}(K[c]/K)$ and $G_c = \mathrm{Gal}(K[c]/K[1])$. For each $\ell \in \Lambda^1$, the group G_ℓ is cyclic of order $\ell + 1$. Indeed,

$$G_\ell \simeq (\mathcal{O}_K/\ell\mathcal{O}_K)^\times / (\mathbb{Z}/\ell\mathbb{Z})^\times \simeq \mathbb{F}_\lambda^\times / \mathbb{F}_\ell^\times.$$

Moreover, $G_c \cong \prod_{\ell|c} G_\ell$ (since $\mathrm{Gal}(K[c]/K[c/\ell]) \cong G_\ell$). Next, fix a generator σ_ℓ of G_ℓ for each $\ell \in \Lambda^1$.

Define $D_\ell = \sum_{i=1}^{\ell} i\sigma_\ell^i \in \mathbb{Z}[G_\ell]$ and let

$$D_c = \prod_{\ell|c} D_\ell \in \mathbb{Z}[G_c].$$

Note that $(\sigma_\ell - 1)D_\ell = 1 + \ell - \mathrm{Tr}_{K[\ell]/K[1]}$.

We refer to D_c as the *Kolyvagin derivative operators*. Finally, let S be a set of coset representatives for the subgroup $G_c \subseteq \mathcal{G}_c$. Define

$$P_c = \sum_{s \in S} sD_c y_c \in E(K[c]).$$

The points P_c are derived from the points y_c, so we will refer to them as *derived Heegner points*.

3. The function $m : \Lambda \to \mathbb{Z}$ and the sequence $\{m_r\}_{r \geqslant 0}$. For any $c \in \Lambda$ let $m'(c)$ be the largest positive integer such that $P_c \in p^{m'(c)}E(K[c])$ (if P_c is torsion then $m'(c) = \infty$). Define a function $m : \Lambda \to \mathbb{Z}$ by

$$m(c) = \begin{cases} m'(c) & \text{if } m'(c) \leqslant M(c), \\ \infty & \text{otherwise.} \end{cases}$$

Finally, let $m_r = \min_{c \in \Lambda^r} m(c)$.

PROPOSITION 3.1. *The sequence $\{m_r\}_{r \geqslant 0}$ is non-increasing, i.e., $m_r \geqslant m_{r+1}$ for every $r \geqslant 0$.*

Proof. This is proved in [Kol91c, Thm.C]. $\qquad\qquad\square$

3.2 Kolyvagin cohomology classes

Kolyvagin uses the points P_c to construct classes $\kappa_{c,m} \in \mathrm{H}^1(K, E[p^m])$ for any $c \in \Lambda_m$. For the details of the construction, we refer to [Gro91, pp.241-242]) and [McC91, §4]. The class $\kappa_{c,m}$ is explicit, in the sense that it is represented by the 1-cocycle

$$\sigma \mapsto \sigma\left(\frac{P_c}{p^m}\right) - \frac{P_c}{p^m} - \frac{(\sigma - 1)P_c}{p^m}, \tag{2}$$

where $\dfrac{(\sigma - 1)P_c}{p^m}$ is the unique p^m-division point of $(\sigma - 1)P_c$ in $E(K[c])$ (see [McC91, Lem. 4.1]). The class $\kappa_{c,m}$ is non-trivial if and only if $P_c \notin p^m E(K[c])$ (which is equivalent to $m > m(c)$).

Finally, let $-\varepsilon$ be the sign of the functional equation corresponding to E. For each $c \in \Lambda_m$, let $\varepsilon(c) = \varepsilon \cdot (-1)^{f_c}$ where $f_c = \#\{\ell : \ell \mid c\}$ (e.g., $f_1 = 0$). It follows from [Gro91, Prop.5.4(ii)] that $\kappa_{c,m}$ lies in the $\varepsilon(c)$-eigenspace for the action of complex conjugation on $\mathrm{H}^1(K, E[p^m])$.

3.3 Statement of the conjecture

We are interested in $m_\infty = \min_{c \in \Lambda} m(c) = \lim_{r \to \infty} m_r$. In the case when the Heegner point $P_1 = y_K$ has infinite order in $E(K)$, the Gross-Zagier formula (see [GZ86]) implies that $r_{\mathrm{an}}(E/K) = 1$, so (by the results of Kolyvagin) $r_{\mathrm{MW}}(E/K) = 1$. This means that $m_0 = \mathrm{ord}_p([E(K) : \mathbb{Z}y_K]) < \infty$. In particular, $m_\infty < \infty$ which is equivalent to the system of cohomology classes

$$T = \{\kappa_{c,m} : m \leqslant M(c)\}$$

containing at least one non-zero class. A much more interesting and subtle is the case of an elliptic curves E over K of analytic rank at least two. In this case, Kolyvagin conjectured (see [Kol91a, Conj.C]) that T contains a non-trivial class as well.

Conjecture 3 (Kolyvagin's conjecture). We have $m_\infty < \infty$, i.e., T contains at least one class $\kappa_{c,m} \neq 0$.

Remark 3. Although Kolyvagin's conjecture is obvious in the case of elliptic curves of analytic rank one over K, the number m_∞ is still interesting. Indeed, the p-part of the Birch and Swinnerton-Dyer conjectural formula for $E_{/K}$ is equivalent to $m_\infty = \mathrm{ord}_p \left(\prod_{q|N} c_q \right)$, where c_q is the Tamagawa number of $E_{/\mathbb{Q}}$ at q. See [Jet07] for some new results related to this question which imply (in many cases) the exact upper bound on the order of the p-primary part of the Shafarevich-Tate group as predicted by the conjectural formula.

3.4 A consequence on the structure of Selmer groups

Let $r_p^\pm(E/K) = \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/K)^\pm$. Kolyvagin (see [Kol91a]) proved the following:

THEOREM 3.2 (Kolyvagin). *Assume Conjecture 3 and let f be the smallest nonnegative integer for which $m_f < \infty$. Then*

$$\mathrm{Sel}_{p^\infty}(E/K)^{\varepsilon(-1)^{f+1}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{f+1} \oplus (\text{a finite group})$$

and

$$\mathrm{Sel}_{p^\infty}(E/K)^{\varepsilon(-1)^f} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r \oplus (\text{a finite group})$$

where $r \leqslant f$ and $f - r$ is even. In other words, $r_p^{\varepsilon(-1)^f}(E/K) = r$ and $r_p^{\varepsilon(-1)^{f+1}}(E/K) = f + 1$.

The above structure theorem of Kolyvagin has the following consequence which strongly supports Conjecture 2.

COROLLARY 3.3. *Assume Conjecture 3. Then (i) If $r_{\mathrm{an}}(E/\mathbb{Q})$ is even and nonzero then*

$$r_p(E/\mathbb{Q}) \geqslant 2.$$

(ii) If $r_{\mathrm{an}}(E/\mathbb{Q})$ is odd and strictly larger than one then

$$r_p(E/\mathbb{Q}) \geqslant 3.$$

Proof. (i) By [BFH90] or [MM97], one can choose a quadratic imaginary field $K = \mathbb{Q}(\sqrt{-D})$ with Heegner discriminant D, such that $L'(E_{/\mathbb{Q}}^D, 1) \neq 0$, where E^D is the twist of E by the quadratic character associated to K (note that D is a Heegner discriminant, so the sign of the functional equation of E^D is always odd since E has even sign). Hence, by Theorem 1.1, the Selmer group $\mathrm{Sel}_{p^\infty}(E^D/\mathbb{Q})$ has $\mathbb{Z}_p$-corank one, i.e., $r_p^-(E/K) = r_p(E^D/\mathbb{Q}) = 1$. We want to prove $r_p^+(E/K) = r_p(E/\mathbb{Q}) \geqslant 2$. Assume the contrary, i.e., $r_p^+(E/K) = r_p(E/\mathbb{Q}) \leqslant 1$. This means (by Theorem 3.2) that $r = f = 0$ (here, r and f are as in Theorem 3.2). Therefore, $m_0 < \infty$ which means that the Heegner point y_K has infinite order in $E(K)$ and hence (by the Gross-Zagier formula), $L'(E_{/K}, 1) \neq 0$. But this is a contradiction since

$$L'(E_{/K}, s) = L'(E_{/\mathbb{Q}}, s)L(E_{/\mathbb{Q}}^D, s) + L(E_{/\mathbb{Q}}, s)L'(E_{/\mathbb{Q}}^D, s),$$

which vanishes at $s = 1$ since $L(E_{/\mathbb{Q}}, 1) = L'(E_{/\mathbb{Q}}, 1) = 0$. Thus, $r_p(E/\mathbb{Q}) = r_p^+(E/K) \geqslant 2$.

(ii) It follows from the work of Waldspurger (see also [BFH90, pp.543-44]) that one can choose a quadratic imaginary field $K = \mathbb{Q}(\sqrt{-D})$ with a Heegner discriminant D, such that $L(E_{/\mathbb{Q}}^D, 1) \neq 0$ (this uses the fact that $r_{\mathrm{an}}(E/\mathbb{Q})$ is odd). Therefore, by Theorem 1.1, $r_p(E^D/\mathbb{Q}) = 0$, i.e., $r_p^-(E/K) = 0$. By Theorem 3.2, $r = 0$ and f is even. If $f \geqslant 2$ we are done since $r_p(E/\mathbb{Q}) = r_p^+(E/K) = f + 1 \geqslant 3$. If $f = 0$, we use the same argument as in (i) to arrive at a contradiction. Therefore, $r_p(E/\mathbb{Q}) = r_p^+(E/K) \geqslant 3$. $\square$

Remark 4. The parity conjecture proved by Nekovář (see [Nek01]) implies that

$$r_p(E/\mathbb{Q}) \equiv r_{\mathrm{an}}(E/\mathbb{Q}) \mod 2.$$

Yet, Nekovář's result does not imply in any obvious way the statements of the above proposition.

3.5 Cornut's theoretical evidence for Kolyvagin's conjecture

The following evidence for Conjecture 3 was proven by Cornut.

PROPOSITION 3.4. *For all but finitely many $c \in \Lambda$ there exists a set R of liftings for the elements of $\mathrm{Gal}(K[1]/K)$ into $\mathrm{Gal}(K^{\mathrm{ab}}/K)$, such that if $P_c = D_0 D_c y_c$ is the derived Heegner point defined in terms of this choice of liftings (i.e, if $D_0 = \sum_{\sigma \in R} \sigma$), then P_c is non-torsion.*

Remark 5. For a non-torsion point P_c, let $m'(c)$ be the function defined in Section 3.1. Proposition 3.4 provides little evidence towards Kolyvagin's conjecture. The reason is that even if one gets non-torsion points P_c, it might still happen that for each such c we have $m'(c) > M(c)$ (i.e., $m(c) = \infty$) in which case all classes $\kappa_{c,m}$ with $m \leqslant M(c)$ will be trivial.

Let $K[\infty] = \bigcup_{c \in \Lambda} K[c]$. The proof of the proposition depends on the following two lemmas:

LEMMA 3.5. *The group $E(K[\infty])_{\mathrm{tors}}$ is finite.*

Proof. Let q be any prime which is a prime of good reduction for E, which is inert in K and which is different from the primes in Λ^1 (there are infinitely many such primes according to Čebotarev density theorem). Let $\mathfrak{q}$ be the unique prime of K over q. It follows from class field theory that the prime $\mathfrak{q}$ splits completely in $K[\infty]$ since it splits completely in each of the finite extensions $K[c]$. Thus, the completion of $K[\infty]$ at any prime which lies over $\mathfrak{q}$ is isomorphic to $K_{\mathfrak{q}}$ and therefore, $E(K[\infty])_{\mathrm{tors}} \hookrightarrow E(K_{\mathfrak{q}})_{\mathrm{tors}}$. The last group is finite since it is isomorphic to an extension of $\mathbb{Z}_q^2$ by a finite group (see [Mil86, Lem.I.3.3] or [Tat67, p.168-169]). Therefore, $E(K[\infty]_{\mathrm{tors}})$ is finite. $\square$

Let $|E(K[\infty])_{\mathrm{tors}}| = M < \infty$ and let $d(c) = [K[c] : K[1]] = \prod_{\ell \mid c}(\ell + 1)$ for any $c \in \Lambda$. Let m_E be the modular degree of E, i.e., the degree of the fixed optimal modular parametrization $\varphi : X_0(N) \to E$.

LEMMA 3.6. *Suppose that $c \in \Lambda$ satisfies $d(c) > m_E M$. There exists a set of lifting R of $\mathrm{Gal}(K[1]/K)$ into $\mathrm{Gal}(K[c]/K)$, such that $D_0 y_c \notin E(K[c])_{\mathrm{tors}}$, where $D_0 = \sum_{\sigma \in R} \sigma$.*

Proof. The $\mathrm{Gal}(K[c]/K[1])$-orbit of the point $x_c \in X_0(N)(K[c])$ consists of $d(c)$ distinct points (since $K[c] = K(j(\mathcal{O}_c))$), so there are at least $d(c)/m_E$ distinct points in the orbit $\mathrm{Gal}(K[c]/K[1])y_c$. Choose a set of representatives R of $\mathrm{Gal}(K[c]/K)/\mathrm{Gal}(K[c]/K[1])$ which contains the identity element $1 \in \mathrm{Gal}(K[c]/K)$. For $\tau \in \mathrm{Gal}(K[c]/K[1])$ define

$$R_\tau = (R - \{1\}) \cup \{\tau\}.$$

Let $S = \sum_{\sigma \in R} \sigma y_c$ and $S_\tau = \sum_{\sigma \in R_\tau} \sigma y_c$. Then

$$S_\tau - S = \tau y_c - y_c,$$

which takes at least $d(c)/m_E > M$ distinct values. Therefore, there exists an automorphism $\tau \in \mathrm{Gal}(K[c]/K[1])$, for which $S_\tau \notin E(K[c])_{\mathrm{tors}}$, which proves the lemma. $\square$

Proof of Proposition 3.4. Suppose that $c \in \Lambda$ satisfies the statement of Lemma 3.6 for some choice of liftings R and the corresponding $D_0 = \sum_{\sigma \in R}$, i.e., $D_0 y_c \notin E(K[c])_{\text{tors}}$. For any ring class character $\chi : \text{Gal}(K[c]/K) \to \mathbb{C}^\times$, let $e_\chi \in \mathbb{C}[\text{Gal}(K[c]/K)]$ be the eidempotent projector corresponding to χ. Explicitly,

$$e_\chi = \frac{1}{\# \text{Gal}(K[c]/K)} \sum_{\sigma \in \text{Gal}(K[c]/K)} \chi^{-1}(\sigma)\sigma \in \mathbb{C}[\text{Gal}(K[c]/K)].$$

Consider $V = E(K[c]) \otimes \mathbb{C}$ as a complex representation of $\text{Gal}(K[c]/K)$. The representation V decomposes as

$$V = \bigoplus_{\chi : \text{Gal}(K[c]/K) \to \mathbb{C}^\times} V_\chi,$$

where V_χ is the one-dimensional subspace on which $\text{Gal}(K[c]/K[1])$ acts via the character χ. Since the vector $D_0 y_c \otimes 1 \in V$ is non-zero, there exists a ring class character χ, such that $e_\chi(D_0 y_c \otimes 1) \neq 0$.

Next, we consider the point $D_0 D_c y_c \in E(K[c])$ and claim that $D_0 D_c y_c \otimes 1 \in E(K[c]) \otimes \mathbb{C}$ is non-zero, which is sufficient to conclude that $P_c = D_0 D_c y_c \notin E(K[c])_{\text{tors}}$. We will prove that $e_\chi(D_0 D_c y_c \otimes 1) \neq 0$. Indeed,

$$e_\chi(D_0 D_c y_c \otimes 1) = e_\chi D_c(D_0 y_c \otimes 1) = \prod_{\ell | c}\left(\sum_{i=1}^{\ell} i\sigma_\ell^i\right) e_\chi(D_0 y_c \otimes 1) =$$

$$= \prod_{\ell | c}\left(\sum_{i=1}^{\ell} i\chi(\sigma_\ell)^i\right) e_\chi(D_0 y_c \otimes 1),$$

the last equality holding since $\tau e_\chi = \chi(\tau)e_\chi$ in $\mathbb{C}[\text{Gal}(K[c]/K)]$ for all $\tau \in \text{Gal}(K[c]/K)$. Thus, it remains to compute $\sum_{i=1}^{\ell} i\chi(\sigma_\ell)^i$ for every $\ell \mid c$. It is not hard to show that

$$\sum_{i=1}^{\ell} i\chi(\sigma_\ell)^i = \begin{cases} \frac{\ell+1}{\chi(\sigma_\ell)-1} & \text{if } \chi(\sigma_\ell) \neq 1 \\ \frac{\ell(\ell+1)}{2} & \text{if } \chi(\sigma_\ell) = 1. \end{cases}$$

Thus, $e_\chi(D_0 D_c y_c \otimes 1) \neq 0$ which means that $P_c = D_0 D_c y_c \notin E(K[c])_{\text{tors}}$ for any c satisfying $D_0 y_c \notin E(K[c])_{\text{tors}}$. To complete the proof, notice that for all, but finitely many $c \in \Lambda$, the hypothesis of Lemma 3.6 will be satisfied. $\square$

3.6 Computational evidence for Kolyvagin's conjecture

Consider the example $E = \mathbf{389a1}$ with equation $y^2 + y = x^3 + x^2 - 2x$. As in Section 2.3, let $D = 7$, $\ell = 5$, and $p = 3$. Using the algorithm of [GJP$^+$05, §2.1] we verify that the mod p Galois representation $\bar{\rho}_{E,p}$ is surjective. Next, we observe that $\ell = 5$ is a Kolyvagin prime for E, p and D. Let $c = 5$ and consider the class $\kappa_{5,1} \in \mathrm{H}^1(K, E[3])$. We claim that $\kappa_{5,1} \neq 0$, which will verify Kolyvagin's conjecture.

PROPOSITION 3.7. *The class $\kappa_{5,1} \neq 0$. In other words, Kolyvagin's conjecture holds for $E = \mathbf{389a1}$, $D = 7$ and $p = 3$.*

Before proving the proposition, we recall some standard facts about division polynomials (see, e.g., [Sil92, Ex.3.7]). For an elliptic curve given in Weierstrass form over any field of characteristic different from 2 and 3, $y^2 = x^3 + Ax + B$, one defines a sequence of polynomials $\psi_m \in \mathbb{Z}[A, B, x, y]$

inductively as follows:

$$\psi_1 = 1, \ \psi_2 = 2y,$$
$$\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,$$
$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),$$
$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \ \text{ for } m \geqslant 2,$$
$$2y\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \ \text{ for } m \geqslant 3.$$

Define also polynomials ϕ_m and ω_m by

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}, \ 4y\omega_m = \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2.$$

After replacing y^2 by $x^3 + Ax + B$, the polynomials ϕ_m and ψ_m^2 can be viewed as polynomials in x with leading terms x^{m^2} and $m^2 x^{m^2-1}$, respectively. Finally, multiplication-by-m is given by

$$mP = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3} \right).$$

Proof of Proposition 3.7. We already computed the Heegner point y_5 on the model $y^2 + y = x^3 + x^2 - 2x$ in Section 2.3. The Weierstrass model for E is $y^2 = x^3 - 7/3x + 107/108$, so $A = -7/3$ and $B = 107/108$. We now compute the point $P_5 = \sum_{i=1}^{5} i\sigma^i(y_5) \in E(K[5])$ on the Weierstrass model, where σ is a generator of $\mathrm{Gal}(K[5]/K)$. To show that $\kappa_{5,1} \neq 0$ we need to check that there is no point $Q = (x, y)$, such that $3Q = P_5$. For the verification of this fact, we use the division polynomial ψ_3 and the polynomial ϕ_3. Indeed, it follows from the recursive definitions that

$$\phi_3(x) = x^9 - 12Ax^7 - 168Bx^6 + (30A^2 + 72B)x^5 - 168ABx^4 +$$
$$+ (36A^3 + 144AB - 96B^2)x^3 + 72A^2Bx^2 +$$
$$+ (9A^4 - 24A^2B + 96AB^2 + 144B^2)x + 8A^3B + 64B^3.$$

Consider the polynomial $g(x) = \phi_3(x) - X(P_5)\psi_3(x)^2$, where $X(P_5)$ is the x-coordinate of the point P_5 on the Weierstrass model. We factor $g(x)$ (which has degree 9) over the number field $K[5]$ and check that it is irreducible. In particular, there is no root of $g(x)$ in $K[5]$, i.e., there is no $Q \in E(K[5])$, such that $3Q = P_5$. Thus, $\kappa_{5,1} \neq 0$. $\qquad\square$

Remark 6. Using exactly the same method as above, we verify Kolyvagin's conjecture for the other two elliptic curves of rank two from Section 2.3. For both $E = \mathbf{709a1}$ and $E = \mathbf{718b1}$ we use $D = 7$, $p = 3$ and $\ell = 5$ (which are valid parameters), and verify that $\kappa_{5,1} \neq 0$ in the two cases. For completeness, we provide all the data of each computation in the three examples in the files `389a1.txt`, `709a1.txt` and `718a1.txt`.

4. Non-trivial elements in the Shafarevich-Tate group

Throughout the entire section, let $E_{/\mathbb{Q}}$ be a non-CM elliptic curve, $K = \mathbb{Q}(\sqrt{-D})$, where D is a Heegner discriminant for E such that the Heegner point y_K has infinite order in $E(K)$ (which, by the Gross-Zagier formula and Kolyvagin's result, means that $E(K)$ has Mordell-Weil rank one) and let p be a prime, such that $p \nmid DN$ and the mod p Galois representation $\bar{\rho}_{E,p}$ is surjective.

4.1 Non-triviality in Kolyvagin classes.

Under the above assumptions, the next proposition provides a criterion which guarantees that an explicit class in the Shafarevich-Tate group $\mathrm{III}(E/K)$ is non-zero.

PROPOSITION 4.1. *Let $c \in \Lambda_m$. Assume that the following hypotheses are satisfied:*

i) *[Selmer hypothesis]: The class $\kappa_{c,m} \in \mathrm{H}^1(K, E[p^m])$ is an element of the Selmer group $\mathrm{Sel}_{p^m}(E/K)$.*

ii) *[Non-divisibility]: The derived Heegner point P_c is not divisible by p^m in $E(K[c])$, i.e., $P_c \notin p^m E(K[c])$.*

iii) *[Parity]: The number $f_c = \#\{\ell : \ell \mid c\}$ is odd.*

Then the image $\kappa'_{c,m} \in \mathrm{H}^1(K, E)[p^m]$ of $\kappa_{c,m}$ is a non-zero element of $\mathrm{III}(E/K)[p^m]$.

Proof. The first hypothesis implies that the image $\kappa'_{c,m}$ of $\kappa_{c,m}$ in $\mathrm{H}^1(K, E)[p^m]$ is an element of the Shafarevich-Tate group $\mathrm{III}(E/K)$. The second one implies that $\kappa_{c,m} \neq 0$. To show that $\kappa'_{c,m} \neq 0$ we use the exact sequence

$$0 \to E(K)/p^m E(K) \to \mathrm{Sel}_{p^m}(E/K) \to \mathrm{III}(E/K)[p^m] \to 0$$

which splits under the action of complex conjugation as

$$0 \to (E(K)/p^m E(K))^{\pm} \to \mathrm{Sel}_{p^m}(E/K)^{\pm} \to \mathrm{III}(E/K)^{\pm}[p^m] \to 0.$$

According to [Gro91, Prop.5.4(2)], the class $\kappa_{c,m}$ lies in the ε_c-eigenspace of the Selmer group $\mathrm{Sel}_{p^m}(E/K)$ for the action of complex conjugation, where $\varepsilon_c = \varepsilon(-1)^{f_c} = -1$ (f_c is odd by the third hypothesis and $\varepsilon = 1$ since $-\varepsilon$ is the sign of the functional equation for $E_{/K}$ which is -1 by Gross-Zagier). On the other hand, the Heegner point $y_K = P_1$ lies in the ε_1-eigenspace of complex conjugation (again, by [Gro91, Prop.5.4(2)]) where $\varepsilon_1 = \varepsilon(-1)^{f_1} = 1$. Since $E(K)$ has rank one, the group $E(K)^-$ is torsion and since $E(K)[p] = 0$, we obtain that $(E(K)/p^m E(K))^- = 0$. Therefore,

$$\mathrm{Sel}_{p^m}(E/K)^- \cong \mathrm{III}(E/K)^-[p^m],$$

which implies $\kappa'_{c,m} \neq 0$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\square$

4.2 The example $E = \mathbf{53a1}$.

The Weierstrass equation for the curve $E = \mathbf{53a1}$ is $y^2 = x^3 + 405x + 16038$ and E has rank one over $\mathbb{Q}$. The Fourier coefficient $a_5(f) \equiv 5 + 1 \equiv 0 \mod 3$, so $\ell = 5$ is a Kolyvagin prime for E, the discriminant $D = 43$ and the prime $p = 3$. Kolyvagin's construction exhibits a class $\kappa_{5,1} \in \mathrm{H}^1(K, E[3])$. We will prove the following proposition:

PROPOSITION 4.2. *The cohomology class $\kappa_{5,1} \in \mathrm{H}^1(K, E[3])$ lies in the Selmer group $\mathrm{Sel}_3(E/K)$ and its image $\kappa'_{5,1}$ in the Shafarevich-Tate group $\mathrm{III}(E/K)$ is a nonzero 3-torsion element.*

Remark 7. Since E/K has analytic rank one, Kolyvagin's conjecture is automatic (since $m_0 < \infty$ by Gross-Zagier's formula) and one knows (see [McC91, Thm. 5.8]) that there exist Kolyvagin classes $\kappa'_{c,m}$ which generate $\mathrm{III}(E/K)[p^\infty]$. Yet, this result is not explicit in the sense that one does not know any particular Kolyvagin class which is non-trivial. The above proposition exhibits an explicit non-zero cohomology class in the p-primary part of the Shafarevich-Tate group $\mathrm{III}(E/K)$.

Proof. Using the data computed in Section 2.3 for this curve, we apply the Kolyvagin derivative to compute the point P_5. In order to do this, one needs a generator of the Galois group $\mathrm{Gal}(K[5]/K)$. Such a generator is determined by the image of α, which will be another root of $f(x)$ in $K[5]$. We check that the automorphism σ defined by

$$\alpha \mapsto \frac{1}{1601320}(47343 + 54795\sqrt{-43})\alpha^5 + \frac{1}{2401980}(-614771 - 936861\sqrt{-43})\alpha^4 +$$

$$+ \frac{1}{600495}(34507457 + 40541607\sqrt{-43})\alpha^3 + \frac{1}{4803960}(102487877 - 767102463\sqrt{-43})\alpha^2 +$$

$$+ \frac{1}{400330}(-61171198 + 52833377\sqrt{-43})\alpha + \frac{1}{200165}(18971815 - 7453713\sqrt{-43})$$

11

is a generator (we found this automorphism by factoring the defining polynomial of the number field over the number field $K[5]$). Thus, we can compute $P_5 = \sum_{i=1}^{5} i\sigma^i(y_5)$.

Note that we are computing the point on the Weierstrass model of E rather than on the original model. The cohomology class $\kappa_{5,1}$ is trivial if and only if $P_5 \in 3E(K[5])$. To show that $P_5 \notin 3E(K[5])$, we repeat the argument from Proposition 3.7 and verify (using any factorization algorithm for polynomials over number fields) that the polynomial $g(x) = \phi_3(x) - X(P_5)\psi_3(x)^2$ has no linear factors over $K[5]$ (here, $X(P_5)$ is the x-coordinate of P_5). This means that there is no point $Q = (x, y) \in E(K[5])$, such that $3Q = P_5$, i.e., $\kappa_{5,1} \neq 0$. Finally, using Proposition 4.1 we conclude that the class $\kappa'_{5,1} \in \text{III}(E/K)[3]$ is non-trivial. $\qquad\square$

Remark 8. For completeness, all the computational data is provided (with the appropriate explanations) in the file `53a1.txt`. We verified the irreducibility of $g(x)$ using MAGMA and PARI/GP independently.

Appendix A. Upper bounds on the logarithmic heights of the Heegner points y_c

We explain how to compute an upper bound on the logarithmic height $h(y_c)$. The method first relates the canonical height $\widehat{h}(y_c)$ to special values of the first derivatives of certain automorphic L-functions via Zhang's generalization of the Gross-Zagier formula. Then we either compute the special values up to arbitrary precision using a well-known algorithm (recently implemented by Dokchitser) or use effective asymptotic upper bounds (convexity bounds) on the special values and Cauchy's integral formula. Finally, using some known bounds on the difference between the canonical and the logarithmic heights, we obtain explicit upper bounds on the logarithmic height $h(y_c)$. We provide a summary of the asymptotic bounds in Section A.4 and refer the reader to [Jet] for complete details.

A.1 The automorphic L-functions $L(f, \chi, s)$ and $L(\pi_{f \otimes \theta_\chi}, s)$

Let $d_c = c^2 D$ and let $f = \sum_{n \geqslant 1} a_n q^n$ be the new eigenform of level N and weight two corresponding to E. Let $\chi : \text{Gal}(K[c]/K) \to \mathbb{C}^\times$ be a ring class character.

1. The theta series θ_χ. Recall that ideal classes for $\text{Pic}(\mathcal{O}_c)$ correspond to primitive, reduced binary quadratic forms of discriminants d_c. To each ideal class $\mathcal{A}$ we consider the corresponding binary quadratic form $Q_\mathcal{A}$ and the theta series $\theta_{Q_\mathcal{A}}$ associated to it via

$$\theta_{Q_\mathcal{A}} = \sum_M e^{2\pi i z Q_\mathcal{A}(M)}$$

which is a modular form for $\Gamma_0(d_c)$ of weight one with character ε (the quadratic character of K) according to Weil's converse theorem (see [Shi71] for details). This allows us to define a cusp form

$$\theta_\chi = \sum_{\mathcal{A} \in \text{Pic}(\mathcal{O}_c)} \chi^{-1}(\mathcal{A})\theta_{Q_\mathcal{A}} \in S_1(\Gamma_0(d_c), \varepsilon).$$

Here, we view χ^{-1} as a character of $\text{Pic}(\mathcal{O}_c)$ via the isomorphism $\text{Pic}(\mathcal{O}_c) \cong \text{Gal}(K[c]/K)$. Let $\theta_\chi = \sum_{m \geqslant 0} b_m q^m$ be the Fourier expansion. By $L(f, \chi, s)$ we will always mean the Rankin L-function $L(f \otimes \theta_\chi, s)$ (equivalently, the L-function associated to the automorphic representation $\pi = f \otimes \theta_\chi$ of GL_4).

2. The functional equation of $L(f, \chi, s)$. We recall some basic facts about the Rankin L-series $L(f \otimes \theta_\chi, s)$ following [Gro84, §III]. Since $(N, D) = 1$, the *conductor* of $L(f \otimes \theta_\chi, s)$ is $Q = N^2 d_c^2$.

The Euler factor at infinity (the gamma factor) is $L_\infty(f \otimes \theta_\chi, s) = \Gamma_{\mathbb{C}}(s)^2$. If we set

$$\Lambda(f \otimes \theta_\chi, s) = Q^{s/2} L_\infty(f \otimes \theta_\chi, s) L(f \otimes \theta_\chi, s)$$

then the function Λ has a holomorphic continuation to the entire complex plane and satisfies the functional equation

$$\Lambda(f \otimes \theta_\chi, s) = -\Lambda(f \otimes \theta_\chi, 2 - s).$$

In particular, the order of vanishing of $L(f \otimes \theta_\chi, s)$ at $s = 1$ is non-negative and odd, i.e., $L(f \otimes \theta_\chi, 1) = 0$.

3. The automorphic L-function $L(\pi_{f \otimes \theta_\chi}, s)$. In order to center the critical line at $\mathrm{Re}(s) = \dfrac{1}{2}$ instead of $\mathrm{Re}(s) = 1$ (which is consistent with Langlands convention), we consider the L-function $L(\pi_{f \otimes \theta_\chi}, s)$ corresponding to the automorphic representation attached to $f \otimes \theta_\chi$ for GL_4. This function satisfies

$$L(\pi_{f \otimes \theta_\chi}, s) = L\left(f \otimes \theta_\chi, s + \frac{1}{2}\right)$$

The function $L(\pi_{f \otimes \theta_\chi}, s)$ then satisfies a functional equation relating the values at s and $1 - s$. For a general automorphic L-function $L(\pi, s)$, we consider the corresponding Dirichlet series and Euler product

$$L(\pi, s) = \sum_{n \geqslant 1} \frac{\lambda_\pi(n)}{n^s} = \prod_p (1 - \alpha_{\pi,1}(p) p^{-s})^{-1} \dots (1 - \alpha_{\pi,d}(p) p^{-s})^{-1},$$

which are absolutely convergent for $\mathrm{Re}(s) > 1$.

A.2 Zhang's formula

For a character χ of $\mathrm{Gal}(K[c]/K)$, let

$$e_\chi = \frac{1}{\# \mathrm{Gal}(K[c]/K)} \sum_{\sigma \in \mathrm{Gal}(K[c]/K)} \chi^{-1}(\sigma)\sigma \in \mathbb{C}[\mathrm{Gal}(K[c]/K)]$$

be the associated eidempotent (see also Section 3.5). The canonical height $\widehat{h}(e_\chi y_c)$ is related via the generalized Gross-Zagier formula of Zhang to a special value of the derivative of the Rankin-Selberg L-function $L(f, \chi, s)$ at $s = 1$ (see [Zha01, Thm.1.2.1]). More precisely,

THEOREM A.1 (Zhang). *If $(\,,)$ denotes the Petersson inner product on $S_2(\Gamma_0(N))$ then*

$$L'(f, \chi, 1) = \frac{4}{\sqrt{D}} (f, f) \widehat{h}(e_\chi y_c).$$

Since $\langle e_{\chi'} y_c, e_{\chi''} y_c \rangle = 0$ whenever $\chi' \neq \chi''$ (here, $\langle\,,\rangle$ denotes the Néron-Tate height pairing for E) and since $\widehat{h}(x) = \langle x, x \rangle$ then

$$\widehat{h}(y_c) = \widehat{h}\left(\sum_\chi e_\chi y_c\right) = \sum_\chi \widehat{h}(e_\chi y_c). \tag{3}$$

Thus, we will have an upper bound on the canonical height $\widehat{h}(y_c)$ if we obtain upper bounds on the special values $L'(f, \chi, 1)$ for every character χ of $\mathrm{Gal}(K[c]/K)$.

A.3 Computing special values of derivatives of automorphic L-functions

For simplicity, let $\gamma(s) = L_\infty(f \otimes \theta_\chi, s + 1/2)$ be the gamma factor of the L-function $L(\pi, s)$. This means that if $\Lambda(\pi, s) = Q^{s/2}\gamma(s)L(\pi, s)$ then $\Lambda(\pi, s)$ satisfies the functional equation $\Lambda(\pi, s) = \Lambda(\pi, 1 - s)$. We will describe a classical algorithm to compute the value of $L^{(k)}(\pi, s)$ at $s = s_0$ up

to arbitrary precision. The algorithm and its implementation is discussed in a greater generality in [Dok04]. The main idea is to express $\Lambda(\pi, s)$ as an infinite series with rapid convergence which is usually done in the following sequence of steps:

i) Consider the inverse Mellin transform of the gamma factor $\gamma(s)$, i.e., the function $\phi(t)$ which satisfies

$$\gamma(s) = \int_0^\infty \phi(t) t^s \frac{dt}{t}.$$

One can show (see [Dok04, §3]) that $\phi(t)$ decays exponentially for large t. Hence, the sum

$$\Theta(t) = \sum_{n=1}^\infty \lambda_\pi(n) \phi\left(\frac{nt}{\sqrt{Q}}\right)$$

converges exponentially fast. The function $\phi(t)$ can be computed numerically as explained in [Dok04, §3-5].

ii) The Mellin transform of $\Theta(t)$ is exactly the function $\Lambda(\pi, s)$. Indeed,

$$\int_0^\infty \Theta(t) t^s \frac{dt}{t} = \int_0^\infty \sum_{n=1}^\infty \lambda_\pi(n) \phi\left(\frac{nt}{\sqrt{Q}}\right) t^s \frac{dt}{t} = \sum_{n=1}^\infty \lambda_\pi(n) \int_0^\infty \phi\left(\frac{nt}{\sqrt{Q}}\right) t^s \frac{dt}{t} =$$

$$= \sum_{n=1}^\infty \lambda_\pi(n) \left(\frac{\sqrt{Q}}{n}\right)^s \int_0^\infty \phi(t') t'^s \frac{dt'}{t'} = Q^{s/2} \gamma(s) L(\pi, s) = \Lambda(\pi, s).$$

iii) Next, we obtain a functional equation for $\Theta(t)$ which relates $\Theta(t)$ to $\Theta(1/t)$. Indeed, since $\Lambda(\pi, s)$ is holomorphic, Mellin's inversion formula implies that

$$\Theta(t) = \int_{c-i\infty}^{c+i\infty} \Lambda(\pi, s) t^{-s} ds, \ \forall c.$$

Therefore,

$$\Theta(1/t) = \int_{c-i\infty}^{c+i\infty} \Lambda(\pi, s)(1/t)^{-s} ds = -t \int_{c-i\infty}^{c+i\infty} \Lambda(\pi, 1-s) t^{-(1-s)} ds =$$

$$= -t \int_{c-i\infty}^{c+i\infty} \Lambda(\pi, s') t^{-s'} ds' = -t\Theta(t).$$

Thus, $\Theta(t)$ satisfies the functional equation $\Theta(1/t) = -t\Theta(t)$.

iv) Next, we consider the incomplete Mellin transform

$$G_s(t) = t^{-s} \int_t^\infty \phi(x) x^s \frac{dx}{x}, \ t > 0$$

of $\phi(t)$. The function $G_s(t)$ satisfies $\lim_{t\to 0} t^s G_s(t) = \gamma(s)$ and it decays exponentially. Moreover, it can be computed numerically (see [Dok04, §4-5]).

v) Finally, we use the functional equation for $\Theta(t)$ to obtain

$$\Lambda(\pi, s) = \int_0^\infty \Theta(t) t^s \frac{dt}{t} = \int_0^1 \Theta(t) t^s \frac{dt}{t} + \int_1^\infty \Theta(t) t^s \frac{dt}{t} =$$

$$= \int_1^\infty \Theta(1/t') t'^{-s} \frac{dt'}{t'} + \int_1^\infty \Theta(t) t^s \frac{dt}{t} =$$

$$= -\int_1^\infty \Theta(t') t'^{1-s} \frac{dt'}{t'} + \int_1^\infty \Theta(t) t^s \frac{dt}{t}.$$

vi) Finally, we compute

$$\int_1^\infty \Theta(t) t^s \frac{dt}{t} = \int_1^\infty \sum_{n=1}^\infty \lambda_\pi(n) \phi\left(\frac{nt}{\sqrt{Q}}\right) t^s \frac{dt}{t} = \sum_{n=1}^\infty \lambda_\pi(n) \int_1^\infty \phi\left(\frac{nt}{\sqrt{Q}}\right) t^s \frac{dt}{t} =$$

$$= \sum_{n=1}^\infty \lambda_\pi(n) \int_{\frac{n}{\sqrt{Q}}}^\infty \phi\left(t'\right) \left(\frac{\sqrt{Q}t'}{n}\right)^s = \sum_{n=1}^\infty \lambda_\pi(n) G_s\left(\frac{n}{\sqrt{Q}}\right).$$

Thus,

$$\Lambda(\pi, s) = \sum_{n=1}^\infty \lambda_\pi(n) G_s\left(\frac{n}{\sqrt{Q}}\right) - \sum_{n=1}^\infty \lambda_\pi(n) G_{1-s}\left(\frac{n}{\sqrt{Q}}\right)$$

is the desired expansion. From here, we obtain a formula for the k-th derivative

$$\frac{\partial^k}{\partial s^k} \Lambda(\pi, s) = \sum_{n=1}^\infty \lambda_\pi(n) \frac{\partial^k}{\partial s^k} G_s\left(\frac{n}{\sqrt{Q}}\right) - \sum_{n=1}^\infty \lambda_\pi(n) \frac{\partial^k}{\partial s^k} G_{1-s}\left(\frac{n}{\sqrt{Q}}\right).$$

The computation of the derivatives of $G_s(x)$ is explained in [Dok04, §3-5].

A.4 Asymptotic estimates on the canonical heights $\widehat{h}(y_c)$

In this section we provide an asymptotic bound on the canonical height $\widehat{h}(y_c)$ by using convexity bounds on the special values of the automorphic L-functions $L(\pi, s)$ defined in Section A.1. We only outline the basic techniques used to prove the asymptotic bounds and refer the reader to [Jet] for the complete details. Asymptotic bounds on heights of Heegner points are obtained in [RV], but these bounds are of significantly different type than ours. In our case, we fix the elliptic curve E and let the fundamental discriminant D and the conductor c of the ring class field both vary. We obtain the following:

PROPOSITION A.2. *Fix the elliptic curve E and let the fundamental discriminant D and the conductor c vary. For any $\varepsilon > 0$ the following asymptotic bound holds*

$$\widehat{h}(y_c) \ll_{\varepsilon, f} h_D D^\varepsilon c^{2+\varepsilon},$$

where h_D is the class number of the quadratic imaginary field $K = \mathbb{Q}(\sqrt{-D})$. Moreover, the implied constant depends only on ε and the cusp form f.

One proves the proposition by combining the formula of Zhang with convexity bounds on special values of automorphic L-functions. The latter are conveniently expressed in terms of a quantity known as the *analytic conductor* associated to the automorphic representation π (see [Mic02, p.12]). It is a function $Q_\pi(t)$ over the real line, which is defined as

$$Q_\pi(t) = Q \cdot \prod_{i=1}^d (1 + |it - \mu_{\pi,i}|), \ \forall t \in \mathbb{R},$$

where $\mu_{\pi,i}$ are obtained from the gamma factor

$$L_\infty(\pi, s) = \prod_{i=1}^d \Gamma_{\mathbb{R}}(s - \mu_{\pi,i}), \ \Gamma_{\mathbb{R}}(s) = \pi^{-s/2} \Gamma(s/2).$$

In our situation for $\pi = \pi_{f\otimes\theta_\chi}$, $d = 4$ and $\mu_{\pi,1} = \mu_{\pi,2} = 0$, $\mu_{\pi,3} = \mu_{\pi,4} = 1$ (see [Mic02, §1.1.1] and [Ser70, §3] for discussions of local factors at archimedian places). Moreover, we let $Q_\pi = Q_\pi(0)$.

The main idea is to prove that for a fixed f, $|L'(\pi_{f\otimes\theta_\chi}, 1/2)| \ll_{\varepsilon, f} Q_{\pi_{f\otimes\theta_\chi}}^{1/4+\varepsilon}$, where the implied constant only depends on f and ε (and is independent of χ and the discriminant D). To establish the bound, we first prove an asymptotic bound for the L-function $L(\pi_{f\otimes\theta_\chi}, s)$ on the vertical line $\text{Re}(s) =$

$1+\varepsilon$ by either using the Ramanujan-Petersson conjecture or a method of Iwaniec (see [Mic02, p.26]). This gives us the estimate $|L(\pi_{f\otimes\theta_\chi}, 1+\varepsilon+it)| \ll_{\varepsilon,f} Q_{\pi_{f\otimes\theta_\chi}}(t)^\varepsilon$. Then, by the functional equation for $L(\pi_{f\otimes\theta_\chi}, s)$ and Stirling's approximation formula, we deduce an upper bound for the L-function on the vertical line $\mathrm{Re}(s) = -\varepsilon$, i.e., $|L(\pi_{f\otimes\theta_\chi}, -\varepsilon+t)| \ll_{\varepsilon,f} Q_{\pi_{f\otimes\theta_\chi}}(t)^{1/2+\varepsilon}$. Next, we apply Phragmen-Lindelöf's convexity principle (see [IK04, Thm.5.53]) to obtain the bound $|L(\pi_{f\otimes\theta_\chi}, 1/2+it)| \ll_{\varepsilon,f} Q_\pi(t)^{1/4+\varepsilon}$ (also known as *convexity bound*). Finally, by applying Cauchy's integral formula for a small circle centered at $s = 1/2$, we obtain the asymptotic estimate $|L'(\pi_{f\otimes\theta_\chi}, 1/2)| \ll_{\varepsilon,f} Q_{\pi_{f\otimes\theta_\chi}}^{1/4+\varepsilon}$. Since $Q = N^2 d_c^2 = N^2 D^2 c^4$ in our situation and since $[K[c] : K] = h_D \prod_{\ell|c}(\ell + 1)$, Zhang's formula (Theorem A.1) and equation (3) imply that for any $\varepsilon > 0$,

$$\widehat{h}(y_c) \ll_{\varepsilon,f} h_D D^\varepsilon c^{2+\varepsilon}.$$

Remark 9. In the above situation (the Rankin-Selberg L-function of two cusp forms of levels N and $d_c = c^2 D$), one can even prove a subconvexity bound $|L'(\pi_{f\otimes\theta_\chi}, 1/2)| \ll_f D^{1/2-1/1057} c^{1-2/1057}$, where the implied constant depends only on f and is independent of χ (see [Mic04, Thm.2]). Yet, the proof relies on much more involved analytic number theory techniques than the convexity principle, so we do not discuss it here.

A.5 Height difference bounds and the main estimates

To estimate $h(y_c)$ we need a bound on the difference between the canonical and the logarithmic heights. Such a bound has been established in [Sil90] and [CPS06] and is effective.

Let F be a number field. For any non-archimedian place v of K, let $E^0(F_v)$ denote the points of $E(F_v)$ which specialize to the identity component of the Néron model of E over the ring of integers $\mathcal{O}_v$ of F_v. Moreover, let $n_v = [F_v : \mathbb{Q}_v]$ and let M_F^∞ denote the set of all archimedian places of F. A slightly weakened (but easier to compute) bounds on the height difference are provided by the following result of [CPS06, Thm.2]

THEOREM A.3 (Cremona-Prickett-Siksek). *Let $P \in E(F)$ and suppose that $P \in E^0(F_v)$ for every non-archimedian place v of F. Then*

$$\frac{1}{3[F : \mathbb{Q}]} \sum_{v\in M_F^\infty} n_v \log\delta_v \leqslant h(P) - \widehat{h}(P) \leqslant \frac{1}{3[F : \mathbb{Q}]} \sum_{v\in M_F^\infty} n_v \log\varepsilon_v,$$

where ε_v and δ_v are defined in [CPS06, §2].

Remark 10. All of the points y_c in our particular examples satisfies the condition $y_c \in E^0(K[c]_v)$ for all non-archimedian places v of $K[c]$. Indeed, according to [GZ86, §III.3] (see also [Jet07, Cor.3.2]) the point y_c lies in $E^0(K[c]_v)$ up to a rational torsion point. Since $E(\mathbb{Q})_{\mathrm{tors}}$ is trivial for all the curves that we are considering, the above proposition is applicable. In general, one does not need this assumption in order to compute height difference bounds (see [CPS06, Thm.1] for the general case).

Remark 11. A method for computing ε_v and δ_v up to arbitrary precision for real and complex archimedian places is provided in [CPS06, §7-9].

References

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).

BFH90 D. Bump, S. Friedberg, and J. Hoffstein, *Eisenstein series on the metaplectic group and nonvanishing theorems for automorphic L-functions and their derivatives*, Ann. of Math. (2) **131** (1990), no. 1, 53–127.

Coh07 H. Cohen, *Number theory II: Analytic and modern methods*, Graduate Texts in Mathematics, vol. 240, Springer, 2007.

Cor02 C. Cornut, *Non-trivialité des points de Heegner*, C. R. Math. Acad. Sci. Paris **334** (2002), no. 12, 1039–1042.

CPS06 J. E. Cremona, M. Prickett, and Samir Siksek, *Height difference bounds for elliptic curves over number fields*, J. Number Theory **116** (2006), no. 1, 42–68.

Cre J. E. Cremona, *Tables of Elliptic Curves,*
http://www.maths.nott.ac.uk/personal/jec/ftp/data/.

Del02 C. Delauney, *Formes modulaires et invariants de courbes elliptiques définies sur* **Q**, Université Bordeaux I, PhD thesis (2002).

Dok04 T. Dokchitser, *Computing special values of motivic L-functions*, Experiment. Math. **13** (2004), no. 2, 137–149.

EJL06 K. Eisentraeger, D. Jetchev, and K. Lauter, *On the computation of the Cassels pairing for certain Kolyvagin classes in the Shafarevich-Tate group*, preprint (2006).

Elk94 N. D. Elkies, *Heegner point computations*, Algorithmic number theory (Ithaca, NY, 1994), Springer, Berlin, 1994, pp. 122–133.

GJP+05 G. Grigorov, A. Jorza, S. Patrikis, C. Patrascu, and W. Stein, *Verification of the Birch and Swinnerton-Dyer Conjecture for Specific Elliptic Curves*, (Submitted)
http://wstein.org/papers/bsdalg/ (2005).

Gro84 B. Gross, *Heegner points on $X_0(N)$*, Modular forms (Durham, 1983), Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., Horwood, Chichester, 1984, pp. 87–105.

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.

IK04 H. Iwaniec and E. Kowalski, *Analytic Number Theory*, vol. 53, American Mathematical Society, 2004.

Jet D. Jetchev, *Asymptotic heights of Heegner points over ring class fields*, in preparation.

Jet07 _____, *Global divisibility of Heegner points and Tamagawa numbers*, preprint (2007).

Kol90 V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.

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

Kol91b V. A. Kolyvagin, *On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves*, Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990) (Tokyo), Math. Soc. Japan, 1991, pp. 429–436.

Kol91c _____, *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.

Mic02 P. Michel, *Analytic number theory and families of L-functions*, www.math.univ-montp2.fr/~michel/fichierdvi/Parkcitylectures.pdf (2002).

Mic04 _____, *The subconvexity problem for Rankin-Selberg L-functions and equidistribution of Heegner points*, Ann. of Math. (2) **160** (2004), no. 1, 185–236.

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

MM97   M. R. Murty and V. K. Murty, *Non-vanishing of L-functions and applications*, Birkhäuser Verlag, Basel, 1997.

Nek01   Jan Nekovář, *On the parity of ranks of Selmer groups. II*, C. R. Acad. Sci. Paris Sér. I Math. **332** (2001), no. 2, 99–104.

RV   G. Ricotta and T. Vidick, *Hauteurs asymptotique des points de Heegner*, preprint.

Ser70   J.-P. Serre, *Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures)*, Séminaire Delange-Pisot-Poitou. Théorie des nombres 11, no. 2, Exposé No. 19 (1969-70).

Shi71   G. Shimura, *On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields*, Nagoya Math. J. **43** (1971), 199–208.

Sil90   Joseph H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. **55** (1990), no. 192, 723–743.

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

Sil94   _____, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.

Tat67   J. T. Tate, $p - divisible\ groups.$, Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin, 1967, pp. 158–183.

Wat04   Mark Watkins, *Some remarks on Heegner point computations*, Preprint, 2004.

Zha01   S. W. Zhang, *Gross-Zagier formula for GL_2*, Asian J. Math. **5** (2001), no. 2, 183–290.

Dimitar Jetchev   jetchev@math.berkeley.edu
Department of Mathematics, University of California at Berkeley, Berkeley, CA 94720

Kristin Lauter   klauter@microsoft.com
Microsoft Research, One Microsoft Way, Redmond, WA 98052

William Stein   wstein@math.washington.edu
Department of Mathematics, University of Washington, Seattle, WA 98195