ON THE COMPUTATION OF THE CASSELS PAIRING FOR CERTAIN KOLYVAGIN CLASSES IN THE SHAFAREVICH-TATE GROUP

KIRSTEN EISENTRÄGER, DIMITAR JETCHEV, AND KRISTIN LAUTER

Abstract. Kolyvagin has shown how to study the Shafarevich-Tate group of elliptic curves over imaginary quadratic fields via Kolyvagin classes constructed from Heegner points. One way to produce explicit non-trivial elements of the Shafarevich-Tate group is by proving that a locally trivial Kolyvagin class is globally non-trivial, which is difficult in practice. We provide a method for testing whether an explicit element of the Shafarevich-Tate group represented by a Kolyvagin class is globally non-trivial by determining whether the Cassels pairing between the class and another locally trivial Kolyvagin class is non-zero. Our algorithm explicitly computes Heegner points over ring class fields to produce the Kolyvagin classes and uses the efficiently computable cryptographic Tate pairing.

1. Introduction

The Kolyvagin Euler system of cohomology classes constructed in [13] (see also [10] and [17]) is one of the most powerful tools for studying the Shafarevich-Tate group of an elliptic curve over a quadratic imaginary field with a Heegner discriminant. Under certain assumptions, it can be used to prove that the Shafarevich-Tate group of the elliptic curve is finite, and to determine its exact group structure (see [10], [13] and [17]). The cohomology classes constructed by Kolyvagin are locally trivial at all but a finite set of places. One can write down local divisibility conditions on the corresponding Heegner points which are equivalent to local triviality at the remaining finite set of places. Yet, even when those conditions are satisfied, there is no guarantee that the Kolyvagin cohomology class is a non-trivial element of the Shafarevich-Tate group.

One strategy for proving that such an element corresponds to a non-trivial element of the Shafarevich-Tate group is to prove that it pairs with another element of the Shafarevich-Tate group via the Cassels pairing to a nonzero element of $\mathbb{Q}/\mathbb{Z}$. The Cassels pairing is a skew-symmetric pairing on the Shafarevich-Tate group $Ш(K, E)$ which is non-degenerate when $Ш(K, E)$ is finite. To use this approach we need a way of explicitly computing the Cassels pairing. Our goal in this paper is to describe a method for deciding whether the Cassels pairing on two suitably chosen distinct locally trivial

Kolyvagin cohomology classes is nonzero. The algorithm uses the cryptographic Tate pairing and the computation of Heegner points over ring class fields.
Our algorithm may have interesting applications to the study of $Ш(K, E)$. For instance, Mazur and Rubin ([16]) have suggested that $Ш(K, E)$ should be generated by locally trivial Kolyvagin cohomology classes. An interesting computational question is to test this conjecture experimentally and to observe in practice and predict bounds on the size of the Kolyvagin primes necessary to find generators for $Ш(K, E)[p]$. Furthermore, our algorithm may be used for producing examples related to visibility of $Ш(K, E)$ at higher level in the sense of Stein and the second author (see [12]).

In Section 2 we recall the definition of the Shafarevich-Tate group of an elliptic curve. Section 3 provides the necessary background on Heegner points and describes the construction of the Kolyvagin cohomology classes out of these points. In Section 4 we explain how to decide whether a Kolyvagin cohomology class is locally trivial. The algorithm takes as input the coordinates of the Heegner point in the corresponding ring class field.

In Section 5 we discuss the Cassels pairing in general and establish a formula for the pairing of two locally trivial Kolyvagin classes in terms of the Tate local pairing. In Section 6 we explain how the Tate local pairing is related to a pairing over finite fields, known in the cryptographic literature as the (cryptographic) Tate pairing. In Section 7 we apply the pairing for suitably chosen Kolyvagin classes to decide whether they pair non-trivially via the Cassels pairing. Finally, in Section 8 we explain the computation of the coordinates of Heegner points over ring class fields and give an example.

Acknowledgments: We thank Ken Ribet and William Stein for many helpful discussions. We thank Noam Elkies for answering several questions regarding Heegner point computations. Finally, we thank Sebastian Pauli for kindly providing a package for computations with non-maximal orders.

2. Notation and Background

For a field K, $\overline{K}$ denotes an algebraic closure of K. For a number field K, M_K denotes the set of places of K (both archimedean and non-archimedean). For $v \in M_K$, K_v is the completion of K at v. For a field K and a smooth commutative K-group scheme G, $\mathrm{H}^i(K, G)$ denotes the Galois cohomology group $\mathrm{H}^i(G_{K_s/K}, G(K_s))$ where K_s is a fixed separable closure of K.

Let E be an elliptic curve over a number field K. The *Shafarevich-Tate group* of E over K is

$$Ш(K, E) := \mathrm{Ker}\left(\mathrm{H}^1(K, E) \to \prod_{v \in M_K} \mathrm{H}^1(K_v, E)\right).$$

We also define the m-Selmer group $\mathrm{Sel}^{(m)}(K,E)$ of the elliptic curve as

$$\mathrm{Sel}^{(m)}(K,E) := \mathrm{Ker}\left(\mathrm{H}^1(K,E_m) \to \prod_{v\in M_K} \mathrm{H}^1(K_v,E)_m\right),$$

where each map $\mathrm{H}^1(K,E_m) \to \mathrm{H}^1(K_v,E)_m$ is the composition of the map $\mathrm{H}^1(K,E_m) \to \mathrm{H}^1(K_v,E_m)$ and $\mathrm{H}^1(K_v,E_m) \to \mathrm{H}^1(K_v,E)_m$ (for more details see [22, Ch.X]).

In general, if m is a positive integer and G is an abelian group object, we denote by either G_m or $G[m]$ the kernel of the multiplication-by-m map on G.

3. Heegner Points and the Kolyvagin Construction

3.1. **Heegner Points over Ring Class Fields.** The standard references for this section are [10], [13] and [17]. Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. Let $K = \mathbb{Q}(\sqrt{-D})$, where $-D$ is a fundamental discriminant, $D \neq 3, 4$, and all prime factors of N are split in K, i.e. $(N) = \mathcal{N}\bar{\mathcal{N}}$ for an ideal $\mathcal{N}$ of the ring of integers $\mathcal{O}_K$ of K with $\mathcal{O}_K/\mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}$. We call such a discriminant a *Heegner discriminant* for $E/\mathbb{Q}$. By the modularity theorem [2], there is a modular parameterization $\varphi : X_0(N) \to E$. 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 $\mathbb{C}/\mathcal{N}^{-1}$. Here $\mathcal{N}^{-1}$ denotes the fractional ideal of $\mathcal{O}_K$ for which $\mathcal{N}\mathcal{N}^{-1} = \mathcal{O}_K$. This isogeny corresponds to a complex point $x_1 \in X_0(N)$. According to the theory of complex multiplication [23, Ch.II], the point x_1 is defined over the Hilbert class field K_1 of K.

More generally, let $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$ be the order of index n in $\mathcal{O}_K$ and let $\mathcal{N}_n = \mathcal{N} \cap \mathcal{O}_n$. Then $\mathcal{O}_n/\mathcal{N}_n \simeq \mathbb{Z}/N\mathbb{Z}$ and the map $\mathbb{C}/\mathcal{O}_n \to \mathbb{C}/\mathcal{N}_n^{-1}$ is a cyclic isogeny of degree N and thus it defines a point $x_n \in X_0(N)(\mathbb{C})$. Again, by the theory of complex multiplication, this point is defined over the ring class field K_n of conductor n over K.

One can use the parameterization $\varphi : X_0(N) \to E$ to obtain points $y_n = \varphi(x_n)$ on E. Define y_K to be the point $y_K = \mathrm{Tr}_{K_1/K}(y_1)$. If $\mathcal{N}'$ is another ideal with $\mathcal{O}/\mathcal{N}' \simeq \mathbb{Z}/N\mathbb{Z}$, we have $y_K = \pm y_K +$ (torsion). We refer to y_K as the Heegner point for the discriminant D.

3.2. **Surjectivity of the Galois Representation and Choice of p.** Let E and K be as above. For a rational prime p, let $\mathbb{Q}(E_p)$ be the extension generated by the p-torsion points of E in $\overline{K}$. If the elliptic curve E does not have complex multiplication then according to a theorem of Serre [21, Thm. 2], the extension $\mathbb{Q}(E_p)/\mathbb{Q}$ has Galois group $\mathrm{GL}_2(\mathbb{F}_p)$ for all but finitely many primes p; i.e., the associated mod p Galois representation is surjective for all but finitely many primes p.

In practice, one tests the surjectivity of the Galois representation for a given E and p by using the algorithm of [9, §2.1] which has been implemented

by Stein in the computer algebra system SAGE [24]. For instance, if E is the curve 681B1 in Cremona's tables [4], then E is given by the Weierstrass equation $y^2 + xy = x^3 + x^2 - 1154x - 15345$, and the algorithm implies that the mod 3 Galois representation associated to E is surjective.

3.3. **Construction of the Cohomology Classes.** In [13], Kolyvagin uses the points y_n for suitably chosen indices n to define cohomology classes $d_{n,m} \in \mathrm{H}^1(K, E)_{p^m}$ which are locally trivial at all places coprime to n. We give a brief account of the construction to the extent to which it will be necessary for the rest of the paper and refer the reader to [10] and [13] for the full details. Our notation follows the notation in [10].

Definition 1. Let E, K, p be as above, and let m be a positive integer. A prime number ℓ is called a *Kolyvagin prime* for (E, K, p, m) if the following three conditions are satisfied

(1) ℓ does not divide $N \cdot D \cdot p$.
(2) ℓ is inert in K.
(3) $a_\ell \equiv \ell + 1 \equiv 0 \mod p^m$.

For each such ℓ, let λ denote the unique prime of K above ℓ and let $G_\ell = G_{K_\ell/K_1}$. Then $G_\ell \simeq (\mathcal{O}_K/\ell\mathcal{O}_K)^\times/(\mathbb{Z}/\ell\mathbb{Z})^\times \simeq \mathbb{F}_\lambda^\times/\mathbb{F}_\ell^\times$ is cyclic of order $\ell + 1$, so one can choose a generator $\sigma_\ell \in G_\ell$. Let $\mathrm{Tr}_\ell = \sum_{i=0}^{\ell} \sigma_\ell^i$ and let $D_\ell \in \mathbb{Z}[G_\ell]$ be chosen in such a way that

$$(\sigma_\ell - 1) \cdot D_\ell = 1 + \ell - \mathrm{Tr}_\ell \,.$$

For instance, one can choose $D_\ell = \displaystyle\sum_{i=1}^{\ell} i \cdot \sigma_\ell^i$.

Now suppose that n is a product of Kolyvagin primes for (E, K, p, m). Let $D_n = \prod_{\ell|n} D_\ell$, $\mathcal{G}_n = G_{K_n/K}$ and $G_n = G_{K_n/K_1}$. Suppose that $S \subset \mathcal{G}_n$ is a system of coset representatives for $\mathcal{G}_n/G_n$. One can show [10, Prop. 3.6] that the image of $D_n y_n$ in $E(K_n)/p^m E(K_n)$ is fixed by G_n. Thus, if we set

$$P_n = \sum_{\sigma \in S} \sigma(D_n y_n),$$

then the image of P_n in $E(K_n)/p^m E(K_n)$ will be fixed by $\mathcal{G}_n$. To define the classes, we consider the following commutative diagram

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & & & & & \mathrm{H}^1(K_n/K, E)_{p^m} & & \\
 & & & & & & \downarrow{\scriptstyle \mathrm{Inf}} & & \\
0 & \longrightarrow & E(K)/p^m E(K) & \xrightarrow{\delta} & \mathrm{H}^1(K, E_{p^m}) & \longrightarrow & \mathrm{H}^1(K, E)_{p^m} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \mathrm{Res}} & & \\
0 & \to & (E(K_n)/p^m E(K_n))^{\mathcal{G}_n} & \xrightarrow{\delta} & \mathrm{H}^1(K_n, E_{p^m})^{\mathcal{G}_n} & \longrightarrow & \mathrm{H}^1(K_n, E)_{p^m}^{\mathcal{G}_n} & &
\end{array}$$

According to [10], the restriction map $\phi : \mathrm{H}^1(K, E_{p^m}) \to \mathrm{H}^1(K_n, E_{p^m})^{\mathcal{G}_n}$ is an isomorphism, so we can define the cohomology class

$$c_{n,m} = \phi^{-1}(\delta(P_n)) \in \mathrm{H}^1(K, E_{p^m}).$$

By Lemma 4.1 in [17], $c_{n,m}$ is represented by the cocycle

$$\sigma \mapsto -\frac{(\sigma-1)P_n}{p^m} + \sigma\frac{P_n}{p^m} - \frac{P_n}{p^m}, \tag{1}$$

where $\frac{(\sigma-1)P_n}{p^m}$ is the unique p^m-division point of $(\sigma-1)P_n$ in $E(K_n)$.

Let $d_{n,m}$ be the image of $c_{n,m}$ in $\mathrm{H}^1(K, E)_{p^m}$.

4. An Algorithm for Deciding Local Triviality

One of the basic properties of the class $d_{n,m}$ is that it is locally trivial at all but the places lying over the prime divisors of n. The following proposition is proved in [10, Prop. 6.2].

Proposition 1. *(i) If v is a place of K such that $v \nmid n$ or if $v = \infty$ is the archimedean place then $\mathrm{res}_v(d_{n,m}) = 0$.*
(ii) If λ is a place of K above a prime divisor ℓ of n then $\mathrm{res}_\lambda(d_{n,m}) = 0$ if and only if $P_{n/\ell} \in p^m E(K_{n/\ell,\lambda'})$ for one (and hence all) places λ' of $K_{n/\ell}$ dividing λ. Here, $K_{n/\ell,\lambda'}$ denotes the completion of $K_{n/\ell}$ at λ'.

The following standard lemma will be used to provide an algorithm for deciding whether a point is divisible.

Lemma 2. *Let F be any number field and let F_v be the completion of F at a non-archimedean place v. Let E be an elliptic curve over F_v with good reduction. Let m be an integer which is relatively prime to the characteristic of the residue field k_v. We have*

1. *$E(F_v)/mE(F_v) \cong \tilde{E}(k_v)/m\tilde{E}(k_v)$, and*
2. *$E_m(F_v) \cong \tilde{E}_m(k_v)$.*

In particular, a point $Q \in E(F_v)$ is m-divisible if and only if its reduction $\tilde{Q} \in \tilde{E}(k_v)$ is m-divisible.

Proof. Consider the following commutative diagram

$$\begin{array}{ccccccccc}
 & & K_1 & & E_m(F_v) & & \tilde{E}_m(k_v) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & E_1(F_v) & \longrightarrow & E(F_v) & \longrightarrow & \tilde{E}(k_v) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle [m]} & & \downarrow{\scriptstyle [m]} & & \downarrow{\scriptstyle [m]} & & \\
0 & \to & E_1(F_v) & \longrightarrow & E(F_v) & \longrightarrow & \tilde{E}(k_v) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & C_1 & & E(F_v)/mE(F_v) & & \tilde{E}(k_v)/m\tilde{E}(k_v) & &
\end{array}$$

where K_1 and C_1 are the kernel and cokernel of the first map, and $E_1(F_v)$ is the kernel of reduction. We use the snake lemma to get an exact sequence

$$C_1 \to E(F_v)/mE(F_v) \to \tilde{E}(k_v)/m\tilde{E}(k_v) \to 0$$

Since m is prime to the characteristic of k_v the multiplication-by-m map on $E_1(F_v)$ is an isomorphism, i.e. $K_1 = C_1 = 0$ ([22, VII, Prop.2.2, IV,§3]). Thus, we get isomorphisms $E(F_v)/mE(F_v) \simeq \tilde{E}(k_v)/m\tilde{E}(k_v)$ and $E_m(F_v) \simeq \tilde{E}_m(k_v)$. This proves the lemma. □

Remark. Applying this to the Kolyvagin setup, by Proposition 1, the class $d_{n,m}$ is locally trivial at λ if and only if $P_{n/\ell}$ is in $p^m E(K_{n/\ell,\lambda'})$. According to the above lemma, this is equivalent to $\tilde{P}_{n/\ell} \in p^m\tilde{E}(k_\lambda)$, since K_λ and $K_{n/\ell,\lambda'}$ have the same residue field. The last condition can be tested by computing the reduction of $P_{n/\ell}$ modulo λ'.

5. The Cassels Pairing on the Shafarevich-Tate Group

In this section we consider an elliptic curve E over an arbitrary number field K. We will describe a skew-symmetric pairing on the Shafarevich-Tate group $Ш(K, E)$, the Cassels pairing, which will be non-degenerate in the case when $Ш(K, E)$ is finite. The description follows [17, §2]. Let $d \in Ш(K, E)_M$ and $d' \in Ш(K, E)_{M'}$ be two elements of the Shafarevich-Tate group. Choose a lift $c' \in \mathrm{Sel}^{(M')}(K, E)$ of d' and for each valuation $v \in M_K$ choose $y_v \in E(K_v)$, such that $c'_v = \delta(y_v)$ ($\delta : E(K_v) \to \mathrm{H}^1(K_v, E_{M'})$ is the connecting homomorphism). Also, assume that there exists a class $d_1 \in \mathrm{H}^1(K, E)_{MM'}$, such that $M'd_1 = d$. Since d is locally trivial, $\mathrm{res}_v(d_1) \in \mathrm{H}^1(K_v, E)_{M'}$. We define the Cassels pairing $\langle\ ,\ \rangle_C$ between d and d' as

$$\langle d, d'\rangle_C := \sum_{v\in M_K} \langle y_v, \mathrm{res}_v(d_1)\rangle_{K_v},$$

where $\langle\ ,\rangle_{K_v} : E(K_v) \times \mathrm{H}^1(K_v, E) \to \mathbb{Q}/\mathbb{Z}$ is the Tate local pairing. For more detail on Tate local duality and the pairing see [18].

5.1. **Computing the Cassels Pairing on Kolyvagin Classes.** The next proposition which is proved in [17, Prop.4.7] specializes the above formula to locally trivial Kolyvagin cohomology classes.

Proposition 3. *Let E, K, p be as in Section 3.3. Let m and m' be positive integers and let n and n' be square-free products of Kolyvagin primes for $(E, K, p, m + m')$ and (E, K, p, m'), respectively. Suppose that the classes $d_{n,m} \in \mathrm{H}^1(K, E)_{p^m}$ and $d_{n',m'} \in \mathrm{H}^1(K, E)_{p^{m'}}$ are everywhere locally trivial (i.e. they lie in $Ш(K, E)$). Then the Cassels pairing is*

$$\langle d_{n,m}, d_{n',m'}\rangle_C = \sum_{\ell|n,(\ell,n')=1} \langle P_{n'}, d_{n,m+m'}\rangle_{K_\lambda}.$$

For simplicity of notation, we write the pairing as $\langle\ ,\ \rangle_{K_\lambda}$ rather than introducing $K_{n',\lambda'}$ as in Proposition 1. We use the definition of the pairing given in the previous section with $M = p^m$ and $M' = p^{m'}$. It follows from [17, Lemma 4.6] that $p^{m'}d_{n,m+m'} = d_{n,m}$, so the element $d_{n,m+m'}$ can be used as d_1 in the definition of the pairing given in the previous section.

In the next section, we will explain how to reduce the Tate local pairing $\langle , \rangle_{K_\lambda}$ to an efficiently computable pairing over finite fields.

6. Relating the Tate Local Pairing to a Pairing over Finite Fields

The main reference for this section is [7]. Throughout this section, let K be any number field, and let K_v be the completion of K at a non-archimedean place v of K. Let k_v be the residue field of K_v, and let E be an elliptic curve over K_v with good reduction. Let m be an integer which is prime to the characteristic of k_v.

Consider the Tate local pairing

$$\langle , \rangle_{K_v} : E(K_v)/mE(K_v) \times \mathrm{H}^1(K_v, E)_m \to \mathbb{Q}/\mathbb{Z}$$

Since the Cassels pairing can be expressed as a sum of local Tate pairings by Proposition 3, we would like to compute the Tate local pairing to determine if two Kolyvagin classes pair non-trivially under the Cassels pairing. Unfortunately, the Tate local pairing in this form is quite hard to compute. We will now show how to relate the pairing $\langle , \rangle_{K_v}$ to a pairing over finite fields, and we will then use this relationship to detect whether certain Kolyvagin classes pair to a non-trivial element.

6.1. **Description of $\mathrm{H}^1(K_v, E)_m$.** We will describe the group $\mathrm{H}^1(K_v, E)_m$ in a way which is more convenient for computations. Fix an algebraic closure $\overline{K}_v$ of K_v. Let π be a uniformizer of K_v and let ζ_m be a primitive m-th root of unity in $\overline{K}_v$. Consider the extensions $L_m = K_v(\zeta_m, \pi^{1/m})$ and $K_v(\zeta_m)$ of K, where $\pi^{1/m} \in \overline{K}_v$. The Galois group $G_{K_v(\zeta_m)/K_v}$ acts on $G_{L_m/K_v(\zeta_m)}$ by conjugation. Let $K_v(E_m)$ be the field obtained by adjoining the coordinates of all m-torsion points of E defined over $\overline{K}_v$. The extension $K_v(E_m)$ is unramified and therefore cyclic over K_v. Moreover, since the Weil pairing is Galois equivariant, it contains $K_v(\zeta_m)$. Therefore, $G_{K_v(E_m)/K_v}$ acts on $G_{L_m/K_v(\zeta_m)}$ through its quotient $G_{K_v(\zeta_m)/K_v}$. The following proposition (see also [7, Prop.3.15]) describes the group $\mathrm{H}^1(K_v, E)_m$ as the cohomology of a finite group acting on a finite module.

Proposition 4. *We have an isomorphism*

$$\mathrm{H}^1(K_v, E)_m \simeq \mathrm{Hom}_{G_{K_v(E_m)/K_v}}(G_{L_m/K_v(\zeta_m)}, E_m).$$

In particular, if $\mu_m \subset K_v$ then the isomorphism becomes

$$\mathrm{H}^1(K_v, E)_m \simeq \mathrm{Hom}_{G_{K_v(E_m)/K_v}}(G_{L_m/K_v}, E_m).$$

Proof. Let $G_{K_v} = G_{\overline{K}_v/K_v}$, let $I_{K_v} \subset G_{K_v}$ be the inertia group of G_{K_v}, and let $G_{k_v} = G_{\overline{k}_v/k_v}$. Consider the exact sequence

$$0 \to E_1(\overline{K}_v) \to E(\overline{K}_v) \to \tilde{E}(\overline{k}_v) \to 0,$$

where $E_1(\overline{K}_v)$ is the kernel of reduction. Consider the corresponding long exact sequence of Galois cohomology, where G_{K_v} acts on $\tilde{E}(\overline{k}_v)$ through its quotient $G_{K_v}/I_{K_v} \simeq G_{k_v}$.

$$\mathrm{H}^1(K_v, E_1) \to \mathrm{H}^1(K_v, E) \to \mathrm{H}^1(K_v, \tilde{E}) \to \mathrm{H}^2(K_v, E_1) \to \dots.$$

Since m is coprime to the characteristic of $\overline{k}_v$ it follows from [22, Prop. 3.1(a)] that the group $E_1(L)$ is m-primary for any finite extension L/K_v, $L \subset \overline{K}_v$, so E_1 is m-primary. It follows from the Kummer sequence for E_1 that $\mathrm{H}^1(K_v, E_1)[m] = \mathrm{H}^2(K_v, E_1)[m] = 0$. Therefore, the map

$$\mathrm{H}^1(K_v, E)[m] \to \mathrm{H}^1(K_v, \tilde{E})[m]$$

is an isomorphism.

Next, the inflation-restriction sequence for $I_{K_v} \subset G_{K_v}$ gives us

$$0 \to \mathrm{H}^1(k_v, \tilde{E}) \to \mathrm{H}^1(K_v, \tilde{E}) \to \mathrm{H}^1(I_{K_v}, \tilde{E})^{G_{K_v}/I_{K_v}} \to \mathrm{H}^2(k_v, \tilde{E})$$

By [14], $\mathrm{H}^1(k_v, \tilde{E}) = 0$, and by [20, p. 189] we also have $\mathrm{H}^2(k_v, \tilde{E}) = 0$. Since I_{K_v} acts trivially on $\tilde{E}$, we obtain an isomorphism

$$\mathrm{H}^1(K_v, \tilde{E}) \cong \mathrm{Hom}(I_{K_v}, \tilde{E})^{G_{K_v}/I_{K_v}}.$$

Finally,

$$\mathrm{Hom}(I_{K_v}, \tilde{E})^{G_{K_v}/I_{K_v}}[m] \cong \mathrm{Hom}(I_{K_v}, \tilde{E}_m)^{G_{K_v}/I_{K_v}} \cong$$
$$\mathrm{Hom}_{G_{K_v(E_m)/K_v}}(G_{L_m/K_v(\zeta_m)}, E_m),$$

where the last isomorphism comes from the fact that a homomorphism $I_{K_v} \to E_m$ factors through the tame inertia group since m is coprime to the residue characteristic. This finishes the proof. □

Let $H := G_{K_v(E_m)/K_v}$. By Proposition 4, we obtain a modified pairing

$$\langle\,,\rangle_{K_v} : E(K_v)/mE(K_v) \times \mathrm{Hom}_H(G_{L_m/K_v(\zeta_m)}, E_m(K_v)) \to \mathrm{Br}(K_v)[m],$$

which is induced by the Tate pairing. Here we use the fact that $\mathrm{Br}(K_v) \cong \mathbb{Q}/\mathbb{Z}$, and that the image of the Tate local pairing (for m) lies in the m-torsion part of $\mathbb{Q}/\mathbb{Z}$.

6.2. **Reducing to the Finite Field Case.** In this section we assume that in addition $\mu_m \subset K_v$, or equivalently that $m \mid \#k_v^\times$. We have that $\mathrm{Br}(K_v)[m]$ is cyclic of order m.

In this situation, we have a description of the Tate pairing (up to sign) that is due to Lichtenbaum (see [15], see also [8, 5.3.4]):

Theorem 5 (Lichtenbaum)**.** *Let σ be a generator of G_{L_m/K_v} and let $P_1 \in E(K_v)$ and $P_2 \in E_m(K_v)$. Let $D_1 \sim (P_1) - (O)$ be such that D_1 is coprime to $D_2 = (P_2) - (O)$. Let $\varrho : G_{L_m/K_v} \to E_m(K_v)$ be the homomorphism sending σ to P_2 and let f_2 be a function on E whose divisor is equivalent to mD_2. Then*

$$\langle P_1 + mE(K_v), \varrho\rangle_{K_v} = f_2(D_1),$$

where $f_2(D_1)$ is considered as an element of $K_v^\times/N_{L_m/K_v}(L_m^\times)$. We have $K_v^\times/N_{L_m/K_v}(L_m^\times) \cong k_v^\times/(k_v^\times)^m$.

Since G_{L_m/K_v} is cyclic, an element $\psi \in \mathrm{Hom}(G_{L_m/K_v}, E_m(K_v))$ is uniquely determined by the image of its generator $\psi(\sigma)$ in $E_m(K_v)$.
So $\mathrm{Hom}(G_{L_m/K_v}, E_m(K_v))$ is non-canonically (depending on the choice of π and the generator σ) isomorphic to $E_m(K_v)$.

Let $\tilde{E}/k_v$ be the reduction of E/K_v. We have $E_m(K_v) \simeq \tilde{E}_m(k_v)$ by Lemma 2. Together with the above argument this implies that $\mathrm{Hom}(G_{L_m/K_v}, E_m(K_v))$ is isomorphic to $\tilde{E}_m(k_v)$. Also, since $\mathrm{Br}(K_v)[m]$ is cyclic of order m, it is isomorphic to $k_v^\times/(k_v^\times)^m$.

By Lemma 2 we also have $E(K_v)/mE(K_v) \simeq \tilde{E}(k_v)/m\tilde{E}(k_v)$. Thus, as a corollary of Lichtenbaum's theorem, we obtain the well known cryptographic Tate pairing which can be efficiently computed.

Corollary 6. *There is a non-degenerate pairing*

$$\varphi_m : \tilde{E}(k_v)/m\tilde{E}(k_v) \times \tilde{E}_m(k_v) \to k_v^\times/(k_v^\times)^m,$$

which is given by the following rule: Let $P_1 \in \tilde{E}(k_v)$ and $P_2 \in \tilde{E}_m(k_v)$ be two points on the reduced elliptic curve. Let D_i be a divisor equivalent to $(P_i)-(O)$ $(i=1,2)$, such that D_1 and D_2 are coprime. Let f_2 be a function on $\tilde{E}$ with divisor mD_2. Then

$$\varphi_m(P_1 + m\tilde{E}(k_v), P_2) = f_2(D_1),$$

where $f_2(D_1)$ is considered as an element of $k_v^\times/(k_v^\times)^m$.

Remark. Let $P_1 \in E(K_v)$ and $P_2 \in E_m(K_v)$ be as in Theorem 1, and let ϱ be the homomorphism sending σ to P_2. Let $\tilde{P}_1$, $\tilde{P}_2$ be the reductions of P_1 and P_2, respectively. By Lemma 2, $E(K_v)/mE(K_v) \cong \tilde{E}(k_v)/m\tilde{E}(k_v)$, and $E_m(K_v) \cong \tilde{E}_m(k_v)$. This implies that $\varphi_m(\tilde{P}_1, \tilde{P}_2)$ is nonzero if and only if $\langle P_1 + mE(K_v), \varrho\rangle_{K_v}$ is nonzero.

Hence we can conclude that the Tate local pairing

$$\langle\,,\rangle_{K_v} : E(K_v)/mE(K_v) \times \mathrm{H}^1(K_v, E)_m \to \mathbb{Q}/\mathbb{Z}$$

is nonzero if the cryptographic Tate pairing $\varphi_m(\tilde{P}_1, \tilde{P}_2)$ for the corresponding points $\tilde{P}_1, \tilde{P}_2$ is nonzero.

For efficient computation of the cryptographic Tate pairing, see [1] and [6].

7. Application to Kolyvagin Cohomology Classes

In this section we apply the results explained in the previous section to certain Kolyvagin cohomology classes. Let E, K, p and m be as in Section 3.3. Suppose that ℓ is a Kolyvagin prime for $(E, K, p, m+1)$, such that the class $d_{\ell,m}$ is an element of the Shafarevich-Tate group $Ш(K, E)$, i.e. $d_{\ell,m}$ is locally trivial at the unique place $\lambda \mid \ell$.

We provide a method for testing whether the class $d_{\ell,m}$ is a non-trivial element of $Ш(K,E)$ by pairing the class $d_{\ell,m}$ with another everywhere locally trivial Kolyvagin cohomology class $d_{n',1}$ (which we call a *test class*) with $\ell \nmid n'$. If $\langle d_{\ell,m}, d_{n',1}\rangle_C \neq 0$, then both the class $d_{\ell,m}$ and the test class $d_{n',1}$ are nonzero elements of $Ш(K,E)$. However, if $\langle d_{\ell,m}, d_{n',1}\rangle_C = 0$, then we cannot conclude anything. So in practice, we will have to compute $\langle d_{\ell,m}, d_{n',1}\rangle_C$ for multiple test classes. Our algorithm takes as input the data (E, K, p, m, ℓ, n') for which both $d_{\ell,m}$ and $d_{n',1}$ are (possibly trivial) elements of $Ш(K,E)$. The output is TRUE or FALSE depending on whether the pairing is nonzero or zero, respectively.

We test whether the Cassels pairing is non-zero via the Tate pairing over finite fields by using Proposition 3 and the reduction in Section 6. First, we use the methods in Section 8 to compute the coordinates of the Heegner points y_ℓ, $y_{n'}$ and their Galois conjugates. Once we do this, we can compute the points P_ℓ and $P_{n'}$ in $E(K)$ defined in Section 3. By Proposition 3,

$$\langle d_{\ell,m}, d_{n',1}\rangle_C = \langle P_{n'}, \mathrm{res}_\lambda(d_{\ell,m+1})\rangle_{K_\lambda}.$$

The field K_λ contains the p^{m+1}-th roots of unity since the Kolyvagin assumptions imply that $\#\mathbb{F}_{\ell^2}^\times = \ell^2 - 1 \equiv 0 \mod p^{m+1}$. Hence we can apply Proposition 4 with the local field K_λ and p^{m+1}. Let $M := p^{m+1}$. We obtain

$$\mathrm{H}^1(K_\lambda, E)_M \cong \mathrm{Hom}_{G_{K_\lambda(E_M)/K_\lambda}}(G_{L_M/K_\lambda}, E_M).$$

By the previous section, $\langle P_{n'}, \mathrm{res}_\lambda(d_{\ell,m+1})\rangle_{K_\lambda}$ is nonzero if $\varphi_{p^{m+1}}(\tilde{P}_{n'}, Q)$ is nonzero, where

$$\varphi_{p^{m+1}} : \tilde{E}(\mathbb{F}_{\ell^2})/p^{m+1}\tilde{E}(\mathbb{F}_{\ell^2}) \times \tilde{E}_{p^{m+1}}(\mathbb{F}_{\ell^2}) \to \mathbb{F}_{\ell^2}^\times/(\mathbb{F}_{\ell^2}^\times)^{p^{m+1}}$$

is the cryptographic Tate pairing, $\tilde{P}_{n'}$ is the image of $P_{n'}$ in $\tilde{E}(\mathbb{F}_{\ell^2})$, and Q is the image of $\mathrm{res}_\lambda(d_{\ell,m+1})$ in $\tilde{E}_{p^{m+1}}(\mathbb{F}_{\ell^2})$.

Since we have an explicit description for a 1-cocycle that represents the class $c_{\ell,m+1}$ associated to the Heegner point y_ℓ (see Equation (1) in Section 3.3), we can compute its image in $\mathrm{Hom}(G_{L_M/K_\lambda}, \tilde{E}_M(F_{\ell^2}))$ and therefore the corresponding point on the reduction $\tilde{E}_M(\mathbb{F}_{\ell^2})$. Thus, we can compute the pairing φ_M.

8. Computational Aspects

We describe computational aspects of the above algorithm and discuss some of the implementation issues.

8.1. **Choice of E, p, D, ℓ, n'.** Choose a non-CM elliptic curve E over $\mathbb{Q}$ of conductor N and analytic rank 1 from Cremona's tables [4] with non-trivial conjectural p-part of $Ш(K,E)$ for some odd prime p such that $\rho_{E,p}$ is surjective, and some quadratic imaginary field K with a Heegner discriminant D coprime to p. In our case, *conjectural order of* $Ш(K,E)$ means the order predicted by a combination of the Birch and Swinnerton-Dyer conjecture and the Gross-Zagier formula for $E/\mathbb{Q}$ and the twist $E^D/\mathbb{Q}$. The precise

conjecture (as stated in [17]) says that if the Heegner point $y_K \in E(K)$ has infinite order then

$$\#Ш(K,E) = \left(\frac{[E(K)/E(K)_{\mathrm{tors}} : \mathbb{Z}y_K]}{c \cdot \prod_{q|N} c_q} \right),$$

where c_q is the Tamagawa number for E at the prime q and c is a constant which depends on the modular parameterization (the Manin constant). The computation of the conjectural order of $Ш(K,E)$ has been implemented in SAGE and uses the Heegner point algorithm of Watkins (see [25]). We use the methods of Section 3.2 to test the surjectivity of the Galois representation $\rho_{E,p}$. For example, we check that the curve $E : y^2 + y = x^3 + x^2$ (curve 43A1 in [4]) has non-trivial 7-torsion in $Ш(K,E)$ for $K = \mathbb{Q}(\sqrt{-163})$ and the representation $\rho_{E,7}$ is surjective.

Once E, p and D are chosen, pick Kolyvagin primes ℓ for $(E,p,D,1)$ and n' for $(E,p,D,2)$.

8.2. **Computation of Heegner points P_n over ring class fields.** To the best of our knowledge, there is no existing package which implements the computation of Heegner points over ring class fields. We have already managed to do several computations and we are currently implementing such a package in MAGMA and SAGE. This section explains some of the difficulties encountered during the implementation.

We compute the Heegner point $P_\ell = \sum_{\sigma \in S} \sigma(D_\ell y_\ell)$ over the ring class field K_ℓ by computing the minimal polynomial of its x-coordinate. The last step is achieved by running through all of the $G_{K_\ell/K} = \mathrm{Pic}(\mathcal{O}_\ell)$-conjugates, where $\mathcal{O}_\ell$ is the order of conductor ℓ in K. Since ℓ is an inert prime in $K = \mathbb{Q}(\sqrt{D})$, the degree of the ring class field over K is $(\ell+1)h_K$, where h_K is the class number of K. We generate ideal class representatives for $\mathrm{Pic}(\mathcal{O}_\ell)$ by using Sebastian Pauli's package.

To compute P_ℓ and its $G_{K_\ell/K}$-conjugates we use the reciprocity law. If $\mathfrak{c}$ represents a class in $\mathrm{Pic}(\mathcal{O}_\ell)$, then the ideal class $[\mathfrak{c}]$ acts on the Heegner point $[\mathbb{C}/I \to \mathbb{C}/J]$ by mapping it to the point $[\mathbb{C}/\mathfrak{c}^{-1}I \to \mathbb{C}/\mathfrak{c}^{-1}J]$. Once we compute τ in the upper half plane corresponding to each conjugate, we need to evaluate $\varphi(\tau)$ to sufficient accuracy, where $\varphi(\tau) = \sum_{n \geq 1} \frac{a_n}{n} q^n$, $q = e^{2\pi i \tau}$, and a_n is the n-th Fourier coefficient of the modular form corresponding to the elliptic curve E.

Evaluating φ to sufficient accuracy turns out to be computationally expensive. First of all, the number of digits of accuracy required is significant and can be estimated as in [3] and [5] in terms of the height of the Heegner point. Cohen and Elkies address the computation of Heegner points with coefficients in $\mathbb{Q}$, and use three tools which hold over $\mathbb{Q}$: (1) known bounds on the difference between the naïve and canonical heights of the Heegner point [3, Thm.8.1.18], (2) the Gross-Zagier formula for the canonical height of the Heegner point in terms of the derivative of the L-series [11], and (3)

the conjectural BSD formula relating the derivative of the L-series to the order of Ш and the regulator (see [3, Alg.8.6.11, Step 1]). In our setting, the Heegner points are defined over the ring class field and we make rough estimates of the accuracy required using a conjectural generalization of the Gross-Zagier formula [19, Statement 2.6].

Secondly, the computation of the Heegner points requires not only large amounts of precision to evaluate and recognize, but also many terms from the Fourier expansion of the modular form. Cohen gives an estimate for the number of terms needed for computing Heegner points over $\mathbb{Q}$ in [3, Alg.8.6.11, Step 4] in terms of the binary quadratic forms representing the ideal classes. Even using the estimate from Cohen, for an example of conductor 681 with $D = -8$ and $\ell = 23$ we need $5,000$ digits of precision for each of the 24 conjugates to be computed, each using more than $20,000$ terms from the Fourier expansion.

Finally, τ can be very close to the real axis. This means that the computation of $\varphi(\tau)$ would require a huge number of Fourier coefficients, thus making the computation impractical. One way to move τ away from the real axis is by replacing it with another complex number in the $\Gamma_0(N)$-orbit. But in practice we only changed the imaginary part of τ from $\sim 10^{-60}$ to 10^{-50} in one example unless we searched extensively for a good transformation. If a Heegner point is very close to a cusp point c for $X_0(N)$, then it cannot be moved away from the real axis by an element of $\Gamma_0(N)$. To fix this problem, one could use a suitable element of the Atkin-Lehner group to move c to the cusp $i\infty$ and notice that the Heegner point would change by multiplication by the Atkin-Lehner sign modulo a rational torsion point on E. This trick was suggested to us by Elkies (see also [5]), but has not been implemented yet in our context.

The last few steps of the algorithm involve applying the Weierstrass $\wp$-function to the point $\varphi(\tau)$ on the complex uniformization $\mathbb{C}/\Lambda$ of E to obtain the x-coordinate of the Heegner point, forming the minimal polynomial of the x-coordinate over the field K, and using the continued fraction algorithm to recognize the coefficients of this polynomial.

8.3. **Example: $D = -43$, $p = 3$, $\ell = 5$, $N = 53$.** Let E be the elliptic curve 53A1 from Cremona's tables [4] with Weierstrass equation $E : y^2 + xy + y = x^3 - x^2$. We check that $D = -43$ is a Heegner discriminant for this elliptic curve and that the Galois representation $\rho_{E,3}$ is surjective. Conjecturally, $Ш(K, E)[3] \cong \mathbb{Z}/3 \times \mathbb{Z}/3$ for $K = \mathbb{Q}(\sqrt{-43})$.

By computing the coefficients of the Fourier expansion, we determine that $\ell = 5$ is a Kolyvagin prime for $(E, -43, 3, 1)$ and $n' = 197$ is a Kolyvagin prime for $(E, -43, 3, 2)$.

Using 1,000 digits of accuracy and 20,000 Fourier coefficients, we computed the minimal polynomial of the x-coordinate of the point P_5:

$P(z) = z^6 + (204596155002839835401984608289005860072264655245368551738618603675573523095892612111012609264002895698166992570358969774928 6$

$$0873834653545400972396303344122757394525081252659 2z^5 + 637250300427671178$$
$$9875656310657529082322095847187680088749381089676444350988958223731882804$$
$$5552577564770066572457434562330022804318247107119741270713336319525261463$$
$$13519104000z^4 + 208054456555015041349655034718856385886923586973910363342$$
$$3684717542932250768432410695234707758519131577122838048680410761259824416$$
$$1610330719290557912354960581970244140798574592 0z^3 + 1240735234271091429703$$
$$1210838098214193316953691457606684929211592451654613884349141104807095763$$
$$0305293154847447583386922959063835433465614902657069991669239746847250304$$
$$861143040z^2 + 406933598347113953183914995631519672347052365235631332364$$
$$8476969994013664804373975729701576229631819378092133583768003093886880559$$
$$0794139456756145472243795226370074363703787 52z + 3520525189854711965475079$$
$$4962147826096710283481706312962021089089720312642151806941533385009243908$$
$$8887379732999121911370 99 72156615957369176680214840841208815378567446236$$
$$9991078 4)/2^{24} * 601^4 * 1929899^4 * 18658515338321250932264264799709^4.$$

Unfortunately, P_{197} and its conjugates have not been computed yet and will require further implementation tricks as discussed above to finish the computation.

References

[1] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairing-based cryptosystems. In M. Yung, editor, *Advances in Cryptology – Crypto 2002*, pp. 354–368. LNCS **2442**, Springer-Verlag, 2002.

[2] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over **Q**: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.

[3] H. Cohen. *Diophantine Equations, p-adic Numbers, and L-functions.* Springer. `http://math.arizona.edu/ swc/notes/files/06CohenExtract.pdf`

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

[5] N. Elkies. Heegner point computations. In: *Algorithmic number theory (Ithaca, NY, 1994)*, pp. 122–133. LNCS **877**, Springer-Verlag, 1994.

[6] K. Eisenträger, K. Lauter, and P.L. Montgomery. Improved Weil and Tate pairings for elliptic and hyperelliptic curves. In Duncan Buell, editor, *ANTS-VI proceedings*, pp. 169–183. LNCS **3076**, Springer-Verlag, 2004.

[7] G. Frey. Applications of arithmetical geometry to cryptographic constructions. In *Finite fields and applications (Augsburg, 1999)*, pp. 128–161. Springer, Berlin, 2001.

[8] G. Frey, T. Lange. Mathematical background of public key cryptography. Arithmetic, geometry and coding theory (AGCT 2003), Sémin. Congr., vol. 11, Soc. Math. France, Paris, 2005, pp. 41–73.

[9] G. Grigorov, A. Jorza, S. Patrikis, W. Stein, C. Tarniţă-Patraşcu. Verification of the Birch and Swinnerton-Dyer conjecture for specific elliptic curves. Preprint.

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

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

[12] D. Jetchev, W. Stein. Visualizing elements of the Shafarevich-Tate group at higher level. Preprint.

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

[14] S. Lang. *Algebraic groups over finite fields.* Amer. J. Math., 78, 1956, pp. 555–563.

[15] S. Lichtenbaum. Duality theorems for curves over p-adic fields. *Inv. Math.*, 7:120–136, 1969.
[16] B. Mazur, K. Rubin. *private communication.*
[17] W. G. McCallum. Kolyvagin's work on Shafarevich-Tate groups. In *L-functions and arithmetic (Durham, 1989)*, pp. 295–316. Cambridge Univ. Press, Cambridge, 1991.
[18] J. S. Milne. *Arithmetic duality theorems.* Academic Press Inc., Boston, 1986.
[19] J. Nekovar, N. Schappacher. On the asymptotic behaviour of Heegner points. *Turkish J. of Math.* 23 (1999), No. 4, pp. 549–556.
[20] J-P. Serre. *Local fields*, volume 67 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1979.
[21] J-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15, 1972, 4, pp. 259–331.
[22] J. H. Silverman. *The arithmetic of elliptic curves.* Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.
[23] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves.* Springer-Verlag, New York, 1994.
[24] W. Stein, `SAGE`, `http://modular.fas.harvard.edu/SAGE`.
[25] M. Watkins. Some remarks on Heegner point computations. Preprint, 2004.

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109
E-mail address: `eisentra@umich.edu`

Department of Mathematics, University of California, Berkeley, CA 94720
E-mail address: `jetchev@math.berkeley.edu`

Microsoft Research, One Microsoft Way, Redmond, WA 98052
E-mail address: `klauter@microsoft.com`