Compositio Math. 144 (2008) 811–826
doi:10.1112/S0010437X08003497

Global divisibility of Heegner points and Tamagawa numbers

Dimitar Jetchev

In memory of my father and my grandfather

Abstract

We improve Kolyvagin's upper bound on the order of the p-primary part of the Shafarevich–Tate group of an elliptic curve of rank one over a quadratic imaginary field. In many cases, our bound is precisely that predicted by the Birch and Swinnerton-Dyer conjectural formula.

1. Introduction

Let $E_{/\mathbb{Q}}$ be an elliptic curve of conductor N and let $-D < 0$ be a fundamental discriminant such that all prime factors of N are split in the quadratic imaginary field $K = \mathbb{Q}(\sqrt{-D})$. We call such a $-D$ a *Heegner discriminant* for the elliptic curve $E_{/\mathbb{Q}}$.

Let $\mathcal{N}$ be an ideal in the ring of integers $\mathcal{O}_K$ of K of norm N, such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/N\mathbb{Z}$. The Heegner point $x_1 = [\mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{N}^{-1}]$ lies on the modular curve $X_0(N)$ and is defined over the Hilbert class field H/K by the theory of complex multiplication. Let $\varphi : X_0(N) \to E$ be a fixed modular parametrization that maps the cusp $i\infty$ of $X_0(N)$ to the origin of E (see [BCDT01] for the existence of such a parametrization). Then the Gross–Zagier formula (see [GZ86, ch. I, 6.5]) relates the height of the point $y_K = \mathrm{Tr}_{H/K}(\varphi(x_1))$ to the special value $L'(E_{/K}, 1)$ of the derivative of the L-function $L(E_{/K}, s)$. Gross and Zagier used this formula (see [GZ86, ch. V, 2.2]) to restate the Birch and Swinnerton-Dyer conjectural formula for $E_{/K}$ (whenever the analytic rank is 1) as follows.

Conjecture 1 (Birch and Swinnerton-Dyer formula). If the point y_K has infinite order, then $E(K)$ has rank 1 and the Shafarevich–Tate group $Ш(E/K)$ is finite of order

$$\#Ш(E/K) = \left(\frac{[E(K) : \mathbb{Z}y_K]}{c \cdot \prod_{q|N} c_q} \right)^2,$$

where c is the Manin constant (known to be a positive integer) and $c_q = [E(\mathbb{Q}_q) : E^0(\mathbb{Q}_q)]$ is the Tamagawa number at q.

Kolyvagin (see [Kol90, Theorem A], [Kol91a] and [Kol91b]) has shown the rank part of the above conjecture, the finiteness of $Ш(E/K)$ and a significant part of the conjectural formula. More precisely, consider the following hypothesis on a prime p.

Received 18 September 2007, accepted in final form 9 January 2008.
2000 Mathematics Subject Classification 11G05.
Keywords: elliptic curves, Heegner points, Selmer groups, Birch and Swinnerton-Dyer conjecture.

Hypothesis (*).[1] We have $p \nmid 2N$ and the extension $\mathbb{Q}(E[p])/\mathbb{Q}$ has Galois group isomorphic to $\mathrm{GL}_2(\mathbb{F}_p)$, that is, the mod p Galois representation $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(E[p])$ is surjective.

For such a prime p, Kolyvagin gives a precise formula for the order of the p-primary part of $Ш(E/K)$ by constructing explicit elements in the p-power Selmer group $\mathrm{Sel}_{p^\infty}(E/K)$ from Heegner points, namely

$$\#Ш(E/K)[p^\infty] = p^{2(m_0 - m_\infty)}, \tag{1}$$

where $m_0 = [E(K) : \mathbb{Z}y_K]$ and m_∞ is a nonnegative integer which is defined in terms of the global p-divisibility of the Heegner points used for the construction of the classes. We give a precise definition of m_∞ in § 4.1. The above formula provides strong evidence for Conjecture 1.

However, Kolyvagin's arguments give no indication of how to relate the correction factor m_∞ to the Manin constant and the Tamagawa numbers. As for the Manin constant, it is already known that $p \nmid c$ if $p \nmid N$ (see [AU96] and [ARS06] for an account on the known results about c). The combination of (1) and Conjecture 1 yields the following reformulation of the Birch and Swinnerton-Dyer conjectural formula for $E_{/K}$ in the case when the analytic rank is 1.

Conjecture 2 (BSD conjectural formula). If p satisfies Hypothesis (*), then

$$m_\infty = \mathrm{ord}_p\left(\prod_{q|N} c_q\right).$$

Our main result provides the following evidence for this conjecture.

Theorem 1.1. *Assume that the Heegner point y_K has infinite order in $E(K)$ and that p satisfies* Hypothesis (*). *If $m_{\max} = \max_{q|N} \mathrm{ord}_p(c_q)$, then $m_\infty \geqslant m_{\max}$.*

As a consequence, we obtain a new upper bound on the p-primary part of the Shafarevich–Tate group over K:

$$\#Ш(E/K)[p^\infty] \leqslant p^{2m_0 - 2m_{\max}}.$$

Here, $m_{\max} = \max_{q|N} \mathrm{ord}_p(c_q)$. If p divides at most one Tamagawa number, our upper bound coincides with the exact upper bound predicted by the Birch and Swinnerton-Dyer conjectural formula for $E_{/K}$.

Remark 1. Results of Schneider, Perrin-Riou and Kato from Iwasawa theory, together with the conjectured nonvanishing of the p-adic regulator, imply the exact upper bound on the p-primary part of the Shafarevich-Tate group for $E_{/\mathbb{Q}}$ predicted by the Birch and Swinnerton-Dyer conjecture [SW08, Theorem 8]. A remark of Colmez (see [Col03, Remark 0.13(ii)]) suggests that this last conjecture is at least as difficult as proving Leopoldt's conjecture. Our results in the analogous situation over K do not depend upon any conjecture.

We prove the theorem by refining Kolyvagin's original arguments. We also apply several techniques from the theory of Kolyvagin systems as developed by Mazur, Rubin and Howard (see [MR04] and [How04]). The paper is organized as follows. Section 2 contains some notation. Section 3 is about Selmer modules as introduced by Mazur and Rubin. We define various local conditions to be used in the proof, recall the notion of a Selmer structure and the associated Selmer modules, discuss the relevant global duality results on Galois cohomology, and introduce a new Selmer structure which will replace the standard Selmer structure obtained from the Kummer local conditions in Kolyvagin's arguments. In § 4 we review the basics of Heegner points over ring class fields, define the numbers m_0 and m_∞ which appear in Kolyvagin's formula for the order of $Ш(E/K)[p^\infty]$ and recall the construction of Kolyvagin's classes. The main contribution in this section is Proposition 4.1 where we

[1] Recently, Byungchul Cha (see [Cha05]) has been able to weaken Hypothesis (*).

https://doi.org/10.1112/S0010437X08003497 Published online by Cambridge University Press

obtain more refined local properties of the constructed classes than those implicitly used by Kolyvagin. The proof is based on certain reduction properties of the Heegner points at bad places. Finally, we prove our main theorem in § 5. The major new ingredients are the combinatorial arguments of §§ 5.2 and 5.3. The remaining part of the proof is a combination of the Čebotarev density theorem and the global duality results. We first prove the result in an easy case (Theorem 5.2) and then use some techniques of Kolyvagin to reduce the general case to the easy case in § 5.3.

2. Notation

Throughout the paper, $\overline{K}$ is a fixed algebraic closure of K, $\mathcal{O}_K$ is the ring of integers of K, $\mathcal{O}_c = \mathbb{Z}+c\mathcal{O}_K$ is the order of conductor c in $\mathcal{O}_K$ and $K[c]$ is the ring class field extension of K of conductor c. Recall that $K[c]$ is an abelian extension of K whose Galois group is isomorphic to $\mathrm{Pic}(\mathcal{O}_c)$ and that is Galois and dihedral over $\mathbb{Q}$. For instance, $K[1]$ is the Hilbert class field of K. For a number field L and a place w of L, let L_w be the completion of L at w, let $\mathcal{O}_w$ be the valuation ring of L_w, let $\overline{L}_w$ be a fixed algebraic closure of L_w and let L_w^{ur} be the maximal unramified extension of L_w. Whenever F is a field with a fixed algebraic closure $\overline{F}$, G_F will denote the Galois group $\mathrm{Gal}(\overline{F}/F)$. If M is a continuous G_F-module, $\mathrm{H}^1(F, M)$ will be the Galois cohomology group $\mathrm{H}^1(G_F, M)$.

Moreover, fix an embedding $\iota_v : \overline{K} \hookrightarrow \overline{K_v}$ for each place v of K (this corresponds to fixing a place of $\overline{K}$ above v for every place v of K). If M is a G_K-module, then ι_v determines an inclusion $G_{K_v} \hookrightarrow G_K$ and, hence, a localization map $\mathrm{loc}_v : \mathrm{H}^1(K, M) \to \mathrm{H}^1(K_v, M)$.

Following Kolyvagin, if $A \cong \mathbb{Z}/p^{x_1}\mathbb{Z} \oplus \mathbb{Z}/p^{x_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{x_n}\mathbb{Z}$ with $x_1 \geqslant x_2 \geqslant \cdots \geqslant x_n > 0$, we write

$$\mathbf{Inv}(A) = (x_1, x_2, \ldots, x_n).$$

For instance, $\mathbf{Inv}(O) = (\,)$. Also, for $a \in A$, $\mathrm{ord}'_p(a)$ stands for the integer n such that p^n is the order of a in A.

Finally, we need to introduce certain special primes needed for the constructions and the arguments of the paper.

Definition 2.1 (Kolyvagin prime). We call a rational prime ℓ a *Kolyvagin prime* relative to E, K and p if ℓ is inert in K and p divides both the ℓth coefficient a_ℓ of the modular form f associated to E and $\ell + 1$, that is, $p \mid (a_\ell, \ell + 1)$. Equivalently, the characteristic polynomial of Fr_ℓ is congruent to $T^2 - 1$ modulo p.

We denote the set of all Kolyvagin primes for E, K and p by Λ^1. Moreover, let Λ^1_m be the set of all $\ell \in \Lambda^1$, such that $p^m \mid (a_\ell, \ell + 1)$.

Finally, for each $\ell \in \Lambda^1$, we fix a generator σ_ℓ of the cyclic group $\mathrm{Gal}(K[\ell]/K[1])$.

3. Selmer modules

3.1 Local conditions

Fix a positive integer m. By a local condition at a finite place v we mean a subgroup of the cohomology group $\mathrm{H}^1(K_v, E[p^m])$.

3.1.1 *General finite place v of K.* We define several local conditions for a finite place v of K.

- *Unramified local condition:* this is defined as

$$\mathrm{H}^1_{\mathrm{ur}}(K_v, E[p^m]) := \ker\{\mathrm{H}^1(K_v, E[p^m]) \to \mathrm{H}^1(K_v^{\mathrm{ur}}, E[p^m])\}.$$

https://doi.org/10.1112/S0010437X08003497 Published online by Cambridge University Press

- *Kummer local condition:* we denote this by $\mathrm{H}^1_{\mathrm{Kum}}(K_v, E[p^m])$ and define it to be the image of the local Kummer map
$$\delta_v : E(K_v)/p^m E(K_v) \hookrightarrow \mathrm{H}^1(K_v, E[p^m]).$$
- *Connected Kummer local condition:* let $E^0(K_v)$ be the subgroup of $E(K_v)$ consisting of all points which specialize to the identity component of the Néron model of $E_{/K}$ at v. We define the connected Kummer local condition $\mathrm{H}^1_{\mathrm{Kum}^0}(K_v, E[p^m])$ to be the image of $E^0(K_v)$ under the map
$$E(K_v) \twoheadrightarrow E(K_v)/p^m E(K_v) \xrightarrow{\delta_v} \mathrm{H}^1(K_v, E[p^m]).$$

The following proposition (see [Cas65] for more details) compares the unramified and the Kummer local conditions.

Proposition 3.1. *Let v be a place of good reduction for E, such that $v \nmid p$. Then* $\mathrm{H}^1_{\mathrm{ur}}(K_v, E[p^m]) = \mathrm{H}^1_{\mathrm{Kum}}(K_v, E[p^m])$.

We also need to compare the Kummer condition with the connected Kummer condition.

Lemma 3.2. *Let $v \mid N$ be a place of K and let $m_v = \mathrm{ord}_p(c_v)$. Suppose that $m > m_v$. Then*
$$\frac{\mathrm{H}^1_{\mathrm{Kum}}(K_v, E[p^m])}{\mathrm{H}^1_{\mathrm{Kum}^0}(K_v, E[p^m])} \cong \mathbb{Z}/p^{m_v}\mathbb{Z}.$$

Proof. This follows immediately from [Sil92, Theorem 15.2] and the above definitions, using that p is odd. □

3.1.2 *A place over a Kolyvagin prime ℓ.* Let $m > 0$ be an integer. For a Kolyvagin prime $\ell \in \Lambda^1_m$ let λ be the unique prime of K lying above ℓ. Let $K[\ell]_\lambda$ be the completion of $K[\ell]$ at the place below the place corresponding to the fixed embedding $\iota_\lambda : \overline{K} \hookrightarrow \overline{K_\lambda}$.

- *Transverse local condition:* we define this as
$$\mathrm{H}^1_{\mathrm{tr}}(K_\lambda, E[p^m]) := \ker\{\mathrm{H}^1(K_\lambda, E[p^m]) \to \mathrm{H}^1(K[\ell]_\lambda, E[p^m])\}.$$

To give an alternative description of $\mathrm{H}^1_{\mathrm{tr}}(K_\lambda, E[p^m])$, we first explain that G_{K_λ} acts trivially on $E[p^m]$. Indeed, G_{K_λ} acts through its quotient $\mathrm{Gal}(K_\lambda^{\mathrm{ur}}/K_\lambda)$ which is topologically generated by Fr_λ. However, $\mathrm{Fr}_\lambda = \mathrm{Fr}_\ell^2$ and since $\ell \in \Lambda^1_m$, then the conjugacy class of Fr_ℓ acting on $E[p^m]$ is the same as the conjugacy class of complex conjugation, that is, Fr_λ acts trivially.

Hence,
$$\mathrm{H}^1(K_\lambda, E[p^m]) = \mathrm{Hom}(G_{K_\lambda}, E[p^m]) \cong \mathrm{Hom}(G^{\mathrm{ab}}_{K_\lambda}/p^m, E[p^m]). \tag{2}$$
By local class field theory,
$$G^{\mathrm{ab}}_{K_\lambda}/p^m \cong \mathrm{Gal}(K_\lambda^{\mathrm{ur}}/K_\lambda)/p^m \times \mathrm{Gal}(K[\ell]_\lambda/K_\lambda)/p^m. \tag{3}$$
By (2) and (3),
$$\mathrm{H}^1(K_\lambda, E[p^m]) = \mathrm{H}^1_{\mathrm{ur}}(K_\lambda, E[p^m]) \oplus \mathrm{H}^1_{\mathrm{tr}}(K_\lambda, E[p^m]).$$
Here,
$$\mathrm{H}^1_{\mathrm{ur}}(K_\lambda, E[p^m]) = \{f \in \mathrm{Hom}(G^{\mathrm{ab}}_{K_\lambda}/p^m, E[p^m]) : f(\mathrm{Gal}(K[\ell]_\lambda/K_\lambda)/p^m) = 0\}$$
and
$$\mathrm{H}^1_{\mathrm{tr}}(K_\lambda, E[p^m]) = \{f \in \mathrm{Hom}(G^{\mathrm{ab}}_{K_\lambda}/p^m, E[p^m]) : f(\mathrm{Gal}(K_\lambda^{\mathrm{ur}}/K_\lambda)/p^m) = 0\}.$$
A homomorphism in $\mathrm{H}^1_{\mathrm{ur}}(K_\lambda, E[p^m])$ is determined by the image of Fr_λ, whereas a homomorphism in $\mathrm{H}^1_{\mathrm{tr}}(K_\lambda, E[p^m])$ is determined by the image of the fixed generator σ_ℓ of the cyclic group

$\mathrm{Gal}(K[\ell]/K[1])$. Thus,

$$\mathrm{H}^1_{\mathrm{ur}}(K_\lambda, E[p^m]) \cong E[p^m] \quad \text{and} \quad \mathrm{H}^1_{\mathrm{tr}}(K_\lambda, E[p^m]) \cong E[p^m].$$

Here $\tau \in \mathrm{Gal}(K_\lambda/\mathbb{Q}_\ell)$ acts on $\mathrm{Hom}(G^{\mathrm{ab}}_{K_\lambda}, E[p^m])$ by sending f to f^τ, where $f^\tau(\sigma) = f(\tau^{-1}\sigma\tau)^\tau$ for $\sigma \in G^{\mathrm{ab}}_{K_\lambda}$. Then the first of the above isomorphisms is Galois equivariant and the second is anti-equivariant (since $K[\ell]/\mathbb{Q}$ is dihedral, so conjugation by τ sends σ to its inverse). Therefore,

$$\mathrm{H}^1_{\mathrm{ur}}(K_\lambda, E[p^m])^\pm \cong E[p^m]^\pm \quad \text{and} \quad \mathrm{H}^1_{\mathrm{tr}}(K_\lambda, E[p^m])^\pm \cong E[p^m]^\mp.$$

The module $E[p^m]$ splits into two eigenspaces of complex conjugation each of which is free of rank 1 over $\mathbb{Z}/p^m\mathbb{Z}$ and, thus, $\mathrm{H}^1_{\mathrm{ur}}(K_\lambda, E[p^m])^\pm$ and $\mathrm{H}^1_{\mathrm{tr}}(K_\lambda, E[p^m])^\pm$ are all free of rank 1 over $\mathbb{Z}/p^m\mathbb{Z}$.

Finally, one can use the explicit description of the $\pm$-eigenspaces to conclude that $\mathrm{H}^1_{\mathrm{tr}}(K_\lambda, E[p^m])$ is self-orthogonal with respect to the Tate local pairing.[2] Indeed, it suffices to show that $\mathrm{H}^1_{\mathrm{tr}}(K_\lambda, E[p^m])$ is isotropic (since it has the rank of a maximal isotropic subspace). Since $\mathrm{H}^1_{\mathrm{tr}}(K_\lambda, E[p^m])^\pm$ are both cyclic $\mathbb{Z}/p^m\mathbb{Z}$-modules, each of them is self-orthogonal, so it will be enough to show that $\mathrm{H}^1_{\mathrm{tr}}(K_\lambda, E[p^m])^+$ is orthogonal to $\mathrm{H}^1_{\mathrm{tr}}(K_\lambda, E[p^m])^-$. The last is an immediate consequence of the $\mathrm{Gal}(K_\lambda/\mathbb{Q}_\ell)$-equivariancy of the symplectic Tate local pairing (i.e. $\langle \tau x, \tau y\rangle_\lambda = \langle x, y\rangle_\lambda$). The same argument shows that $\mathrm{H}^1_{\mathrm{ur}}(K_\lambda, E[p^m])$ is self-orthogonal as well.

3.2 Selmer structures and Selmer modules

Selmer structures and Selmer modules are discussed in great generality by Mazur and Rubin (see [MR04, ch. 2]). Here, we need to consider Selmer structures only on the Galois modules $E[p^m]$ of p^m-torsion points on the elliptic curve E for various m.

3.2.1 *Selmer structures.* A *Selmer structure* $\mathcal{F}$ on $E[p^m]$ consists of a choice of a local condition $\mathrm{H}^1_{\mathcal{F}}(K_v, E[p^m]) \subseteq \mathrm{H}^1(K_v, E[p^m])$ for each place v of K, such that for all but finitely many v, $\mathrm{H}^1_{\mathcal{F}}(K_v, E[p^m]) = \mathrm{H}^1_{\mathrm{ur}}(K_v, E[p^m])$.

3.2.2 *Selmer modules.* Given a Selmer structure $\mathcal{F}$ on $E[p^m]$, one can define the corresponding *Selmer module* as

$$\mathrm{H}^1_{\mathcal{F}}(K, E[p^m]) := \mathrm{Ker}\left\{\mathrm{H}^1(K, E[p^m]) \to \bigoplus_v \mathrm{H}^1(K_v, E[p^m])/\,\mathrm{H}^1_{\mathcal{F}}(K_v, E[p^m])\right\},$$

where the sum is taken over all places v of K. The Selmer module $\mathrm{H}^1_{\mathcal{F}}(K, E[p^m])$ will be a stable $\mathrm{Gal}(K/\mathbb{Q})$-subspace of $\mathrm{H}^1(K, E[p^m])$ provided that $\bigoplus_{v|q} \mathrm{H}^1_{\mathcal{F}}(K_v, E[p^m])$ is a $\mathrm{Gal}(K/\mathbb{Q})$-stable subspace of $\bigoplus_{v|q} \mathrm{H}^1(K_v, E[p^m])$ for every rational prime q. This will always be the case in the rest of this paper.

3.2.3 *Dual Selmer structure.* This is the Selmer structure $\mathcal{F}^*$ on $E[p^m]$ whose local conditions are the orthogonal complements of the local conditions of $\mathcal{F}$ under the Tate local pairing

$$\langle\,,\rangle_v : \mathrm{H}^1(K_v, E[p^m]) \times \mathrm{H}^1(K_v, E[p^m]) \to \mathbb{Z}/p^m\mathbb{Z}.$$

Note that $\mathcal{F}^*$ is a well-defined Selmer structure because the unramified local condition $\mathrm{H}^1_{\mathrm{ur}}(K_v, E[p^m])$ is self-orthogonal for every place $v \nmid pN$ (see [Mil86, Theorem 1.2.6]).

3.2.4 *Comparing Selmer modules and their duals.* If $\mathcal{F}$ and $\mathcal{G}$ are two Selmer structures, we say that $\mathcal{F} \preceq \mathcal{G}$ if $\mathrm{H}^1_{\mathcal{F}}(K_v, E[p^m]) \subseteq \mathrm{H}^1_{\mathcal{G}}(K_v, E[p^m])$ for every place v of K. In addition, if $\mathcal{F} \preceq \mathcal{G}$,

[2] For a different proof using class field theory and Kummer theory, see [MR04, Proposition 1.3.2(ii)].

https://doi.org/10.1112/S0010437X08003497 Published online by Cambridge University Press

one obtains a perfect bilinear pairing

$$\frac{\mathrm{H}^1_{\mathcal{G}}(K_v, E[p^m])}{\mathrm{H}^1_{\mathcal{F}}(K_v, E[p^m])} \times \frac{\mathrm{H}^1_{\mathcal{F}_*}(K_v, E[p^m])}{\mathrm{H}^1_{\mathcal{G}_*}(K_v, E[p^m])} \to \mathbb{Q}/\mathbb{Z}$$

that is induced from the Tate local pairing.

Theorem 3.3. *Let $\mathcal{F} \preceq \mathcal{G}$ be two Selmer structures on $E[p^m]$ and consider the exact sequences*

$$0 \to \mathrm{H}^1_{\mathcal{F}}(K, E[p^m])^{\pm} \hookrightarrow \mathrm{H}^1_{\mathcal{G}}(K, E[p^m])^{\pm} \xrightarrow{(\mathrm{loc}_{\mathcal{F}}^{\mathcal{G}})^{\pm}} \left(\bigoplus_v \frac{\mathrm{H}^1_{\mathcal{G}}(K_v, E[p^m])}{\mathrm{H}^1_{\mathcal{F}}(K_v, E[p^m])} \right)^{\pm}$$

and

$$0 \to \mathrm{H}^1_{\mathcal{G}^*}(K, E[p^m])^{\pm} \hookrightarrow \mathrm{H}^1_{\mathcal{F}^*}(K, E[p^m])^{\pm} \xrightarrow{(\mathrm{loc}_{\mathcal{G}^*}^{\mathcal{F}^*})^{\pm}} \left(\bigoplus_v \frac{\mathrm{H}^1_{\mathcal{F}^*}(K_v, E[p^m])}{\mathrm{H}^1_{\mathcal{G}^*}(K_v, E[p^m])} \right)^{\pm},$$

where $(\mathrm{loc}_{\mathcal{F}}^{\mathcal{G}})^{\pm}$ and $(\mathrm{loc}_{\mathcal{G}^*}^{\mathcal{F}^*})^{\pm}$ are the natural restriction maps on the $\pm$-eigenspaces for complex conjugation and the sum is over all places v, for which $\mathrm{H}^1_{\mathcal{F}}(K_v, E[p^m]) \subsetneq \mathrm{H}^1_{\mathcal{G}}(K_v, E[p^m])$. The images of $(\mathrm{loc}_{\mathcal{F}}^{\mathcal{G}})^{\pm}$ and $(\mathrm{loc}_{\mathcal{G}^*}^{\mathcal{F}^*})^{\pm}$ are orthogonal complements with respect to the local pairings $\sum_v \langle\, , \rangle_v^{\pm}$ obtained from the Tate pairings on the $\pm$-parts of the local cohomology groups.

Proof. This follows easily from Poitou–Tate global duality theorem. Standard references are [Rub00, Theorem 1.7.3], [Mil86, Theorem I.4.10] and [Tat63, Theorem 3.1]. □

3.3 Kummer and connected Kummer Selmer structure

We need two special Selmer structures for the proof of Theorem 1.1.

3.3.1 *Kummer Selmer structure.* The first Selmer structure is the standard *Kummer Selmer structure* $\mathcal{F}$ on $E[p^m]$. It is defined by the local condition $\mathrm{H}^1_{\mathcal{F}}(K_v, E[p^m]) := \mathrm{H}^1_{\mathrm{Kum}}(K_v, E[p^m])$ for every v (it is well defined by Proposition 3.1). By using the compatibility of the Tate local duality with the Weil pairing, one shows that the structure $\mathcal{F}$ is self-dual, that is, the local conditions are self-orthogonal at each place with respect to the Tate local pairing $\langle\, , \rangle_v$.

3.3.2 *Connected Kummer Selmer structure.* This refers to a Selmer structure obtained by replacing the Kummer local condition at one pair of conjugate primes $v, \bar{v} \mid N$ with the corresponding connected local conditions. A similar structure was used in an argument of Mazur and Rubin (see [MR04, Propostion 6.2.6]). Later, we use Lemma 3.2 and Theorem 3.3 to compare the Selmer modules corresponding to a connected Kummer Selmer structure with the usual Selmer group (i.e. the Selmer module corresponding to the Kummer Selmer structure).

3.4 Lozenge diagrams

3.4.1 *Modified Selmer structures.* Let $\mathcal{F}$ be a Selmer structure on $E[p^m]$ and a, b, c be relatively prime integers, such that $abc \in \Lambda_m$. The *modified Selmer structure* $\mathcal{F}_b^a(c)$ is the structure whose local conditions are obtained from those of $\mathcal{F}$ by simply replacing them at the places $v \mid abc$ as follows:

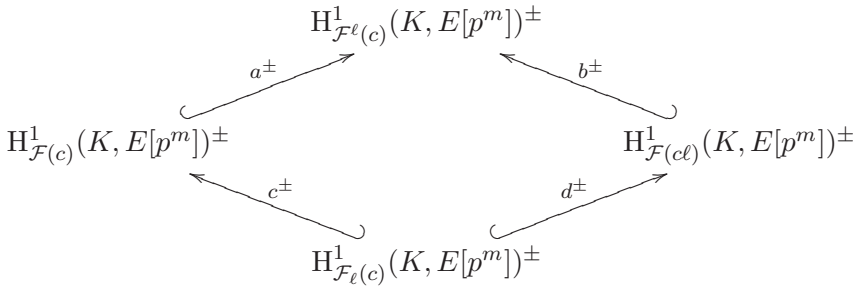
- if $v \mid c$, then $\mathrm{H}^1_{\mathcal{F}_b^a(c)}(K_v, E[p^m]) = \mathrm{H}^1_{\mathrm{tr}}(K_v, E[p^m])$;
- if $v \mid a$, then $\mathrm{H}^1_{\mathcal{F}_b^a(c)}(K_v, E[p^m]) = \mathrm{H}^1(K_v, E[p^m])$;
- if $v \mid b$, then $\mathrm{H}^1_{\mathcal{F}_b^a(c)}(K_v, E[p^m]) = 0$.

If a, b or c equals 1, we simply omit it from the notation (e.g. if $a = 1$, then we write $\mathcal{F}_b(c)$ instead of $\mathcal{F}_b^a(c)$).

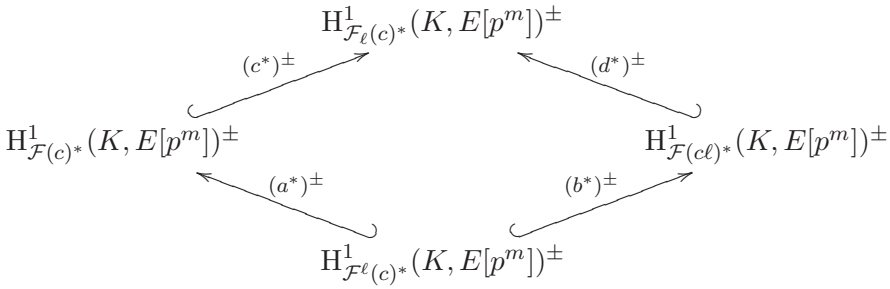
https://doi.org/10.1112/S0010437X08003497 Published online by Cambridge University Press

3.4.2 *Lozenge diagrams.* The following result is a refinement of [MR04, Lemma 4.1.6] and [How04, Lemma 5.1.8], and is useful whenever one needs to compare the structures of two Selmer modules for Selmer structures $\mathcal{F}(c)$ and $\mathcal{F}(c\ell)$.

LEMMA 3.4. *Let $\mathcal{F}$ be a Selmer structure on $E[p^m]$ (not necessarily self-dual). Consider the following diagrams*



and



where each inclusion is labelled with the lengths of the corresponding cyclic cokernels. Then the lengths satisfy:

(i) $0 \leqslant a^\pm, b^\pm, c^\pm, d^\pm, (a^*)^\pm, (b^*)^\pm, (c^*)^\pm, (d^*)^\pm \leqslant m$;

(ii) $a^\pm + c^\pm = b^\pm + d^\pm$ *and* $(a^*)^\pm + (c^*)^\pm = (b^*)^\pm + (d^*)^\pm$;

(iii) $a^\pm + (a^*)^\pm = b^\pm + (b^*)^\pm = c^\pm + (c^*)^\pm = d^\pm + (d^*)^\pm = m$;

(iv) $a^\pm \geqslant d^\pm$, $b^\pm \geqslant c^\pm$, $(c^*)^\pm \geqslant (b^*)^\pm$ *and* $(d^*)^\pm \geqslant (a^*)^\pm$.

Proof. Statement (i) follows from the definition of $\mathcal{F}_\ell(c)$, $\mathcal{F}^\ell(c)$, $\mathcal{F}^\ell(c)^*$ and $\mathcal{F}_\ell(c)^*$ and the fact that the $\pm$-parts $\mathrm{H}^1_{\mathrm{ur}}(K_\lambda, E[p^m])^\pm$ and $\mathrm{H}^1_{\mathrm{tr}}(K_\lambda, E[p^m])^\pm$ of the unramified and the transverse local conditions are free of rank one over $\mathbb{Z}/p^m\mathbb{Z}$. Statement (ii) follows immediately from the diagram. Statement (iii) is an immediate consequence of the split global duality Theorem 3.3. Finally, statement (iv) follows from the following equalities (which are consequences of the self-duality and the non-intersection of the transverse and the unramified local conditions)

$$\mathrm{H}^1_{\mathcal{F}(c)}(K,E[p^m])^\pm \cap \mathrm{H}^1_{\mathcal{F}(c\ell)}(K,E[p^m])^\pm = \mathrm{H}^1_{\mathcal{F}_\ell(c)}(K,E[p^m])^\pm$$

and

$$\mathrm{H}^1_{\mathcal{F}(c)^*}(K,E[p^m])^\pm \cap \mathrm{H}^1_{\mathcal{F}(c\ell)^*}(K,E[p^m])^\pm = \mathrm{H}^1_{\mathcal{F}^\ell(c)^*}(K,E[p^m])^\pm. \qquad \square$$

4. Heegner points over ring class fields

Kolyvagin used Heegner points over ring class fields for certain non-maximal orders of K to construct explicit cohomology classes in $\mathrm{H}^1(K, E[p^m])$ for each m (see [Kol90], [Gro91] or [McC91]). He used these classes to study the structure of the Selmer group $\mathrm{Sel}_{p^\infty}(E/K)$ (see [Kol91a]).

https://doi.org/10.1112/S0010437X08003497 Published online by Cambridge University Press

4.1 Defining Heegner points over ring class fields

4.1.1 *Heegner points over ring class fields.* Let c be a positive integer, let $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$ be the order of conductor c in $\mathcal{O}_K$ and let $\mathcal{N}_c = \mathcal{N} \cap \mathcal{O}_c$. Then $\mathcal{N}_c \subset \mathcal{O}_c$ is an invertible ideal, $\mathcal{O}_c/\mathcal{N}_c \simeq \mathbb{Z}/N\mathbb{Z}$ and the map $\mathbb{C}/\mathcal{O}_c \to \mathbb{C}/\mathcal{N}_c^{-1}$ is a cyclic isogeny of degree N, so it defines a point $x_c \in X_0(N)(\mathbb{C})$ which is $K[c]$-rational by the theory of complex multiplication. One can use the parameterization $\varphi : X_0(N) \to E$ to construct a point $y_c = \varphi(x_c) \in E(K[c])$.

4.1.2 *Kolyvagin primes and conductors.* For each Kolyvagin prime $\ell \in \Lambda^1$ (recall Definition 2.1) let $M(\ell) = \mathrm{ord}_p(a_\ell, \ell + 1)$, where for an integer x, $m = \mathrm{ord}_p(x)$ is the maximal exponent satisfying $p^m \mid x$. Denote by Λ^r the set of all square-free products of exactly r Kolyvagin primes and let $\Lambda = \bigcup_r \Lambda^r$ (by convention, $\Lambda^0 = \{1\}$). For each $c \in \Lambda$ define $M(c) = \min_{\ell|c} M(\ell)$. For the purpose of our argument, we also need to consider the subset $\Lambda_m^r \subset \Lambda^r$ defined as

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

We also set $\Lambda_m = \bigcup_r \Lambda_m^r$.

4.1.3 *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 $\ell + 1$ and $G_c \cong \prod_{\ell|c} G_\ell$ (to see this, one uses that the subgroup of G_c fixing $K[c/\ell]$ is isomorphic to G_ℓ).

We fix a generator σ_ℓ of G_ℓ for each $\ell \in \Lambda^1$ and define $D_\ell = \sum_{i=1}^{\ell} i \cdot \sigma_\ell^i \in \mathbb{Z}[G_\ell]$ and $D_c = \prod_{\ell|c} D_\ell \in \mathbb{Z}[G_c]$. Note that $(\sigma_\ell - 1)D_\ell = 1 + \ell - \mathrm{Tr}_{K[\ell]/K[1]}$. We refer to the D_c as the *Kolyvagin derivative operator* for the conductor c.

Finally, let S be a set of coset representatives for $\mathrm{Gal}(K^{\mathrm{ab}}/K[1]) \subseteq \mathrm{Gal}(K^{\mathrm{ab}}/K)$. Here, K^{ab} denotes the maximal abelian extension of K. For every $c \in \Lambda$, 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 refer to them as *derived Heegner points*.

4.1.4 *Defining m_0 and m_∞.* For what follows, we assume Hypothesis (*). 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 $m_r = \min_{c \in \Lambda^r} m(c)$. Kolyvagin proves [Kol91b, Theorem C] that $m_r \geqslant m_{r+1}$ for every $r \geqslant 0$ and defines $m_\infty = \lim_{r \to \infty} m_r$. Note that $P_1 = y_K$, so (under our assumptions) $m_0 = m'(1) = \mathrm{ord}_p[E(K) : \mathbb{Z}y_K]$ is finite and so are all m_i. Thus, m_∞ is finite.[3]

4.1.5 *Kolyvagin classes $\kappa_{c,m} \in \mathrm{H}^1(K, E[p^m])$.* Let $c \in \Lambda_m$. To construct the class $\kappa_{c,m} \in \mathrm{H}^1(\mathcal{F}, E[p^m])$, one first observes that the image $\tilde{P}_c$ of P_c in $E(K[c])/p^m E(K[c])$ is fixed by $\mathcal{G}_c$ (see [Gro91, Proposition 3.6]). Since the Galois representation $\rho_{E,p}$ is surjective, the restriction map $\mathrm{H}^1(K, E[p^m]) \xrightarrow{\mathrm{res}} \mathrm{H}^1(K[c], E[p^m])^{\mathcal{G}_c}$ is an isomorphism (see [Gro91, pp. 241–242]), so if δ_c :

[3] In fact, Kolyvagin proved that $m_r \geqslant m_{r+1}$ without the assumption that the Heegner point $y_K = P_1$ has infinite order in $E(K)$. In this situation, one could still define m_∞, but it is not at all obvious whether $m_\infty < \infty$. Kolyvagin conjectured this for all elliptic curves (see [Kol91a, Conjecture C] for the original statement of the conjecture and [JLS07] for some applications of Kolyvagin's conjecture and some computational and theoretical evidence).

https://doi.org/10.1112/S0010437X08003497 Published online by Cambridge University Press

$E(K[c])/p^m E(K[c]) \to \mathrm{H}^1(K[c], E[p^m])$ is the Kummer map, one can define

$$\kappa_{c,m} := \mathrm{res}^{-1}(\delta_c(\tilde{P}_c)) \in \mathrm{H}^1(K, E[p^m]).$$

It follows from the definition of the Kummer map that $\kappa_{c,m} = 0$ if and only if $P_c \in p^m E(K[c])$ (which is equivalent to $m \leqslant m(c)$). Moreover, if $m > m(c)$, then $\mathrm{ord}(\kappa_{c,m}) = m - m(c)$. The class $\kappa_{c,m}$ is represented by the 1-cocycle

$$\sigma \mapsto \sigma\left(\frac{P_c}{p^m}\right) - \frac{P_c}{p^m} - \frac{(\sigma-1)P_c}{p^m}, \tag{4}$$

where $(\sigma-1)P_c/p^m$ is the unique p^m-division point of $(\sigma-1)P_c$ in $E(K[c])$ (see [McC91, Lemma 4.1]).

Finally, let $\varepsilon = \pm 1$ be the eigenvalue of the Atkin–Lehner (Fricke) involution w_N on the eigenform f corresponding to E, that is, $f|w_N = \varepsilon \cdot f$. For each $c \in \Lambda_m$, let $\varepsilon(c) = \varepsilon \cdot (-1)^{f_c}$ where $f_c = \#\{\ell : \ell \mid c\}$. It follows from [Gro91, Proposition 5.4(ii)] that $\kappa_{c,m}$ lies in the $\varepsilon(c)$-eigenspace for the action of complex conjugation on $\mathrm{H}^1(K, E[p^m])$, that is, $\kappa_{c,m} \in \mathrm{H}^1(K, E[p^m])^{\varepsilon(c)}$.

4.2 Auxiliary classes $\tilde{\kappa}_{c,m} \in \mathrm{H}^1(K, E[p^m])$

Suppose that $c \in \Lambda$ satisfies $m + m(c) \leqslant M(c)$. We construct a class $\tilde{\kappa}_{c,m} \in \mathrm{H}^1(K, E[p^m])^{\varepsilon(c)}$ such that the cyclic $\mathbb{Z}/p^m\mathbb{Z}$-submodule generated by $\tilde{\kappa}_{c,m}$ is free of rank 1 and contains the original class $\kappa_{c,m}$. Indeed, consider the short exact sequence

$$0 \to E[p^m] \to E[p^{m+m(c)}] \xrightarrow{p^m} E[p^{m(c)}] \to 0,$$

and the corresponding long exact sequence on Galois cohomology

$$0 \to \mathrm{H}^1(K, E[p^m]) \hookrightarrow \mathrm{H}^1(K, E[p^{m+m(c)}]) \xrightarrow{p^m} \mathrm{H}^1(K, E[p^{m(c)}])$$

(here, we have used $\mathrm{H}^0(K, E[p^{m(c)}]) = E(K)[p^{m(c)}] = 0$). Since $m + m(c) \leqslant M(c)$, one has the cohomology class $\kappa_{c,m+m(c)} \in \mathrm{H}^1(K, E[p^{m+m(c)}])$. Using the definition of $\kappa_{c,m}$, we observe that $p^{m(c)}\kappa_{c,m+m(c)} = \kappa_{c,m}$ in $\mathrm{H}^1(K, E[p^{m+m(c)}])$. We claim that $\kappa_{c,m+m(c)}$ is in the image of $\mathrm{H}^1(K, E[p^m])$ under the above inclusion. Indeed, since $\mathrm{ord}(\kappa_{c,m+m(c)}) = m$, then it is in the kernel of the second map in the above exact sequence, that is, it comes from a class $\tilde{\kappa}_{c,m} \in \mathrm{H}^1(K, E[p^m])$. Moreover,

$$\mathrm{ord}\, \tilde{\kappa}_{c,m} = \mathrm{ord}\, \kappa_{c,m+m(c)} = m,$$

that is, $\tilde{\kappa}_{c,m}$ spans a free $\mathbb{Z}/p^m\mathbb{Z}$-submodule of $\mathrm{H}^1(K, E[p^m])^{\varepsilon(c)}$ that contains $\kappa_{c,m} = p^{m(c)}\tilde{\kappa}_{c,m}$.

4.3 Local conditions for Kolyvagin classes

Let $\mathcal{F}$ be the Kummer Selmer structure defined in § 3.3. The cohomology classes $\kappa_{c,m}$ are known to lie in $\mathrm{H}^1_{\mathcal{F}(c)}(K, E[p^m])^{\varepsilon(c)}$ (see [Gro91, Proposition 6.2], [McC91, Lemma 4.3] or [How04, Lemma 1.7.3]). Since the local conditions defining the Selmer structure $\mathcal{F}(c)$ are Cartesian (see [MR04, Definition 1.1.4] for the definition), we have $\tilde{\kappa}_{c,m} \in \mathrm{H}^1_{\mathcal{F}(c)}(K, E[p^m])^{\varepsilon(c)}$ as well.

Our main observation towards the refinement of Kolyvagin's results is the following.

Proposition 4.1. *For any $c \in \Lambda_m$ and any $v \mid N$, one has*

$$\mathrm{loc}_v(\kappa_{c,m}) \in \mathrm{H}^1_{\mathrm{Kum}^0}(K, E[p^m]).$$

To prove the proposition, we need two auxiliary statements.

4.3.1 *Reduction properties of Heegner points.* The following lemma is extracted from several results discussed in the paper of Gross and Zagier (see [GZ86, § III.1] and [GZ86, § III.3, Proposition 3.1]).

https://doi.org/10.1112/S0010437X08003497 Published online by Cambridge University Press

Lemma 4.2. *The Heegner point y_c lies, up to translation by a rational torsion point of E, on $E^0(K[c]_w)$, where $E^0(K[c]_w)$ is the subgroup of $E(K[c]_w)$ of the points that specialize to the identity component of the Néron model of E.*

4.3.2 *A lemma on p-divisibility groups.* We recall the following well-known result (see, e.g., [Cas65]).

Lemma 4.3. *Let $v \nmid p$ be any finite place of K. Then the group $E^0(K_v^{\mathrm{ur}})$ is p-divisible.*

Now, we are ready to prove our refinement.

Proof of Proposition 4.1. By Lemma 4.3 the group $E^0(K_v^{\mathrm{ur}})$ is p-divisible. In other words, there is a short exact sequence

$$0 \to E^0(K_v^{\mathrm{ur}})[p^m] \to E^0(K_v^{\mathrm{ur}}) \xrightarrow{p^m} E^0(K_v^{\mathrm{ur}}) \to 0.$$

By taking the long exact sequence on Galois cohomology and using the fact that Néron models are stable under unramified base change, we obtain the following exact sequence

$$E^0(K_v) \to \mathrm{H}^1(K_v^{\mathrm{ur}}/K_v, E^0(K_v^{\mathrm{ur}})[p^m]) \to \mathrm{H}^1(K_v^{\mathrm{ur}}/K_v, E^0(K_v^{\mathrm{ur}}))[p^m] \to 0.$$

However, $\mathrm{H}^1(K_v^{\mathrm{ur}}/K_v, E^0(K_v^{\mathrm{ur}})) = 0$ according to Lang's theorem (see [Lan56]), that is, the map $E^0(K_v) \to \mathrm{H}^1(K_v^{\mathrm{ur}}/K_v, E^0(K_v^{\mathrm{ur}})[p^m])$ is surjective. We thus consider the following commutative diagram

$$\begin{array}{ccccccc} E^0(K_v) & \longrightarrow & \mathrm{H}^1(K_v^{\mathrm{ur}}/K_v, E^0(K_v^{\mathrm{ur}})[p^m]) & & & & \\ \downarrow & & \downarrow{\scriptstyle \phi} & & & & \\ E(K_v) & \longrightarrow & \mathrm{H}^1(K_v, E[p^m]) & \longrightarrow & \mathrm{H}^1(K_v, E)[p^m] & \longrightarrow & 0 \end{array}$$

where the map ϕ is the composition

$$\mathrm{H}^1(K_v^{\mathrm{ur}}/K_v, E^0(K_v^{\mathrm{ur}})[p^m]) \to \mathrm{H}^1(K_v^{\mathrm{ur}}/K_v, E(K_v^{\mathrm{ur}})[p^m]) \xrightarrow{\inf} \mathrm{H}^1(K_v, E[p^m]).$$

We will be done if we can show that the class $\mathrm{loc}_v(\kappa_{c,m})$ lies in the image of ϕ (the surjectivity then implies that it comes from a point of $E^0(K_v)$). To see that $\mathrm{loc}_v(\kappa_{c,m}) \in \mathrm{im}(\phi)$, we look at the explicit cocycle (4) and use Lemma 4.2 to show that there exists a point $Q \in E(\mathbb{Q})_{\mathrm{tor}}$ such that $Q_c = P_c - Q \in E^0(K_v^{\mathrm{ur}})$. Since $E(\mathbb{Q})[p^\infty] = 0$, the point Q is p-divisible over $\mathbb{Q}$. This, together with the p-divisibility of $E^0(K_v^{\mathrm{ur}})$ (Lemma 4.3) implies

$$\kappa_{c,m}(\sigma) = -\frac{(\sigma-1)P_c}{p^m} + \sigma\left(\frac{P_c}{p^m}\right) - \frac{P_c}{p^m} = -\frac{(\sigma-1)Q_c}{p^m} + \sigma\left(\frac{Q_c}{p^m}\right) - \frac{Q_c}{p^m} \in E^0(K_v^{\mathrm{ur}})[p^m].$$

Therefore, the class $\kappa_{c,m}$ is the image of the cohomology class of $\mathrm{H}^1(K_v^{\mathrm{ur}}/K_v, E^0(K_v^{\mathrm{ur}})[p^m])$ represented by the cocycle

$$\sigma \mapsto -\frac{(\sigma-1)Q_c}{p^m} + \sigma\left(\frac{Q_c}{p^m}\right) - \frac{Q_c}{p^m}$$

under the map ϕ. This proves the proposition. □

4.4 Local comparison between $\kappa_{c,m}$ and $\kappa_{c\ell,m}$

We need to use a (slightly modified) construction of Mazur–Rubin and Howard of a comparison isomorphism

$$\phi_\lambda : \mathrm{H}^1_{\mathrm{ur}}(K_\lambda, E[p^m]) \to \mathrm{H}^1_{\mathrm{tr}}(K_\lambda, E[p^m])$$

at places λ above Kolyvagin primes (also known as the finite-singular comparison map). The definition in the Heegner point setting is given in [How04, Definition 1.1.8]. Here, we use a twisted

https://doi.org/10.1112/S0010437X08003497 Published online by Cambridge University Press

version of Howard's construction in order to avoid some technical difficulties when we establish the local relations at λ between the classes $\kappa_{c,m}$ and $\kappa_{c\ell,m}$.

The difference between our ϕ_λ and the homomorphism constructed by Howard (see [How04, Definition 1.1.8]) is the extra twist by an automorphism $\chi_\ell : E[p^{M(\ell)}] \to E[p^{M(\ell)}]$ (see [How04, Proposition 1.7.4]). This allows us to have an explicit comparison between $\mathrm{loc}_\lambda(\kappa_{c,m})$ and $\mathrm{loc}_\lambda(\kappa_{c\ell,m})$ via the following proposition, whose proof is identical to that of [How04, Proposition 1.7.4].

Proposition 4.4. *For any $c \in \Lambda_m$ and $\ell \in \Lambda_m^1$ for which $\ell \nmid c$,*

$$\phi_\lambda(\mathrm{loc}_\lambda(\kappa_{c,m})) = \mathrm{loc}_\lambda(\kappa_{c\ell,m}).$$

In particular, since ϕ_λ is an isomorphism, $\mathrm{ord}'_p(\mathrm{loc}_\lambda(\kappa_{c,m})) = \mathrm{ord}'_p(\mathrm{loc}_\lambda(\kappa_{c\ell,m}))$.

5. Proof of the main theorem

5.1 An application of Čebotarev density theorem

The following lemma is an application of Čebotarev density theorem and will be used in the proof of our theorem.

Lemma 5.1. *Assume that Hypothesis (*) holds and let*

$$\kappa^+ \in \mathrm{H}^1(K, E[p^m])^+, \ \kappa^- \in \mathrm{H}^1(K, E[p^m])^-$$

be cohomology classes with $M^+ = \mathrm{ord}(\kappa^+)$ and $M^- = \mathrm{ord}(\kappa^-)$. There exist infinitely many primes $\ell \in \Lambda_m^1$ such that $\mathrm{ord}'_p(\mathrm{loc}_\lambda(\kappa^+)) = M^+$ and $\mathrm{ord}'_p(\mathrm{loc}_\lambda(\kappa^-)) = M^-$, where λ is the unique place of K above ℓ.

Proof. This follows immediately from [McC91, Corollary 3.2] since the cohomology classes κ^+ and κ^- are linearly independent. □

Remark 2. Hypothesis (*) can be weakened since the proof of [McC91, Corollary 3.2] does not need the surjectivity of the Galois representation, but simply the weaker assumption that $\mathrm{End}_{\mathbb{F}_p}(E[p])$ is spanned (as an $\mathbb{F}_p$-vector space) by the elements $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$. This fact is equivalent to the absolute irreducibility of the Galois representation $\rho_{E,p}$.

5.2 Core vertices and minimal core vertices

Let m be an integer. For clarity, we denote each Selmer module $\mathrm{H}^1_{\mathcal{G}(c)}(K, E[p^m])$ simply by $\mathcal{H}_{\mathcal{G}(c)}$ for various Selmer structures $\mathcal{G}$ (i.e. we omit the Galois group and the Galois representation since they will stay fixed).

Following the terminology of [MR04], we define a *core vertex* for m and for the Kummer Selmer structure $\mathcal{F}$ to be any conductor $c \in \Lambda_m$, such that either

$$\mathbf{Inv}\,\mathcal{H}^+_{\mathcal{F}(c)} = (m) \quad \text{and} \quad \mathbf{Inv}\,\mathcal{H}^-_{\mathcal{F}(c)} = (\,),$$

or

$$\mathbf{Inv}\,\mathcal{H}^+_{\mathcal{F}(c)} = (\,) \quad \text{and} \quad \mathbf{Inv}\,\mathcal{H}^-_{\mathcal{F}(c)} = (m).$$

A *minimal core vertex* is a core vertex c for m for which $m(c) = m_\infty < m \leqslant M(c)$. To make the argument easier to follow, we prove the theorem in the case when there exists a minimal core vertex for sufficiently large m.

Theorem 5.2. *Assume that there exists a minimal core vertex $c \in \Lambda_m$ for some $m > \max(m_{\max}, m_\infty)$. Then $m_\infty \geqslant m_{\max}$.*

https://doi.org/10.1112/S0010437X08003497 Published online by Cambridge University Press

Proof. We may assume that $m_{\max} > 0$. Since $m > m(c)$, the class $\kappa_{c,m} \in \mathcal{H}^{\varepsilon(c)}_{\mathcal{F}(c)}$ is nontrivial. Since c is a core vertex, we conclude that $\mathcal{H}^{\varepsilon(c)}_{\mathcal{F}(c)} \cong \mathbb{Z}/p^m\mathbb{Z}$ and $\mathcal{H}^{-\varepsilon(c)}_{\mathcal{F}(c)} = 0$.

Fix q such that $\mathrm{ord}_p(c_q) = m_{\max}$. Then $q \mid N$, so q splits in K by the Heigner hypothesis. Let v and $\bar{v}$ be the places of K above q, so $c_v = c_{\bar{v}} = c_q$. Consider the connected Kummer Selmer structure $\mathcal{F}_0$ that differs from $\mathcal{F}$ only at v and $\overline{v}$. Consider the two Selmer modules $\mathcal{H}_{\mathcal{F}_0(c)}$ and $\mathcal{H}_{\mathcal{F}_0(c)^*}$.

Since $\mathcal{H}^{\varepsilon(c)}_{\mathcal{F}_0(c)}$ is a submodule of $\mathcal{H}^{\varepsilon(c)}_{\mathcal{F}(c)}$, we have $\mathcal{H}^{\varepsilon(c)}_{\mathcal{F}_0(c)} \cong \mathbb{Z}/p^{m'}\mathbb{Z}$ for some integer m' satisfying $0 \leqslant m' \leqslant m$. Similarly, $\mathcal{H}^{-\varepsilon(c)}_{\mathcal{F}_0(c)} = 0$.

One can now determine the invariants of the dual modules $\mathcal{H}^{\pm}_{\mathcal{F}_0(c)^*}$ in terms of m, m' and $m_{\max}$ by applying Theorem 3.3 to the exact sequence[4]

$$0 \to \mathcal{H}^{\pm\varepsilon(c)}_{\mathcal{F}_0(c)} \hookrightarrow \mathcal{H}^{\pm\varepsilon(c)}_{\mathcal{F}(c)} \to \left(\frac{\mathrm{H}^1_{\mathrm{Kum}}(K_v, E[p^m])}{\mathrm{H}^1_{\mathrm{Kum}^0}(K_v, E[p^m])} \oplus \frac{\mathrm{H}^1_{\mathrm{Kum}}(K_{\bar{v}}, E[p^m])}{\mathrm{H}^1_{\mathrm{Kum}^0}(K_{\bar{v}}, E[p^m])} \right)^{\pm\varepsilon(c)}$$

and the dualized sequence

$$0 \to \mathcal{H}^{\pm\varepsilon(c)}_{\mathcal{F}(c)} \hookrightarrow \mathcal{H}^{\pm\varepsilon(c)}_{\mathcal{F}_0(c)^*} \to \left(\frac{\mathrm{H}^1_{\mathrm{Kum}^0}(K_v, E[p^m])^{\perp}}{\mathrm{H}^1_{\mathrm{Kum}}(K_v, E[p^m])} \oplus \frac{\mathrm{H}^1_{\mathrm{Kum}^0}(K_{\bar{v}}, E[p^m])^{\perp}}{\mathrm{H}^1_{\mathrm{Kum}}(K_{\bar{v}}, E[p^m])} \right)^{\pm\varepsilon(c)},$$

where $\mathrm{H}^1_{\mathrm{Kum}^0}(K_v, E[p^m])^{\perp}$ and $\mathrm{H}^1_{\mathrm{Kum}^0}(K_{\bar{v}}, E[p^m])^{\perp}$ are the orthogonal complements of the local conditions $\mathrm{H}^1_{\mathrm{Kum}^0}(K_v, E[p^m])$ and $\mathrm{H}^1_{\mathrm{Kum}^0}(K_{\bar{v}}, E[p^m])$ under the Tate local pairing. Since $m > m_{\max} = \mathrm{ord}_p(c_v)$, Lemma 3.2 implies that the last term in each of the above sequences is isomorphic to $\mathbb{Z}/p^{m_{\max}}\mathbb{Z}$. This allows us to apply global duality (Theorem 3.3) to conclude that

$$\mathbf{Inv}(\mathcal{H}^{\varepsilon(c)}_{\mathcal{F}_0(c)^*}) = (m, m_{\max} + m' - m) \text{ and } \mathbf{Inv}(\mathcal{H}^{-\varepsilon(c)}_{\mathcal{F}_0(c)^*}) = (m_{\max}).$$

Moreover, $\mathcal{H}^{\varepsilon(c)}_{\mathcal{F}_0(c)^*} \cong \mathcal{H}^{\varepsilon(c)}_{\mathcal{F}(c)} \oplus T$, where $\mathcal{H}^{\varepsilon(c)}_{\mathcal{F}(c)} \cong \mathbb{Z}/p^m\mathbb{Z}$ is generated by $\tilde{\kappa}_{c,m}$ and T is isomorphic to $\mathbb{Z}/p^{m_{\max}+m'-m}\mathbb{Z}$. Let κ be a generator for the cyclic $\mathbb{Z}/p^m\mathbb{Z}$-module $\mathcal{H}^{-\varepsilon(c)}_{\mathcal{F}_0(c)*} \cong \mathbb{Z}/p^m_{\max}\mathbb{Z}$. By Lemma 5.1, there exists $\ell \in \Lambda^1_m$, $(\ell, c) = 1$, such that $\mathrm{ord}'_p(\mathrm{loc}_\lambda(\tilde{\kappa}_{c,m})) = m$ and $\mathrm{ord}'_p(\mathrm{loc}_\lambda(\kappa)) = m_{\max}$, where λ is the unique prime of K above ℓ.

The key idea to finish the proof is to determine the invariants of the Selmer module $\mathcal{H}^{-\varepsilon(c)}_{(\mathcal{F}_0)^\ell(c)}$. Indeed, by the choice of ℓ, the cyclic cokernel of the map $\mathcal{H}^{-\varepsilon(c)}_{(\mathcal{F}_0)^\ell(c)^*} \to \mathcal{H}^{-\varepsilon(c)}_{\mathcal{F}_0(c)^*}$ has length $m_{\max}$. This means (by Lemma 3.4(iii)) that the cokernel of the corresponding dual map $\mathcal{H}^{-\varepsilon(c)}_{\mathcal{F}_0(c)} \to \mathcal{H}^{-\varepsilon(c)}_{(\mathcal{F}_0)^\ell(c)}$ has length $m - m_{\max}$. Thus, we conclude that $\mathcal{H}^{-\varepsilon(c)}_{(\mathcal{F}_0)^\ell(c)}$ is cyclic of length $m - m_{\max}$.

To complete the argument, notice that $\mathcal{H}^{-\varepsilon(c)}_{\mathcal{F}_0(c\ell)}$ is a submodule of $\mathcal{H}^{-\varepsilon(c)}_{(\mathcal{F}_0)^\ell(c)} \cong \mathbb{Z}/p^{m-m_{\max}}\mathbb{Z}$. Since $\kappa_{c\ell,m} \in \mathcal{H}^{-\varepsilon(c)}_{\mathcal{F}_0(c\ell)}$, then

$$m - m_{\max} \geqslant \mathrm{ord}'_p(\kappa_{c\ell,m}) \geqslant \mathrm{ord}'_p(\mathrm{loc}_\lambda(\kappa_{c\ell,m})) = \mathrm{ord}'_p(\mathrm{loc}_\lambda(\kappa_{c,m})) = \mathrm{ord}'_p(\kappa_{c,m}) = m - m_\infty,$$

where the first equality follows from Proposition 4.4 and the second equality follows because $\mathrm{ord}'_p(\mathrm{loc}_\lambda(\kappa')) = m$ (i.e. loc_λ is injective on $\mathbb{Z}\kappa'$). Thus, $m_\infty \geqslant m_{\max}$. □

5.3 Existence of core vertices and the general case

In this final section, we reduce the proof of Theorem 1.1 to the case when there exists a minimal core vertex (Theorem 5.2). Whenever m is fixed, we accept the Selmer modules notation from the previous section. The most difficult part of the proof is the following proposition.

[4]Note that the exact sequence implies $m - m' \leqslant m_{\max}$.

https://doi.org/10.1112/S0010437X08003497 Published online by Cambridge University Press

Proposition 5.3. *Let $c \in \Lambda$ satisfy $m(c) + m \leqslant M(c)$. There exists a core vertex $c' \in \Lambda_{m+m(c)}$, such that $m(c') \leqslant m(c)$.*

Proof. Since $m(c) + m \leqslant M(c)$, the class $\tilde{\kappa}_{c,m}$ is defined, lies in $\mathcal{H}_{\mathcal{F}(c)}$ (see § 4.3) and generates a free $\mathbb{Z}/p^m\mathbb{Z}$-submodule of $\mathcal{H}_{\mathcal{F}(c)}$ that contains $\kappa_{c,m}$. This means that

$$\mathbf{Inv}(\mathcal{H}_{\mathcal{F}(c)}^{\varepsilon(c)}) = (m, x_1, x_2, \ldots)$$

for some $x_1 \geqslant x_2 \geqslant \cdots \geqslant 0$. Let

$$\mathbf{Inv}(\mathcal{H}_{\mathcal{F}(c)}^{-\varepsilon(c)}) = (y_1, y_2, \ldots),$$

where $y_1 \geqslant y_2 \geqslant \cdots \geqslant 0$. Choose a prime $\ell_1 \in \Lambda^1_{M(c)}$, such that $\mathrm{ord}'_p(\mathrm{loc}_{\lambda_1}(\kappa)) = y_1$ and $\mathrm{ord}'_p(\mathrm{loc}_{\lambda_1}(\tilde{\kappa}_{c,m})) = m$ (here, λ_1 is the unique prime of K above ℓ_1 and κ is a generator for a direct summand of $\mathcal{H}_{\mathcal{F}(c)}^{-\varepsilon(c)}$ corresponding to the invariant y_1). Such a prime can be selected according to Lemma 5.1.

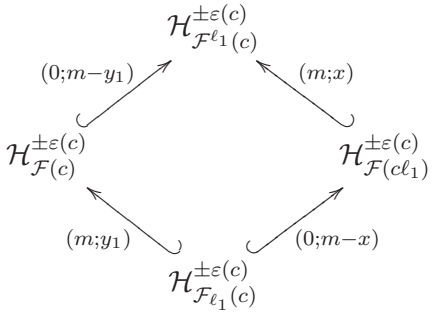
Next, we compute the invariants of $\mathcal{H}_{\mathcal{F}(c\ell_1)}^{\pm\varepsilon(c\ell_1)}$. More precisely, we claim that $y_1 = y_2$ and

$$\mathbf{Inv}(\mathcal{H}_{\mathcal{F}(c\ell_1)}^{-\varepsilon(c\ell_1)}) = (x_1, x_2, \ldots)$$

and

$$\mathbf{Inv}(\mathcal{H}_{\mathcal{F}(c\ell_1)}^{\varepsilon(c\ell_1)}) = (m, y_3, \ldots).$$

To show this, we look at the lozenge diagrams for the self-dual Kummer Selmer structure $\mathcal{F}$ and fill up as much as we can the lengths of the corresponding cokernels (the notation $(a; b)$ means that the cyclic cokernel for the $\varepsilon(c)$-part has length a and the cyclic cokernel for the $-\varepsilon(c)$-part has length b: we refer to it as the type of the cokernels).



Indeed, the choice of ℓ_1 implies that the cokernels of the maps $\mathcal{H}^{\pm\varepsilon(c)}_{\mathcal{F}_{\ell_1}(c)} \hookrightarrow \mathcal{H}^{\pm\varepsilon(c)}_{\mathcal{F}(c)}$ have type $(m; y_1)$. By Lemma 3.4(iii), the corresponding dual maps $\mathcal{H}^{\pm\varepsilon(c)}_{\mathcal{F}(c)} \hookrightarrow \mathcal{H}^{\pm\varepsilon(c)}_{\mathcal{F}^{\ell_1}(c)}$ have cokernels of type $(0; m-y_1)$. Next, by Lemma 3.4(iv), the cokernel of the map $\mathcal{H}^{\varepsilon(c)}_{\mathcal{F}(c\ell_1)} \hookrightarrow \mathcal{H}^{\varepsilon(c)}_{\mathcal{F}^{\ell_1}(c)}$ has length m and the cokernel of the map $\mathcal{H}^{\varepsilon(c)}_{\mathcal{F}_{\ell_1}(c)} \hookrightarrow \mathcal{H}^{\varepsilon(c)}_{\mathcal{F}(c)}$ is trivial. Let x be the length of the cokernel of the map $\mathcal{H}^{-\varepsilon(c)}_{\mathcal{F}(c\ell_1)} \hookrightarrow \mathcal{H}^{-\varepsilon(c)}_{\mathcal{F}^{\ell_1}(c)}$. Again, by Lemma 3.4(iii), the cokernel of the map $\mathcal{H}^{-\varepsilon(c)}_{\mathcal{F}_{\ell_1}(c)} \hookrightarrow \mathcal{H}^{-\varepsilon(c)}_{\mathcal{F}(c)}$ has length $m-x$. This justifies the labelling of the diagram. By using Lemma 3.4(iv), we note that $m-y_1 \geqslant m-x$, that is, $x \geqslant y_1$.

The next crucial observation is that $x = y_1$. To see this, we observe that the comparison isomorphism ϕ_{λ_1} and Proposition 4.4 imply

$$m - m(c\ell_1) \geqslant \mathrm{ord}'_p(\mathrm{loc}_{\lambda_1}(\kappa_{c\ell_1,m})) = \mathrm{ord}'_p(\mathrm{loc}_{\lambda_1}(\kappa_{c,m})) = \mathrm{ord}'_p(\kappa_{c,m}) = m - m(c),$$

and, hence, $m(c\ell_1) \leqslant m(c)$. This means that $m(c\ell_1) + m \leqslant M(c) = M(c\ell_1)$, so the class $\kappa_{c\ell_1,m}$ lives in a free submodule of $\mathcal{H}^{\varepsilon(c\ell_1)}_{\mathcal{F}(c\ell_1)}$ of rank one. Thus, the module $\mathcal{H}_{\mathcal{F}(c\ell_1)}$ contains an invariant m.

https://doi.org/10.1112/S0010437X08003497 Published online by Cambridge University Press

Hence, by looking at the inclusion $\mathcal{H}_{\mathcal{F}_{\ell_1}(c)} \hookrightarrow \mathcal{H}_{\mathcal{F}(c\ell_1)}$ and using that $x \geqslant y_1$, we obtain $x = y_1 = y_2$. Moreover, we determine the invariants

$$\mathbf{Inv}\,\mathcal{H}^{\varepsilon(c\ell_1)}_{\mathcal{F}(c\ell_1)} = (m, y_3, \dots) \quad \text{and} \quad \mathbf{Inv}\,\mathcal{H}^{-\varepsilon(c\ell_1)}_{\mathcal{F}(c\ell_1)} = (x_1, x_2, \dots).$$

We repeat the above process and use Lemma 5.1 to choose a prime $\ell_2 \in \Lambda_{M(c)}$, such that $\mathrm{ord}'_p(\mathrm{loc}_{\lambda_2}(\kappa_2)) = x_1$ and $\mathrm{ord}'_p(\mathrm{loc}_{\lambda_2}(\tilde{\kappa}_{c,m})) = m$, where λ_2 is the unique prime of K lying above ℓ_2 and κ_2 is a generator of a direct summand corresponding to the invariant x_1. By exactly the same argument, $m(c\ell_1\ell_2) \leqslant m(c\ell_1) \leqslant m(c)$, $x_1 = x_2$ and

$$\mathbf{Inv}\,\mathcal{H}^{\varepsilon(c\ell_1\ell_2)}_{\mathcal{F}(c\ell_1\ell_2)} = (m, x_3, x_4, \dots) \quad \text{and} \quad \mathbf{Inv}\,\mathcal{H}^{-\varepsilon(c\ell_1\ell_2)}_{\mathcal{F}(c\ell_1\ell_2)} = (y_3, y_4, \dots).$$

We continue the process of adding primes from $\Lambda^1_{M(c)}$ to the conductor until we reach a conductor $c' = c\ell_1 \dots \ell_s$, such that $\mathcal{H}^{\varepsilon(c')}_{\mathcal{F}(c')} \cong \mathbb{Z}/p^m\mathbb{Z}$ and $\mathcal{H}^{\varepsilon(c')}_{\mathcal{F}(c')} = 0$ and for which $m(c') \leqslant m(c)$. □

Finally, we prove the main Theorem 1.1.

Proof of Theorem 1.1. According to [Kol91b, Theorem 1], one can also describe m_∞ as

$$m_\infty = \lim_{r\to\infty} \inf_{c\in\Lambda^r_{m'}} m(c)$$

for any sufficiently large integer m' (in particular, for $m' > 2m_0$). Fix an integer $m > \max\{m_0, m_{\max}\}$ and let $m' = m + m_0$. Choose $c \in \Lambda^r_{m'}$ for which $m(c) = m_\infty$ (such a c exists according to the above redefinition of m_∞).

Since $m(c)+m = m_\infty+m < m' \leqslant M(c)$, by Theorem 5.3, there exists a core vertex $c' \in \Lambda_{m+m(c)}$, such that $m(c') \leqslant m(c) = m_\infty$ (i.e. $m(c') = m_\infty$). This, together with $m(c') + m \leqslant M(c')$ implies that c' is a minimal core vertex. Thus, Theorem 5.2 implies the desired inequality. □

Remark 3. It is natural to ask whether one could prove the full inequality

$$m_\infty \geqslant \mathrm{ord}_p\left(\prod_{q|N} c_q\right)$$

by using a Selmer structure with more than one connected Kummer local condition and refining the above argument. For instance, if $p \mid c_{q_1}$ and $p \mid c_{q_2}$ for two Tamagawa numbers at primes $q_1 \neq q_2$, then one would like to show that $m_\infty \geqslant 2$. The reason this approach fails is that one would need a local term isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$ in the global duality sequences as opposed to two local terms isomorphic to $\mathbb{Z}/p\mathbb{Z}$ in order to reach a cyclic Selmer module whose length is at most $m-2$ containing $\kappa_{c\ell,m}$ as in the final step of the proof of Theorem 5.2.

Remark 4. A related result in a disjoint setting has recently been established by Büyükboduk in [Büy07] via the machinery of Kolyvagin systems. However, Büyükboduk's result does not provide new upper bounds on the order of the Shafarevich–Tate group since the exact bounds predicted by the Birch and Swinnerton-Dyer conjecture in the corresponding setting have already been established via arguments from Iwasawa theory.

Acknowledgements

I am grateful to William Stein for suggesting the problem to me and for various helpful discussions. I am very grateful to my advisor Ken Ribet for his constant encouragement, guidance and support, and for numerous helpful conversations on the project.

I am indebted to Christophe Cornut for his enormous help and support while working on this project, for the careful reading of the preliminary draft and for sharing his deep and fine understanding of Kolyvagin's method. I am grateful to the anonymous referee for the numerous comments and suggestions which helped me significantly improve the exposition.

I am also grateful to Byungchul Cha, Mladen Dimitrov, Olivier Fouquet, Ralph Greenberg, Ben Howard, Grigor Grigorov, Barry Mazur, Robert Pollack, Bjorn Poonen, Karl Rubin and Olivier Wittenberg, for the many helpful conversations. It is also a pleasure to thank the Mathematical Sciences Research Institute at Berkeley and the Institut de Mathématiques de Jussieu, Paris for their kind hospitality.

References

ARS06 A. Agashe, K. Ribet and W. Stein, *The Manin constant*, Pure Appl. Math. Q. **2** (2006), 617–636.

AU96 A. Abbes and E. Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires*, Compositio Math. **103** (1996), 269–286.

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), 843–939 (electronic).

Büy07 K. Büyükboduk, *Tamagawa defect of Euler systems*, Preprint (2007).

Cas65 J. W. S. Cassels, *Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer*, J. reine angew. Math. **217** (1965), 180–199.

Cha05 B. Cha, *Vanishing of some cohomology groups and bounds for the Shafarevich–Tate groups of elliptic curves*, J. Number Theory **111** (2005), 154–178.

Col03 P. Colmez, *La conjecture de Birch et Swinnerton-Dyer p-adique*, in *Séminaire Bourbaki (2003), Exposé 919*, Asterisque, vol. 294 (Société Mathématique de France, Paris, 2003).

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

GZ86 B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225–320.

How04 B. Howard, *The Heegner point Kolyvagin system*, Compositio Math. **140** (2004), 1439–1472.

JLS07 D. Jetchev, K. Lauter and W. Stein, *Explicit Heegner points: Kolyvagin's conjecture and nontrivial elements of the Shafarevich–Tate group*, Preprint (2007), available at http://modular.math.washington.edu/papers/kolyconj/.

Kol90 V. A. Kolyvagin, *Euler systems*, in *The Grothendieck Festschrift*, vol. II (Birkhäuser, Boston, MA, 1990), 435–483.

Kol91a V. A. Kolyvagin, *On the structure of Selmer groups*, Math. Ann. **291** (1991), 253–259.

Kol91b V. A. Kolyvagin, *On the structure of Shafarevich–Tate groups*, in *Algebraic geometry*, Chicago, IL, 1989 (Springer, Berlin, 1991), 94–121.

Lan56 S. Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563.

McC91 W. G. McCallum, *Kolyvagin's work on Shafarevich–Tate groups*, in *L-functions and arithmetic*, Durham, 1989 (Cambridge University Press, Cambridge, 1991), 295–316.

Mil86 J. S. Milne, *Arithmetic duality theorems* (Academic Press, Boston, MA, 1986).

MR04 B. Mazur and K. Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), viii+96.

Rub00 K. Rubin, *Euler systems*, Annals of Mathematics Studies, vol. 147 (Princeton University Press, Princeton, NJ, 2000).

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

SW08 W. Stein and C. Wuthrich, *Computations about Tate–Shafarevich groups using Iwasawa theory.* Preprint (2008), available at http://modular.math.washington.edu/papers/shark.

Tat63 J. Tate, *Duality theorems in Galois cohomology over number fields*, in *Proceedings of the International Congress of Mathematicians*, Stockholm, 1962 (Institute Mittag-Leffler, Djursholm, 1963), 288–295.

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

https://doi.org/10.1112/S0010437X08003497 Published online by Cambridge University Press