TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 349, Number 10, October 1997, Pages 4181–4200
S 0002-9947(97)01762-5

ON THE CONJECTURE OF BIRCH AND SWINNERTON-DYER

CRISTIAN D. GONZALEZ-AVILÉS

A mis padres

Abstract. In this paper we complete Rubin's partial verification of the conjecture for a large class of elliptic curves with complex multiplication by $\mathbb{Q}(\sqrt{-7})$.

1. Introduction

In this paper we prove the full Birch and Swinnerton-Dyer conjecture for a class of elliptic curves with complex multiplication by $\mathbb{Q}(\sqrt{-7})$.

This paper is an expanded version of the author's doctoral thesis [11], which was completed at The Ohio State University under the supervision of Karl Rubin. It is to be the first in a series of papers aimed at completing Rubin's partial verification of one important case of the conjecture (see Theorem 11.1(i) of [21]).

The setting is as follows.

Let E be an elliptic curve defined over the field $K = \mathbb{Q}(\sqrt{-7})$ (which is one of the 9 imaginary quadratic fields of class number 1), with complex multiplication by the ring of integers $\mathcal{O}$ of K, and with minimal period lattice generated by $\Omega \in \mathbb{C}^\times$. Suppose that the L-function of E over K does not vanish at $s = 1$, i.e. $L(E_{/K}, 1) \neq 0$. Then $E(K)$ is finite [5] and the Tate-Shafarevich group $\text{Ш}(E_{/K})$ is finite [20]. Now for each prime $\mathfrak{q}$ of K let $c_\mathfrak{q} = [E(K_\mathfrak{q}) : E_0(K_\mathfrak{q})]$, where $E_0(K_\mathfrak{q})$ is the subgroup of $E(K_\mathfrak{q})$ of points with non-singular reduction modulo $\mathfrak{q}$. In this work we prove the following theorem.

Theorem A. *Suppose $L(E_{/K}, 1) \neq 0$. Then*

$$L(E_{/K}, 1) = \Omega\bar{\Omega} \cdot (\#E(K))^{-2} \cdot \#\text{Ш}(E_{/K}) \cdot \prod c_\mathfrak{q} .$$

In other words, the full Birch and Swinnerton-Dyer conjecture is true for E.

In addition, we will deduce from Theorem A the following result concerning curves defined over $\mathbb{Q}$. For any $d \in \mathbb{Z} - \{0\}$, let E^d be the elliptic curve $y^2 = x^3 + 21dx^2 + 112d^2x$, which has complex multiplication by $\mathcal{O} = \mathbb{Z}[(1 + \sqrt{-7})/2]$.

Theorem B. *If $L(E^d_{/\mathbb{Q}}, 1) \neq 0$, then the full Birch and Swinnerton-Dyer conjecture is true for $E^d_{/\mathbb{Q}}$.*

Received by the editors May 19, 1995 and, in revised form, March 6, 1996.
1991 *Mathematics Subject Classification.* Primary 11G40, 11G05.
Supported by Fondecyt, proyecto no. 1950543.

The following is a summary of the paper.

Write ψ for the Hecke character of K attached to E. Then $L(\psi,1)/\Omega \in K$ and the L-function of E over K factors as

$$L(E_{/K}, s) = L(\psi, s)L(\bar{\psi}, s). \tag{1}$$

Now write $Ш = Ш(E_{/K})$ and let B be the set of primes of K where E has bad reduction. We will see below (Proposition 2.6) that $c_{\mathfrak{q}} = 4$ for all $\mathfrak{q} \in B$, so $\prod c_{\mathfrak{q}} = 4^b$ where $b = \#B$. Further, the theorem of Rubin alluded to above ([21], Theorem 11.1(i)) together with the fact that $\#(Ш_{\mathfrak{q}^\infty}) = \#(Ш_{\bar{\mathfrak{q}}^\infty})$ for every prime $\mathfrak{q}$ of K ([14], p. 228) shows that if $\mathfrak{q} \nmid \#\mathcal{O}^\times$, then

$$L(\bar{\psi},1)/\Omega \ \sim_{\mathfrak{q}} \ 2^b \cdot (\#E(K))^{-1} \cdot \sqrt{\#Ш}, \tag{2}$$

where $\sim_{\mathfrak{q}}$ means "equal up to a unit of $K_{\mathfrak{q}}$".

In this paper we prove (2) for the primes $\mathfrak{q}$ that divide $\#\mathcal{O}^\times = 2$. Since 2 splits in K (and we note that $K = \mathbb{Q}(\sqrt{-7})$ is the only imaginary quadratic field of class number 1 with this property), it will be sufficient to show that

$$L(\bar{\psi},1)/\Omega \ \sim_{\mathfrak{p}} \ 2^b \cdot (\#E(K)_{2^\infty})^{-1} \cdot \#Ш_{\mathfrak{p}^\infty} \tag{3}$$

for $\mathfrak{p} | 2$. It will then follow that Gross' refinement [14] of the Birch and Swinnerton-Dyer conjecture for E is true, i.e.

$$L(\bar{\psi},1)/\Omega = \pm\, 2^b \cdot (\#E(K))^{-1} \cdot \sqrt{\#Ш}. \tag{4}$$

Using (1), this formula immediately implies Theorem A.

For convenience, we will exclude from the remainder of this discussion a small number of "exceptional" curves (these are defined at the beginning of §2 and will be studied in §8).

To establish (3) for the remaining, non-exceptional, curves, we will first show that

$$\#\mathrm{Hom}(X_\infty, E_{\mathfrak{p}^\infty})^{\mathcal{G}} = 2^{b^*} \cdot \#E(K_{\mathfrak{p}})_{\bar{\mathfrak{p}}^\infty} \cdot (\#E(K)_{2^\infty})^{-1} \cdot \#Ш_{\mathfrak{p}^\infty}, \tag{5}$$

where $b^* = \#(B - \{\mathfrak{p}\})$, X_∞ is the Galois group of the maximal abelian 2-extension of $K_\infty = K(E_{\mathfrak{p}^\infty})$ which is unramified outside of the primes above $\mathfrak{p}$, and $\mathcal{G} = \mathrm{Gal}(K_\infty/K)$. The essential ingredient in the derivation of this result is a theorem of Bashmakov [1], which describes the image of a certain localization map. See Theorem 3.2 below. The rest of the argument leading to (5) is likely to seem familiar to those readers acquainted with Coates' paper [4] (but also a little more complicated, because here we deal with the troublesome prime 2 and we do not assume good reduction at 2).

Now Rubin [21] has shown how to relate the integer on the left-hand side of formula (5) to $\mathrm{ord}_{\mathfrak{p}}(L(\bar{\psi},1)/\Omega)$ when $\mathfrak{p} \nmid 2$, as an application of the "main conjecture" of Iwasawa theory for K. In this work we prove a main conjecture for the extension K_∞/K (see Theorem 4.1 below) which has similar applications. Since 2 splits in K, we are in the setting of a one-variable main conjecture, which makes the case $K = \mathbb{Q}(\sqrt{-7})$ the simplest of all. We will then use the main conjecture to show that

$$\#\mathrm{Hom}(X_\infty, E_{\mathfrak{p}^\infty})^{\mathcal{G}} \sim_{\mathfrak{p}} \ 2^{b^* - b} \cdot \#E(K_{\mathfrak{p}})_{\bar{\mathfrak{p}}^\infty} \cdot L(\bar{\psi},1)/\Omega.$$

This formula together with (5) yields (3), thereby completing the verification of the Birch and Swinnerton-Dyer conjecture in the present case.

Acknowledgements

I would like to express my gratitude to Karl Rubin for his guidance and help. I also thank Robert Gold, Cristian Popescu and Warren Sinnott for many helpful conversations, and the referee for several suggestions regarding the presentation.

2. Preliminaries

Let $K = \mathbb{Q}(\sqrt{-7})$, and write $\mathcal{O}$ for the ring of integers of K. Fix a prime $\mathfrak{p}$ of K lying above 2, and let $\bar{\mathfrak{p}}$ denote the complex conjugate of $\mathfrak{p}$. Then $\mathfrak{p} \neq \bar{\mathfrak{p}}$. Now fix an elliptic curve E defined over K with complex multiplication by $\mathcal{O}$.

As explained in the Introduction, to prove Theorem A it suffices to check formula (3) at both primes $\mathfrak{p}$ and $\bar{\mathfrak{p}}$. In fact, we need only check (3) at the prime $\mathfrak{p}$, for after this is done we can certainly repeat the entire argument replacing $\mathfrak{p}$ by $\bar{\mathfrak{p}}$ throughout to obtain a proof of (3) for the prime $\bar{\mathfrak{p}}$.

Now let B denote the set of primes of K where E has bad reduction. The theory of complex multiplication shows that B is never empty. We shall say that E is *exceptional* if E has bad reduction at $\mathfrak{p}$ and good reduction at all other primes, i.e. if $B = \{\mathfrak{p}\}$. (We remark here that there are very few exceptional curves.) As it turns out, it is convenient to prove formula (3) for exceptional and non-exceptional curves separately, so throughout this and the next several sections we will work under the assumption that E is non-exceptional, deferring the study of the exceptional curves to §8.

We now introduce some additional notations. If F is any field, we will write G_F for $\mathrm{Gal}(\bar{F}/F)$, where $\bar{F}$ denotes the algebraic closure of F. Further, if M is an $\mathcal{O}$-module and $\mathfrak{a}$ is an ideal of $\mathcal{O}$, we will write $M_{\mathfrak{a}}$ for the $\mathfrak{a}$-torsion in M and $M_{\mathfrak{a}^\infty}$ for $\bigcup_{n\geq 1} M_{\mathfrak{a}^n}$. There will be two exceptions to this rule: if $\mathfrak{q}$ is a prime of K, $\mathcal{O}_{\mathfrak{q}}$ (resp. $K_{\mathfrak{q}}$) will denote the completion of $\mathcal{O}$ (resp. K) at $\mathfrak{q}$. Also, for convenience, we will write $E_{\mathfrak{a}}$ for $E(\bar{K})_{\mathfrak{a}}$.

Now, for each n with $1 \leq n \leq \infty$, let $K_n = K(E_{\mathfrak{p}^n})$. Further, for any ideal $\mathfrak{a} \subset \mathcal{O}$ set $\mathbf{N}(\mathfrak{a}) = \#(\mathcal{O}/\mathfrak{a})$ and write $K(\mathfrak{a})$ for the ray class field of K modulo $\mathfrak{a}$. The theory of complex multiplication shows that $K(\mathfrak{p}^n) \subset K_n$ for all $n \leq \infty$, where $K(\mathfrak{p}^\infty)$ is defined as $\bigcup_{n\geq 1} K(\mathfrak{p}^n)$.

Lemma 2.1. (i) *If $n \geq 2$, then $E_{/K_n}$ has good reduction at every prime of K_n not lying above $\mathfrak{p}$.*
(ii) $E(K)_{\mathfrak{p}^\infty} = E_{\mathfrak{p}}$.

Proof. For (i), see for example [5] Theorem 2. The proof is a variant of the criterion of Néron-Ogg-Shafarevich, using the facts that E has potential good reduction everywhere and $\mathrm{Gal}(K_\infty/K_n) \subset 1 + \mathfrak{p}^n\mathcal{O}_{\mathfrak{p}}$ is torsion-free if $n \geq 2$. To prove (ii) we note first that $\#E_{\mathfrak{p}} = \mathbf{N}(\mathfrak{p}) = 2$, so G_K acts trivially on $E_{\mathfrak{p}}$.Thus $E_{\mathfrak{p}} \subset E(K)$. Now if we had $E_{\mathfrak{p}^2} \subset E(K)$, then (i) would show that E is an exceptional curve, contravening our hypothesis. □

Remark. For each result in this section which depends on the choice of $\mathfrak{p}$, there is a corresponding result with the prime $\mathfrak{p}$ replaced by $\bar{\mathfrak{p}}$, provided $B \neq \{\bar{\mathfrak{p}}\}$. We will make use of this fact at various places below.

Lemma 2.2. (i) *Every prime in $B - \{\mathfrak{p}\}$ is ramified in K_2/K.*
(ii) *If $2 \leq n \leq \infty$, then* $[K_n : K(\mathfrak{p}^n)] = \#\mathcal{O}^\times = 2$.

Proof. For (i) see [22], Corollary 2 of Theorem 2 (note that the set $B - \{\mathfrak{p}\}$ is non-empty, because E is non-exceptional). As regards assertion (ii), it is shown in [19] (Lemma 21(iv)) that $[K_n : K(\mathfrak{p}^n)] \leq \#\mathcal{O}^\times = 2$ for all $n < \infty$. On the other hand (i) shows that $K_n \not\subset K(\mathfrak{p}^\infty)$ for all $n \geq 2$, and (ii) follows. □

Let $\mathcal{G} = \mathrm{Gal}(K_\infty/K)$ and define an injective map $\chi_{_E} : \mathcal{G} \to \mathcal{O}_\mathfrak{p}^\times$ by $P^\sigma = \chi_{_E}(\sigma)P$ for all $P \in E_{\mathfrak{p}^\infty}$ and all $\sigma \in \mathcal{G}$.

Proposition 2.3. *The map* $\chi_{_E}$ *is an isomorphism.*

Proof. The theory of complex multiplication shows that $\mathcal{O}^\times \chi_{_E}(\mathcal{G}) = \mathcal{O}_\mathfrak{p}^\times$ (see [23], Theorem 5.4). On the other hand Lemma 2.2(ii) shows that $\mathcal{G}$ contains a subgroup of order 2, namely $\mathrm{Gal}(K_\infty/K(\mathfrak{p}^\infty))$. Consequently $\{\pm 1\} = \mathcal{O}^\times \subset \chi_{_E}(\mathcal{G})$, which completes the proof. □

Define $\tau = \chi_{_E}^{-1}(-1)$, i.e. τ is that element of $\mathcal{G}$ which acts as multiplication by -1 on $E_{\mathfrak{p}^\infty}$. Now let $\langle\tau\rangle$ be the cyclic group generated by τ.

Corollary 2.4. (i) $\mathrm{Gal}(K_\infty/K(\mathfrak{p}^\infty)) = \langle\tau\rangle$.
(ii) $\mathrm{Gal}(K_2/K)$ *is cyclic, generated by the restriction of* τ *to* K_2.

Proof. Assertion (i) follows from the proof of Proposition 2.3. Now by Proposition 2.3, $\chi_{_E}$ induces an isomorphism $\mathrm{Gal}(K_2/K) \simeq \mathcal{O}_\mathfrak{p}^\times/(1+\mathfrak{p}^2\mathcal{O}_\mathfrak{p})$. Noting that $\mathcal{O}_\mathfrak{p}^\times = 1+\mathfrak{p}\mathcal{O}_\mathfrak{p} = \{\pm 1\} \times (1+\mathfrak{p}^2\mathcal{O}_\mathfrak{p})$, (ii) follows at once. □

Lemma 2.5. *Suppose* $\mathfrak{q} \in B - \{\mathfrak{p}\}$*. Then:*
(i) *The inertia group of* $\mathfrak{q}$ *in* K_∞/K *is* $\langle\tau\rangle$.
(ii) $E(K_\mathfrak{q})_{\mathfrak{p}^\infty} = E_\mathfrak{p}$.

Proof. By Lemma 2.2(i), $\mathfrak{q}$ ramifies in K_∞/K. Further $\mathfrak{q} \neq \mathfrak{p}$, so (i) follows from Corollary 2.4(i). Now if $E(K_\mathfrak{q})_{\mathfrak{p}^\infty} = E_{\mathfrak{p}^j}$, then $\mathfrak{q}$ splits completely in K_j/K. But $\mathfrak{q}$ ramifies in K_2/K (Lemma 2.2(i)), so $j \leq 1$. Since $j \geq 1$ by Lemma 2.1(ii), the proof is complete. □

For each $\mathfrak{q} \in B$ let

$$c_\mathfrak{q} = [E(K_\mathfrak{q}) : E_0(K_\mathfrak{q})],$$

where $E_0(K_\mathfrak{q})$ is the subgroup of $E(K_\mathfrak{q})$ of points with non-singular reduction modulo $\mathfrak{q}$.

Proposition 2.6. *For every* $\mathfrak{q} \in B$, $c_\mathfrak{q} = 4$.

Proof. If $\mathfrak{q} \in B$ and $\mathfrak{q} \nmid 2$, then $c_\mathfrak{q} = \#E(K_\mathfrak{q})_2$ ([14], Proposition 4.9). Thus by Lemma 2.5(ii) and its analogue for $\bar{\mathfrak{p}}$ (see the remark following the proof of Lemma 2.1), we have $c_\mathfrak{q} = 4$ for such $\mathfrak{q}$. It remains to show that $c_\mathfrak{p} = 4$ if $\mathfrak{p} \in B$ (the equality $c_{\bar{\mathfrak{p}}} = 4$ when $\bar{\mathfrak{p}} \in B$ is proved similarly).

It is shown in [14] (proof of Proposition 4.5) that the only possible Kodaira types for E over $K_\mathfrak{p}$ are I_ν^* (in which case $c_\mathfrak{p} = 4$), II and II* (which have $c_\mathfrak{p} = 1$, i.e. $E(K_\mathfrak{p}) = E_0(K_\mathfrak{p})$). To see that the last two types cannot occur, simply note that $E_0(K_\mathfrak{p})$ is $\bar{\mathfrak{p}}$-divisible (cf. [25]) but $E(K_\mathfrak{p})$ is not, by the analogue of Lemma 2.5(ii) for $\bar{\mathfrak{p}}$. □

We devote the remainder of this section to proving a number of results on the Galois cohomology of E.

If F is any field, we will write $H^1(F, E)$ for $H^1(G_F, E(\bar{F}))$.

Let $\Gamma = \mathrm{Gal}(K_\infty/K_2)$. Then by Proposition 2.3, $\Gamma \simeq 1+\mathfrak{p}^2\mathcal{O}_\mathfrak{p} \simeq \mathbb{Z}_2$.

Lemma 2.7. (i) *The restriction map induces an isomorphism*

$$H^1(K_2, E_{\mathfrak{p}^\infty}) \simeq H^1(K_\infty,\, E_{\mathfrak{p}^\infty})^\Gamma.$$

(ii) $\# H^1(\mathcal{G},\, E_{\mathfrak{p}^\infty}) = \# E(K)_{\mathfrak{p}^\infty}$.

Proof. A standard calculation shows that $H^i(\Gamma, E_{\mathfrak{p}^\infty}) = 0$ for all $i \geq 1$ (cf. Lemma 6 of [4]). This fact together with the appropriate inflation-restriction exact sequences gives (i), and shows in addition that

$$H^1(\mathcal{G},\, E_{\mathfrak{p}^\infty}) \simeq H^1(G_2,\, E_{\mathfrak{p}^2}),$$

where $G_2 = \mathrm{Gal}(K_2/K)$. Now using Corollary 2.4(ii) and Lemma 2.1(ii), we have

$$H^1(G_2,\, E_{\mathfrak{p}^2}) \simeq E_{\mathfrak{p}^2}/2E_{\mathfrak{p}^2} \simeq E_{\mathfrak{p}} = E(K)_{\mathfrak{p}^\infty}.$$

□

If $\mathfrak{Q}$ is a prime of K_∞ and $n < \infty$, we will write $K_{n,\,\mathfrak{Q}}$ for the completion of K_n at the prime below $\mathfrak{Q}$. Now let $K_{\infty,\,\mathfrak{Q}} = \bigcup_{n\geq 1} K_{n,\,\mathfrak{Q}}$.

Lemma 2.8. *Let $\mathfrak{Q}$ be a prime of K_∞ and let $\mathfrak{q}$ be the prime of K lying below $\mathfrak{Q}$. Then, if $\mathfrak{q} \notin B \cup \{\mathfrak{p}\}$,*

$$H^1(\mathrm{Gal}(K_{\infty,\,\mathfrak{Q}}/K_{\mathfrak{q}}), E(K_{\infty,\,\mathfrak{Q}})) = 0.$$

Proof. This is well-known, coming from the facts that E has good reduction over $K_{\mathfrak{q}}$ and $K_{\infty,\,\mathfrak{Q}}/K_{\mathfrak{q}}$ is unramified. See for example [17], Corollary 4.4. □

Lemma 2.9. *Let $\mathfrak{Q}$ be a prime of K_∞ and let $\mathfrak{q}$ be the prime of K lying below $\mathfrak{Q}$. Then, if $\mathfrak{q} \in B$ and $\mathfrak{q} \nmid 2$,*

$$\# H^1(\mathrm{Gal}(K_{\infty,\,\mathfrak{Q}}/K_{\mathfrak{q}}), E(K_{\infty,\,\mathfrak{Q}}))_{\mathfrak{p}^\infty} = \# E(K_{\mathfrak{q}})_{\bar{\mathfrak{p}}^\infty}.$$

Proof. E has good reduction over $K_{2,\,\mathfrak{Q}}$ by Lemma 2.1(i) , so $K_{\infty,\,\mathfrak{Q}}/K_{2,\,\mathfrak{Q}}$ is unramified (see [24], §VII.4). Thus by an analogue of Lemma 2.8 and the usual inflation-restriction exact sequence, there is an isomorphism

$$H^1(\mathrm{Gal}(K_{\infty,\,\mathfrak{Q}}/K_{\mathfrak{q}}), E(K_{\infty,\,\mathfrak{Q}})) \simeq H^1(G_{2,\,\mathfrak{Q}}, E(K_{2,\,\mathfrak{Q}})),$$

where $G_{2,\,\mathfrak{Q}} = \mathrm{Gal}(K_{2,\,\mathfrak{Q}}/K_{\mathfrak{q}})$. Now since $\mathfrak{Q} \nmid \mathfrak{p}$ there is a decomposition $E(K_{2,\,\mathfrak{Q}}) \simeq E(K_{2,\,\mathfrak{Q}})_{\mathfrak{p}^\infty} \oplus A$, where A is a uniquely $\mathfrak{p}$-divisible $\mathcal{O}[G_{2,\,\mathfrak{Q}}]$-module (see §VII.6.3 of [24]). It follows that

$$H^1(G_{2,\,\mathfrak{Q}}, E(K_{2,\,\mathfrak{Q}}))_{\mathfrak{p}^\infty} \simeq H^1(G_{2,\,\mathfrak{Q}}, E(K_{2,\,\mathfrak{Q}})_{\mathfrak{p}^\infty}).$$

Now since the quadratic extension K_2/K is ramified at $\mathfrak{q}$ (see Corollary 2.4(ii) and Lemma 2.2(i)), we have $G_{2,\,\mathfrak{Q}} \simeq \mathrm{Gal}(K_2/K)$, whence $H^1(G_{2,\,\mathfrak{Q}}, E(K_{2,\,\mathfrak{Q}})_{\mathfrak{p}^\infty}) \simeq E_{\mathfrak{p}}$ (cf. the proof of Lemma 2.7). Finally, using the analogue of Lemma 2.5(ii) for $\bar{\mathfrak{p}}$, we have $\# E_{\mathfrak{p}} = \# E_{\bar{\mathfrak{p}}} = \# E(K_{\mathfrak{q}})_{\bar{\mathfrak{p}}^\infty}$, and the lemma follows. □

Lemma 2.10. *Suppose $\bar{\mathfrak{p}} \in B$. Then there is a unique prime of K_∞ lying above $\bar{\mathfrak{p}}$.*

Proof. We must show that the unique prime of K_2 lying above $\bar{\mathfrak{p}}$, say $\bar{\wp}$, is inert in K_∞/K_2. To this end let $m \leq \infty$ be such that $\bar{\wp}$ splits completely in K_m/K_2, so $E_{\mathfrak{p}^m} \subset E(K_{2,\,\bar{\wp}})$. Since $\bar{\wp} \nmid \mathfrak{p}$ the reduction-modulo-$\bar{\wp}$ map sends $E_{\mathfrak{p}^m}$ injectively into $\widetilde{E}(\mathcal{O}/\bar{\mathfrak{p}})$, where $\widetilde{E}$ denotes the reduction of E modulo $\bar{\wp}$. As $\#\widetilde{E}(\mathcal{O}/\bar{\mathfrak{p}}) \leq 5$, we conclude that $m = 2$, which proves the lemma. □

3. The infinite descent

In this section we prove formula (5) of the Introduction.

Keep the notation and assumptions of §2. In addition, assume that our elliptic curve E satisfies $L(E_{/K},1) \neq 0$. In this case the finiteness of $E(K)$ and of the Tate-Shafarevich group of E over K have been demonstrated by Coates and Wiles [5] and Rubin [20], respectively.

Let $Ш_{\mathfrak{p}^\infty}$ and S denote, respectively, the $\mathfrak{p}$-power torsion in the Tate-Shafarevich group of E over K and the direct limit of the Selmer groups of E relative to powers of $\mathfrak{p}$. Thus

$$Ш_{\mathfrak{p}^\infty} = \ker\left[H^1(K,E)_{\mathfrak{p}^\infty} \to \bigoplus_{\mathfrak{q}} H^1(K_{\mathfrak{q}},E)_{\mathfrak{p}^\infty}\right]$$

and

$$S = \ker\left[H^1(K,E_{\mathfrak{p}^\infty}) \to \bigoplus_{\mathfrak{q}} H^1(K_{\mathfrak{q}},E)_{\mathfrak{p}^\infty}\right].$$

We note that the $\mathfrak{q}$-component $\lambda_{\mathfrak{q}} : H^1(K,E_{\mathfrak{p}^\infty}) \to H^1(K_{\mathfrak{q}},E)_{\mathfrak{p}^\infty}$ of the map appearing in the definition of S is the restriction homomorphism to $H^1(K_{\mathfrak{q}},E_{\mathfrak{p}^\infty})$ followed by the canonical map from this group to $H^1(K_{\mathfrak{q}},E)_{\mathfrak{p}^\infty}$.

Lemma 3.1. *There is an isomorphism*

$$Ш_{\mathfrak{p}^\infty} \simeq S.$$

Proof. Galois cohomology gives us an exact sequence

$$0 \to E(K) \otimes_{\mathcal{O}} (K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}) \to S \to Ш_{\mathfrak{p}^\infty} \to 0.$$

See §1 of [20]. Since $E(K)$ is finite, the group on the left is zero, which gives the lemma. □

Recall the set B of primes of K where E has bad reduction. Let $B' = B \cup \{\mathfrak{p}\}$, and define a modified Selmer group $S(B') \supset S$ by

$$S(B') = \ker\left[H^1(K,E_{\mathfrak{p}^\infty}) \to \bigoplus_{\mathfrak{q}\notin B'} H^1(K_{\mathfrak{q}},E)_{\mathfrak{p}^\infty}\right].$$

There is a natural exact sequence

$$0 \to S \to S(B') \xrightarrow{\lambda_{B'}} \bigoplus_{\mathfrak{q}\in B'} H^1(K_{\mathfrak{q}},E)_{\mathfrak{p}^\infty}, \tag{6}$$

where $\lambda_{B'}$ is the restriction of $\bigoplus_{\mathfrak{q}\in B'} \lambda_{\mathfrak{q}}$ to $S(B')$. The image of $\lambda_{B'}$ has been described by Bashmakov [1] in terms of the local Tate pairing, and we now proceed to state his result.

For any field $F \supset K$ let $E^*(F) = \varprojlim E(F)/\bar{\mathfrak{p}}^n E(F)$, where the inverse limit is taken with respect to the natural maps. Note that $E^*(K) = E(K)_{\bar{\mathfrak{p}}^\infty}$ injects into $E^*(K_{\mathfrak{q}})$ for any prime $\mathfrak{q}$. Now for each $\mathfrak{q} \in B'$ write $\langle\ ,\ \rangle_{\mathfrak{q}}$ for the non-degenerate pairing $E^*(K_{\mathfrak{q}}) \times H^1(K_{\mathfrak{q}},E)_{\mathfrak{p}^\infty} \to \mathbb{Q}/\mathbb{Z}$ which is induced by the Tate pairing.

Theorem 3.2. (Bashmakov) *Suppose $Ш_{\bar{\mathfrak{p}}^\infty}$ is finite. Then a necessary and sufficient condition for an element $(\xi_{\mathfrak{q}}) \in \bigoplus_{\mathfrak{q}\in B'} H^1(K_{\mathfrak{q}},E)_{\mathfrak{p}^\infty}$ to be in the image of*

$\lambda_{B'}$ is that

$$\sum_{\mathfrak{q}\in B'} \langle x, \xi_{\mathfrak{q}}\rangle_{\mathfrak{q}} = 0$$

for every $x \in E(K)_{\bar{\mathfrak{p}}^\infty}$. In particular,

$$\#\mathrm{coker}(\lambda_{B'}) = \#E(K)_{\bar{\mathfrak{p}}^\infty}.$$

Proof. See §3.3 of [1]. □

Viewing $H^1(K_{\mathfrak{p}}, E)_{\mathfrak{p}^\infty}$ as a subgroup of $\bigoplus_{\mathfrak{q}\in B'} H^1(K_{\mathfrak{q}}, E)_{\mathfrak{p}^\infty}$ in a natural way, we have the following:

Corollary 3.3. $H^1(K_{\mathfrak{p}}, E)_{\mathfrak{p}^\infty} \not\subset \mathrm{image}(\lambda_{B'})$.

Proof. This is immediate from Theorem 3.2 and the non-degeneracy of $\langle\ ,\ \rangle_{\mathfrak{p}}$. □

Lemma 3.4. *Suppose $\mathfrak{q} \in B' - \{\bar{\mathfrak{p}}\}$. Then*

$$\#H^1(K_{\mathfrak{q}}, E)_{\mathfrak{p}^\infty} = \#E(K_{\mathfrak{q}})_{\bar{\mathfrak{p}}^\infty}.$$

Proof. The groups $H^1(K_{\mathfrak{q}}, E)_{\mathfrak{p}^\infty}$ and $E^*(K_{\mathfrak{q}})$ are dual to one another under $\langle\ ,\ \rangle_{\mathfrak{q}}$. On the other hand, as $E(K_{\mathfrak{q}}) \simeq E(K_{\mathfrak{q}})_{\mathrm{torsion}} \oplus \mathcal{O}_{\mathfrak{q}}$ (see [24] §VII.6.3) and $\mathfrak{q} \neq \bar{\mathfrak{p}}$, we have $E^*(K_{\mathfrak{q}}) = E(K_{\mathfrak{q}})_{\bar{\mathfrak{p}}^\infty}$, which proves the lemma. □

Remark. The proof of the above lemma shows that $H^1(K_{\bar{\mathfrak{p}}}, E)_{\mathfrak{p}^\infty}$ is infinite, so $S(B')$ is infinite if $\bar{\mathfrak{p}} \in B'$ (see (6) and Theorem 3.2).

Proposition 3.5. *Suppose E has good reduction at $\bar{\mathfrak{p}}$, i.e. $\bar{\mathfrak{p}} \notin B'$. Then*

$$\#S(B') = 2^{b^*} \cdot \#E(K_{\mathfrak{p}})_{\bar{\mathfrak{p}}^\infty} \cdot (\#E(K)_{\bar{\mathfrak{p}}^\infty})^{-1} \cdot \#\text{Ш}_{\mathfrak{p}^\infty},$$

where $b^* = \#(B - \{\mathfrak{p}\})$.

Proof. This follows from (6), Lemma 3.1 and Theorem 3.2, using Lemmas 3.4 and 2.5(ii) (for $\bar{\mathfrak{p}}$) to compute the order of $\bigoplus_{\mathfrak{q}\in B'} H^1(K_{\mathfrak{q}}, E)_{\mathfrak{p}^\infty}$. □

The above result brings us closer to a proof of (5) for those curves which have a good reduction at $\bar{\mathfrak{p}}$. We have yet to relate $S(B')$ to $\mathrm{Hom}(X_\infty, E_{\mathfrak{p}^\infty})^{\mathcal{G}}$, as well as deal with the curves that have a bad reduction at $\bar{\mathfrak{p}}$. To these ends, we now introduce Selmer groups over the field K_∞.

For any set T of primes of K, we write $\widetilde{T}$ for the set of primes of K_∞ which lie above the primes in T, and define

$$S_\infty(T) = \ker\left[H^1(K_\infty, E_{\mathfrak{p}^\infty}) \to \bigoplus_{\mathfrak{Q}\notin\widetilde{T}} H^1(K_{\infty,\mathfrak{Q}}, E)_{\mathfrak{p}^\infty}\right].$$

Now recall $B' = B \cup \{\mathfrak{p}\}$ and set $\mathcal{T} = B' \cap \{\mathfrak{p}, \bar{\mathfrak{p}}\}$. Thus $\mathcal{T} = \{\mathfrak{p}\}$ if E has good reduction at $\bar{\mathfrak{p}}$ and $\mathcal{T} = \{\mathfrak{p}, \bar{\mathfrak{p}}\}$ otherwise. In what follows we shall be concerned with the groups $S_\infty(\mathfrak{p})$ and $S_\infty(\mathcal{T})$. Clearly $S_\infty(\mathcal{T}) \supset S_\infty(\mathfrak{p})$ and $S_\infty(\mathcal{T}) = S_\infty(\mathfrak{p})$ if E has good reduction at $\bar{\mathfrak{p}}$. Recall $\mathcal{G} = \mathrm{Gal}(K_\infty/K)$.

Lemma 3.6. *Let X_∞ denote the Galois group of the maximal abelian 2-extension of K_∞ which is unramified outside of the primes above $\mathfrak{p}$. Then there is a canonical $\mathcal{G}$-isomorphism*

$$S_\infty(\mathfrak{p}) \simeq \mathrm{Hom}(X_\infty, E_{\mathfrak{p}^\infty}).$$

Proof. This is well-known. See for example [4], Theorem 12. □

Now consider the standard inflation-restriction exact sequence

$$0 \to H^1(\mathcal{G}, E_{\mathfrak{p}^\infty}) \to H^1(K, E_{\mathfrak{p}^\infty}) \xrightarrow{\text{Res}} H^1(K_\infty, E_{\mathfrak{p}^\infty})^{\mathcal{G}}. \tag{7}$$

In contrast to the situation prevalent in the case $\mathfrak{p} \nmid 2$, the restriction map Res is neither injective (see Lemma 2.7(ii)) nor surjective. The following result is all we need, however.

Lemma 3.7. $S_\infty(\mathfrak{p})^{\mathcal{G}} \subset \text{image(Res)}$.

Proof. Let $G_2 = \text{Gal}(K_2/K)$, and let $r : H^1(K, E_{\mathfrak{p}^\infty}) \to H^1(K_2, E_{\mathfrak{p}^\infty})^{G_2}$ and $\rho : H^1(K_2, E_{\mathfrak{p}^\infty})^{G_2} \to H^1(K_\infty, E_{\mathfrak{p}^\infty})^{\mathcal{G}}$ be the natural restriction maps. Then ρ is an isomorphism by Lemma 2.7(i), and Res is the composition of r and ρ. Thus to prove the lemma it suffices to check that $\rho^{-1}(S_\infty(\mathfrak{p})^{\mathcal{G}}) \subset \text{image}(r)$. Choose a prime $\mathfrak{q} \in B - \{\mathfrak{p}\}$, fix a prime of $\bar{K}$ lying above $\mathfrak{q}$, and write $I_{\mathfrak{q}}$ for the corresponding inertia group. Now recall the automorphism $\tau \in \mathcal{G}$ which acts as multiplication by -1 on $E_{\mathfrak{p}^\infty}$. Since τ generates the inertia group of $\mathfrak{q}$ in K_∞/K (see Lemma 2.5(i)), we can find an element $\bar{\tau} \in I_{\mathfrak{q}}$ whose restriction to K_∞ is τ. Then $\bar{\tau}^2 \in G_{K_\infty} \cap I_{\mathfrak{q}}$. Now using the fact that the elements of $S_\infty(\mathfrak{p})$ are unramified outside of $\mathfrak{p}$ by Lemma 3.6, it is not difficult to see that every cohomology class $\{\xi\}$ in $\rho^{-1}(S_\infty(\mathfrak{p})^{\mathcal{G}})$ satisfies $\xi(\bar{\tau}^2) = 0$. It is now a simple matter to check that the map $c = c_\xi : G_K \to E_{\mathfrak{p}^\infty}$ given by $c(\sigma\bar{\tau}^i) = \xi(\sigma)$ $(\sigma \in G_{K_2},\ i = 0,\ 1)$ is a 1-cocycle whose cohomology class in $H^1(K, E_{\mathfrak{p}^\infty})$ is mapped to $\{\xi\}$ by r. $\square$

Define $S^*_\infty(\mathcal{T}) = S_\infty(\mathcal{T}) \cap \text{image(Res)}$. The above lemma shows that $S^*_\infty(\mathcal{T}) \supset S_\infty(\mathfrak{p})^{\mathcal{G}}$ and $S^*_\infty(\mathcal{T}) = S_\infty(\mathfrak{p})^{\mathcal{G}}$ if E has good reduction at $\bar{\mathfrak{p}}$ (since $S_\infty(\mathcal{T}) = S_\infty(\mathfrak{p})$ for such curves). Now recall the group $S(B') \subset H^1(K, E_{\mathfrak{p}^\infty})$ defined at the beginning of this section.

Proposition 3.8. *The inflation-restriction exact sequence (7) induces an exact sequence*

$$0 \to H^1(\mathcal{G}, E_{\mathfrak{p}^\infty}) \to S(B') \xrightarrow{\text{Res}} S^*_\infty(\mathcal{T}) \to 0.$$

Proof. That the inflation homomorphism maps $H^1(\mathcal{G}, E_{\mathfrak{p}^\infty})$ into $S(B')$ follows easily from Lemma 2.8. Now for each prime $\mathfrak{Q}$ of K_∞ we have a commutative diagram

$$\begin{array}{ccc} H^1(K, E_{\mathfrak{p}^\infty}) & \xrightarrow{\lambda_{\mathfrak{q}}} & H^1(K_{\mathfrak{q}}, E)_{\mathfrak{p}^\infty} \\ {\scriptstyle\text{Res}}\big\downarrow & & \big\downarrow{\scriptstyle\text{Res}_{\mathfrak{Q}}} \\ H^1(K_\infty, E_{\mathfrak{p}^\infty}) & \xrightarrow{\lambda_{\infty,\mathfrak{Q}}} & H^1(K_{\infty,\mathfrak{Q}}, E)_{\mathfrak{p}^\infty} \end{array}$$

where $\mathfrak{q}$ is the prime of K lying below $\mathfrak{Q}$, $\lambda_{\mathfrak{q}}$ is the localization map defined before the statement of Lemma 3.1, $\lambda_{\infty,\mathfrak{Q}}$ is the analogue of $\lambda_{\mathfrak{q}}$ for the field K_∞, and $\text{Res}_{\mathfrak{Q}}$ is the local restriction map.

If $\mathfrak{Q}$ lies above a prime $\mathfrak{q} \in B' - \mathcal{T} = B - \{\mathfrak{p}, \bar{\mathfrak{p}}\}$, then Lemmas 2.9 and 3.4 show that $\text{Res}_{\mathfrak{Q}}$ is the zero map. If $\mathfrak{Q}|\mathfrak{q}$ with $\mathfrak{q} \notin B'$, then Lemma 2.8 shows that $\text{Res}_{\mathfrak{Q}}$ is injective. Now let $c \in S(B')$. Then, using the above diagram,

$$\lambda_{\infty,\mathfrak{Q}}(\text{Res}(c)) = \text{Res}_{\mathfrak{Q}}(\lambda_{\mathfrak{q}}(c)) = 0$$

if $\mathfrak{q} \notin B'$ (by definition of $S(B')$) or if $\mathfrak{q} \in B' - \mathcal{T}$ (since then $\text{Res}_{\mathfrak{Q}}$ is the zero map). Thus $\text{Res}(S(B')) \subset S^*_\infty(\mathcal{T})$. To prove the reverse inclusion, select an $f \in S^*_\infty(\mathcal{T})$

and find an element $c \in H^1(K, E_{\mathfrak{p}^\infty})$ such that $f = \mathrm{Res}(c)$. Then, for $\mathfrak{Q}|\mathfrak{q}$ with $\mathfrak{q} \notin B'$,

$$\mathrm{Res}_{\mathfrak{Q}}(\lambda_{\mathfrak{q}}(c)) = \lambda_{\infty,\mathfrak{Q}}(f) = 0,$$

whence $\lambda_{\mathfrak{q}}(c) = 0$ because $\mathrm{Res}_{\mathfrak{Q}}$ is injective for such $\mathfrak{Q}$. We conclude that $c \in S(B')$, which completes the proof. $\square$

We are now in a position to prove formula (5) of the Introduction.

Theorem 3.9. *Let* $b^* = \#(B - \{\mathfrak{p}\})$. *Then*

$$\#\mathrm{Hom}(X_\infty, E_{\mathfrak{p}^\infty})^{\mathcal{G}} = 2^{b^*} \cdot \#E(K_{\mathfrak{p}})_{\bar{\mathfrak{p}}^\infty} \cdot (\#E(K)_{2^\infty})^{-1} \cdot \#Ш_{\mathfrak{p}^\infty}.$$

Proof. By Lemmas 3.1 and 3.6, the above formula is equivalent to

$$\#S_\infty(\mathfrak{p})^{\mathcal{G}} = 2^{b^*} \cdot \#E(K_{\mathfrak{p}})_{\bar{\mathfrak{p}}^\infty} \cdot (\#E(K)_{2^\infty})^{-1} \cdot \#S. \tag{8}$$

Case I. E has good reduction at $\bar{\mathfrak{p}}$.

In this case $S_\infty(\mathfrak{p})^{\mathcal{G}} = S_\infty^*(\mathcal{T})$, and Proposition 3.8 yields

$$\#S_\infty(\mathfrak{p})^{\mathcal{G}} = (\#H^1(\mathcal{G}, E_{\mathfrak{p}^\infty}))^{-1} \cdot \#S(B').$$

Formula (8) now follows from Proposition 3.5 and Lemma 2.7(ii).

Case II. E has bad reduction at $\bar{\mathfrak{p}}$.

The argument in this case is more involved, due to the fact that $S(B')$ is infinite (see the remark preceding the statement of Proposition 3.5). To circumvent this difficulty, consider the commutative diagram

$$\begin{array}{ccc}
S(B') & \xrightarrow{\mathrm{Res}} & S_\infty^*(\mathcal{T}) \\
{\scriptstyle\lambda_{B'}}\downarrow & & \downarrow{\scriptstyle\lambda_{\bar{\wp}}} \\
\bigoplus_{\mathfrak{q}\in B'} H^1(K_{\mathfrak{q}}, E)_{\mathfrak{p}^\infty} & \xrightarrow{\varphi} & H^1(K_{\infty,\bar{\wp}}, E)_{\mathfrak{p}^\infty}
\end{array}$$

where $\bar{\wp}$ is the unique prime of K_∞ lying above $\bar{\mathfrak{p}}$ (see Lemma 2.10), $\lambda_{\bar{\wp}}$ is the restriction to $S_\infty^*(\mathcal{T})$ of the natural map $H^1(K_\infty, E_{\mathfrak{p}^\infty}) \to H^1(K_{\infty,\bar{\wp}}, E)_{\mathfrak{p}^\infty}$, and φ is the composition of the projection map $\bigoplus_{\mathfrak{q}\in B'} H^1(K_{\mathfrak{q}}, E)_{\mathfrak{p}^\infty} \to H^1(K_{\bar{\mathfrak{p}}}, E)_{\mathfrak{p}^\infty}$ and the restriction map $H^1(K_{\bar{\mathfrak{p}}}, E)_{\mathfrak{p}^\infty} \to H^1(K_{\infty,\bar{\wp}}, E)_{\mathfrak{p}^\infty}$. By Proposition 3.8, the map Res in the above diagram is surjective with kernel $H^1(\mathcal{G}, E_{\mathfrak{p}^\infty})$, and the definitions together with Lemma 3.7 show that $\ker(\lambda_{B'}) = S$ and $\ker(\lambda_{\bar{\wp}}) = S_\infty(\mathfrak{p})^{\mathcal{G}}$. Applying the snake lemma to the above diagram then yields the formula

$$\#H^1(\mathcal{G}, E_{\mathfrak{p}^\infty}) \cdot \#\mathrm{coker}(\lambda_{B'}) \cdot \#S_\infty(\mathfrak{p})^{\mathcal{G}} = \#\ker(\varphi) \cdot \#\mathrm{image}(\widetilde{\varphi}) \cdot \#S, \tag{9}$$

where $\widetilde{\varphi} : \mathrm{coker}(\lambda_{B'}) \to \mathrm{coker}(\lambda_{\bar{\wp}})$ is the map induced by φ. Now Lemma 2.7(ii) and Theorem 3.2 show that $\#H^1(\mathcal{G}, E_{\mathfrak{p}^\infty}) \cdot \#\mathrm{coker}(\lambda_{B'}) = \#E(K)_{2^\infty}$. On the other hand, the order of

$$\ker(\varphi) = H^1(\mathrm{Gal}(K_{\infty,\bar{\wp}}/K_{\bar{\mathfrak{p}}}), E(K_{\infty,\bar{\wp}}))_{\mathfrak{p}^\infty} \bigoplus \left(\bigoplus_{\mathfrak{q}\in B^\star} H^1(K_{\mathfrak{q}}, E)_{\mathfrak{p}^\infty} \right),$$

where $B^\star = B' - \{\bar{\mathfrak{p}}\}$, may be computed as follows: the proof of Lemma 2.9 shows that $\#H^1(\mathrm{Gal}(K_{\infty,\bar{\wp}}/K_{\bar{\mathfrak{p}}}), E(K_{\infty,\bar{\wp}}))_{\mathfrak{p}^\infty} = \#E_{\mathfrak{p}} = 2$, and Lemmas 3.4 and

2.5(ii) together show that $\#(\bigoplus_{\mathfrak{q}\in B^*} H^1(K_{\mathfrak{q}}, E)_{\mathfrak{p}^\infty}) = 2^{b^*-1} \cdot \#E(K_{\mathfrak{p}})_{\bar{\mathfrak{p}}^\infty}$, where $b^* = \#(B - \{\mathfrak{p}\})$. Thus

$$\#\ker(\varphi) = 2^{b^*} \cdot \#E(K_{\mathfrak{p}})_{\bar{\mathfrak{p}}^\infty}.$$

Finally, we claim that $\widetilde{\varphi}$ is the zero map, so $\#\mathrm{image}(\widetilde{\varphi}) = 1$. To prove our claim, we use the above diagram to obtain the equivalent statement

$$\bigoplus_{\mathfrak{q}\in B'} H^1(K_{\mathfrak{q}}, E)_{\mathfrak{p}^\infty} = \ker(\varphi) + \mathrm{image}(\lambda_{B'}).$$

This must hold since $\#\mathrm{coker}(\lambda_{B'}) = 2$ by Theorem 3.2 and Lemma 2.1(ii), and $\ker(\varphi) \not\subset \mathrm{image}(\lambda_{B'})$ by Corollary 3.3.

Using all of the above in (9) gives (8), thereby completing the proof of the theorem. $\square$

4. The main conjecture: statement and beginning of the proof

Keep the notation of §§2 and 3. Thus E is an elliptic curve defined over K with complex multiplication by the ring of integers $\mathcal{O}$ of K, $\mathfrak{p}$ is a prime of K lying above 2, and $K_n = K(E_{\mathfrak{p}^n})$ for $1 \leq n \leq \infty$. We continue to assume that E is non-exceptional.

We begin this section by defining the elliptic units of K_n that we will use in this paper.

Fix a minimal model of E over K, let L denote the corresponding period lattice, and write $I(6)$ for the set of ideals of $\mathcal{O}$ which are prime to 6. For each $\mathfrak{a} \in I(6)$ define a function

$$\Theta_0(z;\mathfrak{a}) = \eta(\mathfrak{a}) \prod_u (\wp(z;L) - \wp(u;L))^{-1},$$

where $\wp(z;L)$ is the Weierstrass $\wp$-function for the lattice L, the product is taken over representatives of the non-zero classes u in $(\mathfrak{a}^{-1}L/L)/\pm 1$, and $\eta(\mathfrak{a}) \in K$ is the 12-th root of $\Delta(L)^{\mathbf{N}(\mathfrak{a})}/\Delta(\mathfrak{a}^{-1}L)$ constructed by Robert in [18], where Δ is the usual Ramanujan Δ-function. This function Θ_0 is the unique 12-th root of the function $\Theta(z;L,\mathfrak{a})$ used in §II.2 of [8] which satisfies a certain distribution relation. See [18] for more details.

Write $\mathfrak{f}$ for the conductor of the Hecke character of K attached to E, and let $\mathfrak{f}'$ be the least common multiple of the prime-to-$\mathfrak{p}$ part of $\mathfrak{f}$ and $\bar{\mathfrak{p}}^2$ (so $\mathfrak{f}'$ is prime to $\mathfrak{p}$ and $\mathfrak{f}' \nmid 2 = \#\mathcal{O}^\times$). Now, for every $n \leq \infty$, let $F_n = K(E_{\mathfrak{f}'})K_n$. Further, set $\mathfrak{f}_n = \mathfrak{f}'\mathfrak{p}^n$ and fix a point $v \in \mathbb{C}/L$ of order exactly $\mathfrak{f}_n$. Then $\Theta_0(v;\mathfrak{a}) \in K(\mathfrak{f}_n) \subset F_n$ if $(\mathfrak{a}, 6\mathfrak{f}) = 1$ ([18], no. 12), and we let $\mathcal{C}_{\mathfrak{f}_n}$ denote the group generated by all norms $\mathbf{N}_{F_n/K_n}(\Theta_0(v;\mathfrak{a}))$ ($(\mathfrak{a}, 6\mathfrak{f}) = 1$) and by all roots of unity in K_n. Then $\mathcal{C}_{\mathfrak{f}_n}$ is a $\mathbb{Z}[\mathrm{Gal}(K_n/K)]$-submodule of the global units of K_n ([8], §II.2.4) whose definition is independent of the choice of v.

We will also need the elliptic units of conductor $\mathfrak{p}^n$, whose definition we now recall. Choose a point $w \in \mathbb{C}/L$ of order exactly $\mathfrak{p}^n$. Then $\Theta_0(w;\mathfrak{a}) \in K(\mathfrak{p}^n)$ for all $\mathfrak{a} \in I(6)$, and we write $\mathcal{C}_{\mathfrak{p}^n}$ for the group generated by all products $\prod \Theta_0(w;\mathfrak{a})^{m(\mathfrak{a})}$ with $\sum m(\mathfrak{a})(\mathbf{N}(\mathfrak{a}) - 1) = 0$ ($\mathfrak{a} \in I(6)$) and by all roots of unity in $K(\mathfrak{p}^n)$. Then $\mathcal{C}_{\mathfrak{p}^n}$ is a Galois-stable subgroup of the global units of $K(\mathfrak{p}^n)$ whose definition is independent of the choice of w.

We are now ready to define the various Iwasawa modules that enter into the statement of the main conjecture.

Write U_n for the group of local units of $K_n \otimes_K K_{\mathfrak{p}}$ which are congruent to 1 modulo the primes above $\mathfrak{p}$. Let $\bar{\mathcal{C}}_{\mathfrak{f}_n}$ and $\bar{\mathcal{C}}_{\mathfrak{p}^n}$ denote the closures of $\mathcal{C}_{\mathfrak{f}_n} \cap U_n$ and $\mathcal{C}_{\mathfrak{p}^n} \cap U_n$, respectively, in U_n. Define

$$U_\infty = \varprojlim U_n, \;\; \bar{\mathcal{C}}_{\mathfrak{f}'} = \varprojlim \bar{\mathcal{C}}_{\mathfrak{f}_n}, \;\; \bar{\mathcal{C}}_1 = \varprojlim \bar{\mathcal{C}}_{\mathfrak{p}^n} \quad \text{and} \quad \bar{\mathcal{C}}_\infty = \bar{\mathcal{C}}_{\mathfrak{f}'}\, \bar{\mathcal{C}}_1,$$

all inverse limits being taken with respect to the norm maps. Global class field theory gives us a map

$$U_\infty/\bar{\mathcal{C}}_\infty \to X_\infty,$$

where X_∞ denotes, as before, the Galois group of the maximal abelian 2-extension of K_∞ which is unramified outside of the primes above $\mathfrak{p}$.

Now recall $\Gamma = \mathrm{Gal}(K_\infty/K_2) \simeq \mathbb{Z}_2$, and consider the standard Iwasawa algebra

$$\Lambda = \mathbb{Z}_2[[\,\Gamma\,]] = \varprojlim \mathbb{Z}_2[\,\mathrm{Gal}(K_n/K_2)\,],$$

inverse limit over $n \geq 2$. Then X_∞ and $U_\infty/\bar{\mathcal{C}}_\infty$ are finitely generated torsion Λ-modules. See [21].

It follows from the well-known classification theorem for Λ-modules that for every finitely generated torsion Λ-module Y we can find elements $f_i \in \Lambda$ and a finite Λ-module Z such that there is an exact sequence

$$0 \to \bigoplus \Lambda/f_i\Lambda \to Y \to Z \to 0.$$

We will write $\mathrm{char}(Y)$ for the characteristic ideal $(\prod f_i)\Lambda$ of Y.

We can now state the "main conjecture" of Iwasawa theory for the extension K_∞/K (E non-exceptional).

Theorem 4.1. *We have*

$$\mathrm{char}(X_\infty) = \mathrm{char}(U_\infty/\bar{\mathcal{C}}_\infty).$$

We will now show how the proof of Theorem 4.1 reduces to the verification of the equality of the Iwasawa invariants of $U_\infty/\bar{\mathcal{C}}_\infty$ and X_∞.

Write A_n for the 2-primary part of the ideal class group of K_n, let $\mathcal{E}_n$ denote the group of global units of K_n, and write $\bar{\mathcal{E}}_n$ for the closure of $\mathcal{E}_n \cap U_n$ in U_n. Define

$$A_\infty = \varprojlim A_n \quad \text{and} \quad \bar{\mathcal{E}}_\infty = \varprojlim \bar{\mathcal{E}}_n,$$

inverse limits with respect to the norm maps. Global class field theory gives us an exact sequence

$$0 \to \bar{\mathcal{E}}_\infty/\bar{\mathcal{C}}_\infty \to U_\infty/\bar{\mathcal{C}}_\infty \to X_\infty \to A_\infty \to 0. \tag{10}$$

Proposition 4.2. *There is an integer $r \geq 0$ such that*

$$\mathrm{char}(A_\infty) \quad \textit{divides} \quad 2^r\,\mathrm{char}(\bar{\mathcal{E}}_\infty/\bar{\mathcal{C}}_\infty).$$

Proof. This result is similar to a theorem of Rubin ([21], Theorem 8.3) and may be proved using methods analogous to those of §§1, 2 and 8 of [21]. For the details see §3.8 of [11]. □

Corollary 4.3. *There is an integer $r \geq 0$ such that*

$$\mathrm{char}(X_\infty) \quad \textit{divides} \quad 2^r\,\mathrm{char}(U_\infty/\bar{\mathcal{C}}_\infty).$$

Proof. This is immediate from (10) and Proposition 4.2. □

The above corollary shows that in order to prove Theorem 4.1 it is sufficient to verify that X_∞ and $U_\infty/\bar{\mathcal{C}}_\infty$ have the same Iwasawa invariants. This verification is carried out below.

5. The main conjecture: conclusion of the proof

Recall that $\mathfrak{f}$ denotes the conductor of the Hecke character of K attached to E, $\mathfrak{f}'$ is the least common multiple of the prime-to-$\mathfrak{p}$ part of $\mathfrak{f}$ and $\bar{\mathfrak{p}}^2$, and $F_n = K(E_{\mathfrak{f}'})K_n$ for $n \leq \infty$. For each $n < \infty$, let $\mathcal{U}_n$ be the group of local units of $F_n \otimes_K K_{\mathfrak{p}}$ which are congruent to 1 modulo the primes above $\mathfrak{p}$, and define

$$\mathcal{U}(\mathfrak{f}') = \varprojlim \mathcal{U}_n \quad \text{and} \quad V_\infty = \mathbf{N}_{F_\infty/K_\infty}(\mathcal{U}(\mathfrak{f}')) \subset U_\infty,$$

inverse limit with respect to the norm maps. Local class field theory shows that U_∞/V_∞ is finite, so $\operatorname{char}(U_\infty/\bar{\mathcal{C}}_\infty) = \operatorname{char}(V_\infty/\bar{\mathcal{C}}_\infty \cap V_\infty)$.

In this section we will generalize arguments from §III.2 of [8] to prove that the Iwasawa invariants of X_∞ and $V_\infty/(\bar{\mathcal{C}}_\infty \cap V_\infty)$ are equal. As explained above, this will complete the proof of Theorem 4.1.

Recall that $\mathcal{G} = \operatorname{Gal}(K_\infty/K)$, $\Gamma = \operatorname{Gal}(K_\infty/K_2)$ and τ is the element of $\mathcal{G}$ which acts as multiplication by -1 on $E_{\mathfrak{p}^\infty}$. Then $\mathcal{G} = \langle\tau\rangle \times \Gamma$ (see Corollary 2.4(ii)). We now define, for any ideal $\mathfrak{g}$ of $\mathcal{O}$, $K(\mathfrak{g}\mathfrak{p}^\infty) = \bigcup_{n\geq 1} K(\mathfrak{g}\mathfrak{p}^n)$ and $\mathcal{G}(\mathfrak{g}) = \operatorname{Gal}(K(\mathfrak{g}\mathfrak{p}^\infty)/K)$. Using Corollary 2.4(i), we will often identify $\mathcal{G}(1)$ with Γ. Further, it is shown in §II.1.6 of [8] (for example) that $F_\infty = K(\mathfrak{f}'\mathfrak{p}^\infty)$, so $\mathcal{G}$ is a quotient of $\mathcal{G}(\mathfrak{f}')$.

Let $\mathbf{D}$ be the ring of integers of the completion of the maximal unramified extension of $\mathbb{Q}_2$, and let $\operatorname{Res} : \mathbf{D}[[\mathcal{G}(\mathfrak{f}')]] \to \mathbf{D}[[\mathcal{G}]]$ be the map induced by the restriction map $\mathcal{G}(\mathfrak{f}') \to \mathcal{G}$. Define $m(\mathfrak{f}') \in \mathbf{D}[[\Gamma]]$ by the equality

$$(1-\tau)m(\mathfrak{f}') = (1-\tau)\operatorname{Res}(\nu(\mathfrak{f}')),$$

where $\nu(\mathfrak{f}') \in \mathbf{D}[[\mathcal{G}(\mathfrak{f}')]]$ is the 2-adic integral measure constructed in §II.4.12 of [8]. Further, let $\nu(1)$ denote the "pseudo-measure" defined there, so that $(\gamma - 1)\nu(1) \in \mathbf{D}[[\mathcal{G}(1)]]$ for every $\gamma \in \mathcal{G}(1)$. Now fix a topological generator γ_0 of $\Gamma \simeq Z_2$. Then identifying $\mathcal{G}(1)$ with Γ, we define $m(1) = (\gamma_0 - 1)\,\nu(1) \in \mathbf{D}[[\Gamma]]$.

Now recall that if $R = \mathbb{Z}_2$ or $\mathbf{D}$ and $h \in R[[\Gamma]]$, the Iwasawa invariants $\mu(h)$ and $\lambda(h)$ of h are defined as follows: $\mu(h)$ is the largest non-negative integer such that $2^{\mu(h)}$ divides h, and $\lambda(h)$ is the degree of the "distinguished polynomial" part of h given by the Weierstrass preparation theorem. Recall also that $\Lambda = \mathbb{Z}_2[[\Gamma]]$. Let

$$\mathbf{g} = m(\mathfrak{f}')m(1) \in \mathbf{D}[[\Gamma]].$$

Proposition 5.1. *Let $f \in \Lambda$ be any generator of* $\operatorname{char}(X_\infty)$*. Then the Iwasawa invariants of f and $\mathbf{g}$ are equal.*

Proof. This may be proved using straightforward adaptations of arguments from §§III.2.2 – 2.11 of [8]. See §§3.9 and 3.10 of [11] for the details. □

Thus it remains to show that the Iwasawa invariants of $\mathbf{g}$ agree with those of $\operatorname{char}(V_\infty/\bar{\mathcal{C}}_\infty \cap V_\infty)$. In fact, we will show that $\mathbf{g}$ and $\operatorname{char}(V_\infty/\bar{\mathcal{C}}_\infty \cap V_\infty)$ generate the same ideal in $\mathbf{D}[[\Gamma]]$.

For each n with $2 \leq n \leq \infty$, let τ_n denote the restriction of $\tau = \tau_\infty$ to K_n, and write K_n^+ for the fixed field of $\langle\tau_n\rangle$ in K_n.

Proposition 5.2. *For all $n \geq 2$,*

$$K_n^+ = K(\mathfrak{p}^n).$$

Proof. The proposition holds for $n = \infty$ by Corollary 2.4(i), so $K_n^+ = K_n \cap K_\infty^+ \supset K(\mathfrak{p}^n)$ for every n. But $[K_n : K(\mathfrak{p}^n)] = [K_n : K_n^+] = 2$ if $n \geq 2$ by Lemma 2.2(ii), and the proposition follows. □

Recall $V_\infty = \mathbf{N}_{F_\infty/K_\infty}(\mathcal{U}(\mathfrak{f}'))$. Let $i(\mathfrak{f}') : \mathcal{U}(\mathfrak{f}') \to \mathbf{D}[[\mathcal{G}(\mathfrak{f}')]]$ be the injective $\mathcal{G}(\mathfrak{f}')$-homomorphism defined in §§II.4.6 and 4.7 of [8] (which is available to us since $\mathfrak{f}' \not| \#\mathcal{O}^\times = 2$). Since $(1+\tau)V_\infty = \mathbf{N}_{K_\infty/K_\infty^+}(V_\infty)$ and $K_\infty^+ = K(\mathfrak{p}^\infty)$ by the above proposition, we may define, as on p. 100 of [8], maps $i : V_\infty \to \mathbf{D}[[\mathcal{G}]]$ and $j : (1+\tau)V_\infty \to \mathbf{D}[[\mathcal{G}(1)]]$ so that the following diagram commutes:

$$\begin{array}{ccccc}
\mathcal{U}(\mathfrak{f}') & \xrightarrow{\mathbf{N}_{F_\infty/K_\infty}} & V_\infty & \xrightarrow{\mathbf{N}_{K_\infty/K_\infty^+}} & (1+\tau)V_\infty \\
{\scriptstyle i(\mathfrak{f}')}\big\downarrow & & \big\downarrow{\scriptstyle i} & & \big\downarrow{\scriptstyle j} \\
\mathbf{D}[[\mathcal{G}(\mathfrak{f}')]] & \xrightarrow{\mathrm{Res}} & \mathbf{D}[[\mathcal{G}]] & \xrightarrow{\mathrm{Res}^+} & \mathbf{D}[[\mathcal{G}(1)]]
\end{array}$$

where Res is as defined above and Res^+ is the obvious analogue of Res. Once again identifying $\mathcal{G}(1)$ with Γ, we may view j as a map from $(1+\tau)V_\infty$ into $\mathbf{D}[[\Gamma]]$.

For any $\mathbb{Z}_2$-module M, we will write $M \widehat{\otimes}_{\mathbb{Z}_2} \mathbf{D}$ for the completion of $M \otimes_{\mathbb{Z}_2} \mathbf{D}$. Now recall the Iwasawa modules $\bar{\mathcal{C}}_{\mathfrak{f}'}$ and $\bar{\mathcal{C}}_1$ defined in the preceding section.

Proposition 5.3. (i) *The map i induces an isomorphism of* $\mathbf{D}[[\Gamma]]$*-modules*

$$\{(1-\tau)V_\infty/(1-\tau)\bar{\mathcal{C}}_{\mathfrak{f}'}\} \widehat{\otimes}_{\mathbb{Z}_2} \mathbf{D} \simeq \mathcal{A}/m(\mathfrak{f}')\mathcal{B}$$

where $\mathcal{A}$ and $\mathcal{B}$ are ideals of height 2 in $\mathbf{D}[[\Gamma]]$.
(ii) *The map j embeds $(1+\tau)V_\infty \widehat{\otimes}_{\mathbb{Z}_2} \mathbf{D}$ in $\mathbf{D}[[\Gamma]]$ as an ideal of height 2. Under this embedding,*

$$\{(1+\tau)V_\infty \cap \bar{\mathcal{C}}_1\} \widehat{\otimes}_{\mathbb{Z}_2} \mathbf{D} \subset m(1)\mathbf{D}[[\Gamma]].$$

Prof. Both parts of the proposition follow from direct analogues of Propositions III.1.3 and 1.4 of [8]. See [11], §3.10. □

Corollary 5.4. *We have*

$$\mathrm{char}((1-\tau)V_\infty/(1-\tau)\ \bar{\mathcal{C}}_{\mathfrak{f}'})\ \mathbf{D}[[\Gamma]] = m(\mathfrak{f}')\ \mathbf{D}[[\Gamma]].$$

Proof. This is immediate from part (i) of the above proposition. □

We will show next that $m(1)$ is a unit of $\mathbf{D}[[\Gamma]]$ and that the characteristic ideal appearing in the statement of the above corollary is equal to $\mathrm{char}(V_\infty/\bar{\mathcal{C}}_\infty \cap V_\infty)$. These facts and the equality of the corollary will show that $\mathrm{char}(V_\infty/\bar{\mathcal{C}}_\infty \cap V_\infty)$ and $\mathbf{g} = m(\mathfrak{f}')m(1)$ generate the same ideal in $\mathbf{D}[[\Gamma]]$, thereby completing the proof of the main conjecture.

Recall that $\mathrm{Gal}(K(\mathfrak{p}^\infty)/K) = \mathcal{G}(1) \simeq \Gamma \simeq \mathbb{Z}_2$.

Lemma 5.5. *The class number of K_n^+ is odd for all $n < \infty$.*

Proof. Since $K_\infty^+ = K(\mathfrak{p}^\infty)$ by Proposition 5.2, K_∞^+/K is a $\mathbb{Z}_2$-extension in which only $\mathfrak{p}$ ramifies, and this prime is totally ramified since K has class number 1. The lemma is thus a special case of a well-known result. See [26], Theorem 13.22. □

For every $n \le \infty$ and any $\mathrm{Gal}(K_n/K)$-module Y, we will write Y^+ for the submodule of Y of all elements fixed by τ_n. Now recall the Iwasawa module of global units $\bar{\mathcal{E}}_\infty = \varprojlim \bar{\mathcal{E}}_n$.

Lemma 5.6. *We have*

$$\bar{\mathcal{C}}_1 = \bar{\mathcal{E}}_\infty^+.$$

Proof. Fix an n with $2 \leq n < \infty$. Noting that $K(\mathfrak{p}^n) = K_n^+$ is a cyclic extension of K, one can easily see that the group of elliptic units of $K(\mathfrak{p}^n)$ defined by Gillard in §6 of [10] agrees with our group $\mathcal{C}_{\mathfrak{p}^n}$. Then Théorème 5 of [10] gives

$$[\mathcal{E}_n^+ : \mathcal{C}_{\mathfrak{p}^n}] = h(K_n^+),$$

where $h(K_n^+)$ is the class number of K_n^+. Since $h(K_n^+)$ is odd by Lemma 5.5 and the $\mathfrak{p}$-adic analogue of Leopoldt's conjecture is true for K_n, we conclude that

$$\bar{\mathcal{C}}_{\mathfrak{p}^n} = \mathcal{C}_{\mathfrak{p}^n} \otimes \mathbb{Z}_2 = \mathcal{E}_n^+ \otimes \mathbb{Z}_2 = \bar{\mathcal{E}}_n^+.$$

Since $\bar{\mathcal{C}}_1 = \varprojlim \bar{\mathcal{C}}_{\mathfrak{p}^n}$, the lemma follows. □

Write $M(K_\infty^+)$ for the maximal abelian 2-extension of K_∞^+ which is unramified outside of the prime above $\mathfrak{p}$, and let $X(K_\infty^+) = \mathrm{Gal}(M(K_\infty^+)/K_\infty^+)$.

Lemma 5.7. (i) $X(K_\infty^+) = 0$.
(ii) $\bar{\mathcal{E}}_\infty^+ = U_\infty^+$.

Proof. (ii) is immediate from (i) and the inclusion $U_\infty^+/\bar{\mathcal{E}}_\infty^+ \subset X(K_\infty^+)$ of global class field theory. Now set $\mathcal{G}^+ = \mathrm{Gal}(K_\infty^+/K)$ and write $I(\mathcal{G}^+)$ for the augmentation ideal of $\mathbb{Z}_2[[\mathcal{G}^+]]$. Then

$$X(K_\infty^+)/I(\mathcal{G}^+)X(K_\infty^+) = \mathrm{Gal}(M_1/K_\infty^+),$$

where M_1 is the maximal abelian extension of K in $M(K_\infty^+)$. But $K_\infty^+ = K(\mathfrak{p}^\infty)$ is the maximal abelian 2-extension of K which is unramified outside of $\{\mathfrak{p}\}$, so $M_1 = K_\infty^+$ and $X(K_\infty^+)/I(\mathcal{G}^+)X(K_\infty^+) = 0$. Now an application of Nakayama's lemma gives (i). □

Proposition 5.8. (i) $m(1)$ *is a unit of* $\mathbf{D}[[\Gamma]]$.
(ii) $\mathrm{char}((1-\tau)V_\infty/(1-\tau)\,\bar{\mathcal{C}}_{\mathfrak{f}'}) = \mathrm{char}(V_\infty/\bar{\mathcal{C}}_\infty \cap V_\infty)$.

Proof. Lemmas 5.6 and 5.7(ii) show that $\bar{\mathcal{C}}_1 = U_\infty^+$, so $(1+\tau)V_\infty \subset \bar{\mathcal{C}}_1$. Then Proposition 5.3(ii) implies that $m(1)\mathbf{D}[[\Gamma]]$ contains an ideal of height 2, which gives (i). Now $U_\infty^+ \subset \bar{\mathcal{C}}_{\mathfrak{f}'}\bar{\mathcal{C}}_1 = \bar{\mathcal{C}}_\infty$, so the natural map

$$(V_\infty + \bar{\mathcal{C}}_\infty)/\bar{\mathcal{C}}_\infty \longrightarrow (1-\tau)(V_\infty + \bar{\mathcal{C}}_\infty)/(1-\tau)\bar{\mathcal{C}}_\infty$$

is an isomorphism. Noting that $(1-\tau)\bar{\mathcal{C}}_\infty = (1-\tau)\bar{\mathcal{C}}_{\mathfrak{f}'}$, (ii) follows easily. □

It is immediately clear from the above proposition and Corollary 5.4 that $\mathbf{g} = m(\mathfrak{f}')m(1)$ and $\mathrm{char}(V_\infty/\bar{\mathcal{C}}_\infty \cap V_\infty)$ generate the same ideal in $\mathbf{D}[[\Gamma]]$. This concludes the proof of Theorem 4.1.

6. The Birch and Swinnerton-Dyer conjecture over K

In this section we will use the results of §§4 and 5 to relate $\#\mathrm{Hom}(X_\infty, E_{\mathfrak{p}^\infty})^{\mathcal{G}}$ to $L(\bar{\psi}, 1)/\Omega$ when E is non-exceptional. We will then combine this information with the main result of §3 (Theorem 3.9) to establish formula (3) of the Introduction for these curves.

Recall that ψ denotes the Hecke character of K attached to E and $\Omega \in \mathbb{C}^\times$ is a generator of the period lattice of a minimal model of E over K. Also recall that $X_\infty = \mathrm{Gal}(M_\infty/K_\infty)$, where M_∞ is the maximal abelian 2-extension of K_∞ which is unramified outside of the primes above $\mathfrak{p}$.

Let $\kappa : \Gamma \to \mathbb{Z}_2^\times$ denote the character giving the action of Γ on $E_{\mathfrak{p}^\infty}$. If $a, b \in K^\times$, we will write $a \sim b$ to signify that a/b is a unit at $\mathfrak{p}$.

Proposition 6.1. *If* $L(\bar{\psi}, 1) \neq 0$ *then*

$$\#\mathrm{Hom}(X_\infty, E_{\mathfrak{p}^\infty})^\Gamma \sim (1 - \psi(\mathfrak{p})/\mathbf{N}(\mathfrak{p}))\, L(\bar{\psi}, 1)/\Omega.$$

Proof. Arguing as in [21] (proof of Theorem 11.4), the main conjecture (Theorem 4.1 above) implies that for any generator $g \in \Lambda$ of $\mathrm{char}(V_\infty/\bar{\mathcal{C}} \cap V_\infty)$,

$$\#\mathrm{Hom}(X_\infty, E_{\mathfrak{p}^\infty})^\Gamma \sim \kappa(g).$$

Now Theorem II.4.12 of [8], Corollary 5.4 and Proposition 5.8(ii) above show that $\mathrm{char}(V_\infty/\bar{\mathcal{C}} \cap V_\infty)$ has a generator g such that $\kappa(g) = (1 - \psi(\mathfrak{p})/\mathbf{N}(\mathfrak{p}))L(\bar{\psi}, 1)/\Omega$, which gives the proposition. □

Recall that $\mathcal{G} = \langle\tau\rangle \times \Gamma$. Also recall that for any $\mathcal{G}$-module Y, Y^+ denotes the submodule of Y of elements fixed by τ. The next proposition shows that $\mathrm{Hom}(X_\infty, E_{\mathfrak{p}^\infty})^\Gamma = \mathrm{Hom}(X_\infty, E_{\mathfrak{p}^\infty})^{\mathcal{G}}$.

Proposition 6.2. *We have*

$$X_\infty^+ = 0.$$

Proof. We will prove that $X_\infty/(1-\tau)X_\infty$ is finite. This will show that X_∞^+ is finite, hence zero because X_∞ has no non-zero finite submodules (see [12], Proposition 3 and the comments at the end of §4).

Since $X_\infty/(1 - \tau)X_\infty$ is the largest quotient of X_∞ on which τ acts trivially,

$$X_\infty/(1 - \tau)X_\infty = \mathrm{Gal}(L/K_\infty),$$

where L is the maximal extension of K_∞ in M_∞ which is abelian over K_∞^+. We will now show that $\mathrm{Gal}(L/K_\infty^+)$ is finite. By Lemma 5.7(i) there is no non-trivial abelian 2-extension of K_∞^+ which is unramified outside of $\mathfrak{p}$, so

$$\mathrm{Gal}(L/K_\infty^+) = \prod_{v \nmid \mathfrak{p}} I_v,$$

where the product extends over all primes v of K_∞^+ not lying above $\mathfrak{p}$ and I_v is the inertia group of v in $\mathrm{Gal}(L/K_\infty^+)$. Since L/K_∞ is unramified outside of $\mathfrak{p}$, I_v injects into the inertia group of v in $\mathrm{Gal}(K_\infty/K_\infty^+)$ for each $v \nmid \mathfrak{p}$. This inertia group is clearly finite, and non-trivial only when v lies above one of the finitely many primes of K where E has bad reduction. Finally, class field theory shows that the primes of K other than $\mathfrak{p}$ are finitely decomposed in $K_\infty^+ = K(\mathfrak{p}^\infty)$, and the proposition follows. □

Now recall the set B of primes of K where E has bad reduction, and write $b = \#B$ and $b^* = \#(B - \{\mathfrak{p}\})$.

Lemma 6.3. *We have*

$$1 - \psi(\mathfrak{p})/\mathbf{N}(\mathfrak{p}) \sim 2^{b^* - b} \cdot \#E(K_\mathfrak{p})_{\bar{\mathfrak{p}}^\infty}.$$

Proof. When E has good reduction at $\mathfrak{p}$ this follows from Lemma 1 of [4]. If E has bad reduction at $\mathfrak{p}$ then $\psi(\mathfrak{p}) = 0$ and $\#E(K_\mathfrak{p})_{\bar{\mathfrak{p}}^\infty} = 2$ by Lemma 2.5(ii) for $\bar{\mathfrak{p}}$, so the assertion of the lemma is the trivial statement $1 \sim 1$. □

We can now prove formula (3) of the Introduction for non-exceptional curves.

Theorem 6.4. *Suppose E is non-exceptional. Let b denote the number of primes of K where E has bad reduction, and let $\text{Ш}_{\mathfrak{p}^\infty}$ denote the $\mathfrak{p}$-power torsion in the Tate-Shafarevich group of E over K. Then, if $L(\bar{\psi},1)\neq 0$,*

$$L(\bar{\psi},1)/\Omega \sim\ 2^{b}\cdot(\#E(K)_{2^\infty})^{-1}\cdot\#\text{Ш}_{\mathfrak{p}^\infty}.$$

Proof. Propositions 6.1 and 6.2 together with Lemma 6.3 show that

$$2^{b^*-\,b}\cdot\#E(K_{\mathfrak{p}})_{\bar{\mathfrak{p}}^\infty}\cdot L(\bar{\psi},1)/\Omega \sim\ \#\mathrm{Hom}(X_\infty,E_{\mathfrak{p}^\infty})^{\mathcal{G}}.$$

On the other hand, Theorem 3.9 gives

$$\#\mathrm{Hom}(X_\infty,E_{\mathfrak{p}^\infty})^{\mathcal{G}}=2^{b^*}\cdot\#E(K_{\mathfrak{p}})_{\bar{\mathfrak{p}}^\infty}\cdot(\#E(K)_{2^\infty})^{-1}\cdot\#\text{Ш}_{\mathfrak{p}^\infty},$$

which completes the proof. □

7. The conjecture over $\mathbb{Q}$

For any non-zero, square-free integer d, let E^d denote the elliptic curve with equation

$$y^2=x^3+21dx^2+112d^2x,$$

which has discriminant $-2^{12}7^3d^6$. The family of curves E^d is exactly the class of elliptic curves over $\mathbb{Q}$ with complex multiplication by the ring of integers $\mathcal{O}$ of $K=\mathbb{Q}(\sqrt{-7})$ (see [15]). Suppose now that $L(E^d_{/\mathbb{Q}},1)\neq 0$. In this section we will show that Birch and Swinnerton-Dyer's conjectural formula for $L(E^d_{/\mathbb{Q}},1)$ is valid, i.e. we will show that

$$L(E^d_{/\mathbb{Q}},1)=W_d\cdot(\#E^d(\mathbb{Q}))^{-2}\cdot\#\text{Ш}(E^d_{/\mathbb{Q}})\cdot\prod c_p^{(d)} \tag{11}$$

where $c_p^{(d)}=[E^d(\mathbb{Q}_p):E^d_0(\mathbb{Q}_p)]$ is the Tamagawa factor for the rational prime p, W_d is the fundamental real period of E^d, and

$$\text{Ш}(E^d_{/\mathbb{Q}})=\ker\Big[H^1(\mathbb{Q},E^d)\to\bigoplus_v H^1(\mathbb{Q}_v,E^d)\Big],$$

where the sum extends over all places v (including the archimedean one) of $\mathbb{Q}$.

First we note that if d is divisible by 7 the curves E^d and $E^{-d/7}$ are isogenous over $\mathbb{Q}$ (see [13]). Thus E^d and $E^{-d/7}$ have the same L-function. Further, Cassels [3] has shown that the right-hand side of (11) is an isogeny invariant of E^d. From these facts it follows that we need only consider values of d which are prime to 7. We may further assume that d is positive, for if d is prime to 7, then the sign in the functional equation of $L(E^d_{/\mathbb{Q}},s)$ is $d/|d|$ ([13] §19), so $L(E^d_{/\mathbb{Q}},1)=0$ if $d<0$.

So let d be positive and prime to 7, and let $\mathcal{D}_d$ and L^d denote, respectively, the discriminant ideal and period lattice of a minimal model of E^d over $\mathbb{Q}$. Define

$$I_d=\int_0^\infty\frac{dx}{\sqrt{x^3+21dx^2+112d^2x}}.$$

Then $(2^{m_d})^{12}\,\mathcal{D}_d=(-2^{12}7^3d^6)$ with $m_d=0$ or 1, the fundamental real period W_d equals $2^{m_d}I_d$, and (using the fact that $+1$ and -1 are the only roots of unity in $\mathbb{Q}(\sqrt{d})$ since $d>0$)

$$L^d=\left(2^{m_d-m_1}/\sqrt{d}\right)L^1. \tag{12}$$

Lemma 7.1. (i) $W_d = W_{-7d}$.

(ii) *For any* d, $E^d_{/K}$ *has bad reduction at* $\sqrt{-7}$.

(iii) $L^d = W_d \cdot \mathcal{O}$.

Proof. E^{-7d} is the twist of E^d by the non-trivial character of $\mathrm{Gal}(\mathbb{Q}(\sqrt{-7})/\mathbb{Q})$. Thus $\mathcal{D}_d$ and $\mathcal{D}_{-7d}$ differ by a power of (7) (see [7]). In particular $\mathrm{ord}_2(\mathcal{D}_d) = \mathrm{ord}_2(\mathcal{D}_{-7d})$, so $m_d = m_{-7d}$. On the other hand formula 241.00 of [2] shows that $I_{-1} = \sqrt{7}\, I_1$, so $I_d = I_1/\sqrt{d} = I_{-1}/\sqrt{7d} = I_{-7d}$. This proves (i). Assertion (ii) is clear since $\mathrm{ord}_{\sqrt{-7}}(-2^{12}7^3d^6) \not\equiv 0 \pmod{12}$. Finally, (iii) is known to hold for $d = 1$ ([13], p. 82). This fact together with (12) gives (iii) for all $d > 0$. $\square$

Lemma 7.2. *Let* b *denote the number of primes of* K *where* $E^d_{/K}$ *has bad reduction. Then, for all* d,

$$\prod c_p^{(d)} = 2^b.$$

In particular, E^d *and* E^{-7d} *have the same Tamagawa product.*

Proof. An application of Tate's algorithm [25] to compute the $c_p^{(d)}$ terms yields the following: if $E^d_{/\mathbb{Q}}$ has bad reduction at p, then $c_p^{(d)} = 2^{n(p)}$, where $n(p)$ is the number of primes of K lying above p. The first assertion of the lemma now follows easily, using the semi-stable reduction theorem ([24], Proposition VII.5.4) and Lemma 7.1(ii). As to the second, simply note that the K-isomorphic curves E^d and E^{-7d} have the same b. $\square$

Let ψ_d denote the Hecke character of K attached to E^d.

Lemma 7.3. (i) $L(E^d_{/\mathbb{Q}}, s) = L(\psi_d, s) = L(\bar{\psi}_d, s)$.

(ii) *For any* d, $E^d(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ *and* $E^d(K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(iii) $L(\psi_d, 1) > 0$.

Proof. Statement (i) is due to Deuring [9], and (ii) is proved in §14 of [13]. As regards to (iii), Theorem 2 of [16] shows that $L(\psi_d, 1) \geq 0$, whence (iii) follows since $L(\psi_d, 1) \neq 0$ by hypothesis. $\square$

Proposition 7.4. *We have*

$$L(E^d_{/\mathbb{Q}}, 1) = W_d \cdot (\#E^d(\mathbb{Q}))^{-2} \cdot \sqrt{\#\text{Ш}(E^d_{/K})} \cdot \prod c_p^{(d)}.$$

Proof. If B denotes the set of primes of K where $E^d_{/K}$ has bad reduction, then $B \neq \{\mathfrak{p}\}$ by Lemma 7.1(ii). Thus $E^d_{/K}$ in a non-exceptional curve, so formula (3) of the Introduction is valid for the prime $\mathfrak{p}$ (see Theorem 6.4 above). Similarly $B \neq \{\bar{\mathfrak{p}}\}$, so (3) is valid at the prime $\bar{\mathfrak{p}}$ as well (see the comments at the beginning of §2). As explained in the Introduction, this gives Gross' refined Birch and Swinnerton-Dyer formula (4). Now since d is prime to 7, a minimal model of E^d over $\mathbb{Q}$ is also minimal over K, so by Lemma 7.1(iii) we can take $\Omega = W_d$ in (4). Finally, using Lemmas 7.2 and 7.3 in (4) yields the formula of the proposition. $\square$

To complete the proof of (11) we will show that for every rational prime p

$$\#\text{Ш}(E^d_{/K})_{p^\infty} = (\#\text{Ш}(E^d_{/\mathbb{Q}})_{p^\infty})^2. \tag{13}$$

For convenience, we will write $G_{K/\mathbb{Q}}$ for $\mathrm{Gal}(K/\mathbb{Q})$.

Proposition 7.5. *For all d, the restriction map $H^1(\mathbb{Q}, E^d) \to H^1(K, E^d)^{G_{K/\mathbb{Q}}}$ is an isomorphism.*

Proof. A trite calculation based on Lemma 7.3(ii) shows that for all $i \geq 1$,

$$H^i(G_{K/\mathbb{Q}}, E^d(K)) = 0.$$

The lemma now follows easily. $\square$

Proposition 7.6. *For all d, the restriction map $H^1(\mathbb{Q}, E^d) \xrightarrow{\sim} H^1(K, E^d)^{G_{K/\mathbb{Q}}}$ induces an isomorphism*

$$Ш(E^d_{/\mathbb{Q}}) \simeq Ш(E^d_{/K})^{G_{K/\mathbb{Q}}}.$$

Proof. It suffices to check that if v is a place of $\mathbb{Q}$ and w is a place of K lying above v, then the local restriction map $H^1(\mathbb{Q}_v, E^d) \to H^1(K_w, E^d)$ is injective. The kernel of this map is $H^1(\mathrm{Gal}(K_w/\mathbb{Q}_v), E^d(K_w))$, which is clearly zero if $K_w = \mathbb{Q}_v$ or if v is a prime of good reduction for $E^d_{/\mathbb{Q}}$ (since then $v \neq 7$, so $K_w/\mathbb{Q}_v$ is unramified; cf. Lemma 2.8). Suppose now that v is a (finite) prime of bad reduction for $E^d_{/\mathbb{Q}}$ which does not split in $K/\mathbb{Q}$ (hence $v \neq 2$). We will identify $\mathrm{Gal}(K_w/\mathbb{Q}_v)$ with $G_{K/\mathbb{Q}}$.

There is an isomorphism $E^d(K_w) \simeq E^d(K_w)_{2^\infty} \oplus A$, where A is a uniquely 2-divisible $G_{K/\mathbb{Q}}$-module. Further, since $E^d_{/K}$ has bad reduction at w (see Lemma 7.1(ii) and Proposition VII.5.4(a) of [24]), Lemma 2.5(ii) shows that $E^d(K_w)_{2^\infty} = E^d_2$. It follows that there is an isomorphism

$$H^1(G_{K/\mathbb{Q}}, E^d(K_w)) \simeq H^1(G_{K/\mathbb{Q}}, E^d_2).$$

As $H^i(G_{K/\mathbb{Q}}, E^d_2) = 0$ for all $i \geq 1$ by Lemma 7.3(ii), the proof for finite v is complete. If v is the infinite place, the last-mentioned fact shows that the multiplication-by-2 map $H^1(G_{K/\mathbb{Q}}, E^d(\mathbb{C})) \to H^1(G_{K/\mathbb{Q}}, E^d(\mathbb{C}))$ is an isomorphism. But $H^1(G_{K/\mathbb{Q}}, E^d(\mathbb{C}))$ is annihilated by 2, so $H^1(G_{K/\mathbb{Q}}, E^d(\mathbb{C})) = 0$. $\square$

We can now prove formula (13). Let c denote the non-trivial element of $G_{K/\mathbb{Q}}$.

Case I. $p = 2$.

Recall that 2 splits in K as $\mathfrak{p}\bar{\mathfrak{p}}$ with $\bar{\mathfrak{p}} \neq \mathfrak{p}$ ($\bar{\mathfrak{p}} = \mathfrak{p}^c$). We have $\#Ш(E^d_{/K})_{2^\infty} = (\#Ш(E^d_{/K})_{\bar{\mathfrak{p}}^\infty})^2$, and multiplication by $(1+c)$ on $Ш(E^d_{/K})_{\bar{\mathfrak{p}}^\infty}$ induces an isomorphism

$$Ш(E^d_{/K})_{\bar{\mathfrak{p}}^\infty} \simeq Ш(E^d_{/K})_{2^\infty}^{G_{K/\mathbb{Q}}}.$$

Since $Ш(E^d_{/K})_{2^\infty}^{G_{K/\mathbb{Q}}} \simeq Ш(E^d_{/\mathbb{Q}})_{2^\infty}$ by Proposition 7.6, formula (13) for $p = 2$ follows.

Case II. $p \neq 2$.

Writing $Ш(E^d_{/K})^-_{p^\infty}$ for $(1-c)Ш(E^d_{/K})_{p^\infty}$, we have the decomposition

$$Ш(E^d_{/K})_{p^\infty} = Ш(E^d_{/K})_{p^\infty}^{G_{K/\mathbb{Q}}} \oplus Ш(E^d_{/K})^-_{p^\infty}.$$

Now the "minus component" $Ш(E^d_{/K})^-_{p^\infty}$ may be identified with $Ш(E^{-7d}_{/K})_{p^\infty}^{G_{K/\mathbb{Q}}}$ (for if χ denotes the non-trivial character of $G_{K/\mathbb{Q}}$, then E^{-7d} is the twist of E^d by χ and there is a K-isomorphism $\varphi : E^{-7d} \to E^d$ such that $\varphi^\sigma = \chi(\sigma)\varphi$ for all $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$). Therefore, using Proposition 7.6,

$$\#Ш(E^d_{/K})_{p^\infty} = \#Ш(E^d_{/\mathbb{Q}})_{p^\infty} \cdot \#Ш(E^{-7d}_{/\mathbb{Q}})_{p^\infty}.$$

Finally, the $\mathbb{Q}$-isogenous curves E^d and E^{-7d} have the same real period (Lemma 7.1(i)), the same Tamagawa product (Lemma 7.2) and the same number of $\mathbb{Q}$-rational points (Lemma 7.3(ii)). Thus by the result of Cassels referred to above

$$\#\text{Ш}(E^{-7d}_{/\mathbb{Q}})_{p^\infty} = \#\text{Ш}(E^{d}_{/\mathbb{Q}})_{p^\infty}$$

which completes the proof of formula (13), and of conjecture (11).

8. The exceptional curves

Recall that the curve E is called exceptional if E has bad reduction at $\mathfrak{p}$ and good reduction at all other primes. In this section we will check formula (3) of the Introduction for these curves.

As before, write $K_\infty = K(E_{\mathfrak{p}^\infty})$ and $\mathcal{G} = \mathrm{Gal}(K_\infty/K)$. Keep the rest of the notation from §§2–6 as well.

Lemma 8.1. (i) $K_\infty = K(\mathfrak{p}^\infty)$.
(ii) $H^i(\mathcal{G}, E_{\mathfrak{p}^\infty}) = 0$ *for all* $i \geq 1$.

Proof. Since E has good reduction away from $\mathfrak{p}$, the extension K_∞/K is unramified outside of $\mathfrak{p}$. This gives (i). Statement (ii) follows from (i), noting that $\mathcal{G} = \mathrm{Gal}(K(\mathfrak{p}^\infty)/K) \simeq \mathbb{Z}_2$. $\square$

Proposition 8.2. *We have* $\text{Ш}_{\mathfrak{p}^\infty} = 0$.

Proof (notation as in §3). Part (ii) of the above lemma shows that the restriction homomorphism $H^1(K, E_{\mathfrak{p}^\infty}) \to H^1(K_\infty, E_{\mathfrak{p}^\infty})$ maps S (which is isomorphic to $\text{Ш}_{\mathfrak{p}^\infty}$) injectively into $S_\infty(\mathfrak{p})$ (cf. the proof of Proposition 3.8). Now Lemmas 3.6, 8.1(i) and a result analogous to Lemma 5.7(i) (with K_∞^+ replaced by $K(\mathfrak{p}^\infty)$) show that $S_\infty(\mathfrak{p}) = 0$, which completes the proof. $\square$

Recall that if $a, b \in K^\times$ then $a \sim b$ means that a/b is a unit at $\mathfrak{p}$.

Proposition 8.3. *If* $L(\bar{\psi}, 1) \neq 0$, *then*

$$L(\bar{\psi}, 1)/\Omega \sim (\#E(K)_{\mathfrak{p}^\infty})^{-1}.$$

Proof (notation as in §5). Setting $\mathfrak{f}' = \bar{\mathfrak{p}}^2$ in the discussion that precedes the statement of Proposition 5.3, we obtain an injective map $i = j : V_\infty \to \mathbf{D}[[\mathcal{G}]]$, where $V_\infty = \mathbf{N}_{K(\bar{\mathfrak{p}}^2\mathfrak{p}^\infty)/K(\mathfrak{p}^\infty)}(\mathcal{U}(\bar{\mathfrak{p}}^2))$. Then results analogous to Proposition 5.3(ii) (with $(1+\tau)V_\infty$ and Γ replaced by V_∞ and $\mathcal{G}$, respectively) and Lemmas 5.5 to 5.7 (with K_n^+ replaced by $K(\mathfrak{p}^n)$ for every n) hold true. It follows that $m(1)$ is a unit of $\mathbf{D}[[\mathcal{G}]]$, whence Theorem II.4.12 of [8] gives

$$(\kappa(\gamma_0) - 1)L(\bar{\psi}, 1)/\Omega \sim 1,$$

where γ_0 is a topological generator of $\mathcal{G}$ and κ is the character giving the action of $\mathcal{G}$ on $E_{\mathfrak{p}^\infty}$. As $\kappa(\gamma_0) - 1 \sim \#E(K)_{\mathfrak{p}^\infty}$ by definition of κ, the proof is complete. $\square$

We can now verify formula (3) for the exceptional curves. Using Propositions 8.2 and 8.3 and the analogue of Lemma 2.1(ii) for $\bar{\mathfrak{p}}$, we have

$$L(\bar{\psi}, 1)/\Omega \sim (\#E(K)_{\mathfrak{p}^\infty})^{-1} = 2 \cdot (\#E(K)_{2^\infty})^{-1} = 2^b \cdot (\#E(K)_{2^\infty})^{-1}\#\text{Ш}_{\mathfrak{p}^\infty},$$

as desired.

References

[1] M.I. Bashmakov, *The cohomology of abelian varieties over a number field*, Russian Math. Surveys **27 no. 6** (1972), 25-70. MR **53:**2961

[2] P. Byrd and M. Friedman, *Handbook of Elliptic Integrals for Enginners and Scientists*, second ed., Springer-Verlag, 1971. MR **43:**3506

[3] J.W.S. Cassels, *Arithmetic on curves of genus 1 (VIII)*, J. Reine Angew. Math. **217** (1965), 180-189. MR **31:**3420

[4] J. Coates, *Infinite descent on elliptic curves with complex multiplication*, Arithmetic and Geometry, papers dedicated to I.R. Shafarevich on the occasion of his 60^{th} birthday. Prog. Math. **35**, Birkhäuser, 1983, pp. 107-136. MR **85d:**11101

[5] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), 223-251. MR **57:**3134

[6] ———, *Kummer's criterion for Hurwitz numbers*, Alg. Number Theory, Kyoto 1976, Japan Soc. for the Promotion of Science, Tokyo, 1977, pp. 9-23. MR **56:**8537

[7] S. Comalada, *Twists and reduction of an elliptic curve*, J. Number Theory **49** (1994), 45-62. MR **95g:**11047

[8] E. de Shalit, *The Iwasawa Theory of Elliptic Curves with Complex Multiplication*, Perspect. Math. **3**, Academic Press, 1987. MR **89g:**11046

[9] M. Deuring, *Die Zetafunktion einer algebraischen Kurve von Geschlechte Eins, I-IV*, Gott. Nachr. 1953, 85–94; 1955, 13–42; 1956, 37–76; 1957, 55–80. MR **15:**779d; MR **17:**17c; MR **18:**113e; MR **19:**637a

[10] R. Gillard, *Remarques sur les unités cyclotomiques et les unités elliptiques*, J. Number Theory **11** (1979), 21-48. MR **80j:**12004

[11] C.D. Gonzalez-Avilés, *On the "2-part" of the Birch and Swinnerton-Dyer conjecture for elliptic curves with complex multiplication*, Ph.D. thesis, The Ohio State University, 1994.

[12] R. Greenberg, *On the structure of certain Galois groups*, Invent. Math. **47** (1978), 85-99. MR **80b:**12007

[13] B. Gross, *Arithmetic on elliptic curves with complex multiplication*, Lect. Notes in Math. **776**, Springer-Verlag, 1980. MR **81f:**10041

[14] ———, *On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication*, Number Theory related to Fermat's Last Theorem. Prog. Math. **26**, Birkhäuser, 1982, pp. 219-236. MR **84e:**14020

[15] T. Hadano, *Conductor of elliptic curves with complex multiplication and elliptic curves of prime conductor*, Proc. Japan Acad. **51** (1975), 92-95. MR **51:**8124

[16] J. Lehman, *Rational points on elliptic curves with complex multiplication by the ring of integers in* $\mathbb{Q}(\sqrt{-7})$, J. Number Theory **27** (1987), 253-272. MR **89a:**11059

[17] B. Mazur, *Rational points of abelian varietes with values in towers of number fields*, Invent. Math. **18** (1972), 183-266. MR **56:**3020

[18] G. Robert, *Concernant la relation de distribution satisfaite par la fonction φ associeé à un réseau complexe*, Invent. Math. **100** (1990), 231-257. MR **91j:**11049

[19] K. Rubin, *Congruences for special values of L-functions of elliptic curves with complex multiplication*, Invent. Math. **71** (1983), 339-364. MR **84h:**12018

[20] ———, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), 527-560. MR **89a:**11065

[21] ———, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), 25-68. MR **92f:**11151

[22] J-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492-517. MR **38:**4488

[23] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton Univ. Press, 1971. MR **47:**3318

[24] J. Silverman, *The Arithmetic of Elliptic Curves.*, Grad. Texts in Math. **106**, Springer-Verlag, 1986. MR **87g:**11070

[25] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable (IV). Lect. Notes in Math. **476**, Springer-Verlag, 1975, pp. 33-52. MR **52:**13850

[26] L. Washington, *Introduction to Cyclotomic Fields.*, Grad. Texts in Math. **83**, Springer-Verlag, 1982. MR **85g:**11001

Facultad de Ciencias, Universidad de Chile, Casilla 653, Santiago, Chile

E-mail address: `cgonzale@abello.dic.uchile.cl`