ON THE CONJECTURE OF BIRCH AND SWINNERTON-DYER

CRISTIAN D. GONZALEZ-AVILÉS

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 \( \text{Sha}(E/K) \) is finite [20]. Now for each prime \( q \) of \( K \) let \( c_q = [E(K_q) : E_0(K_q)] \), where \( E_0(K_q) \) is the subgroup of \( E(K_q) \) of points with non-singular reduction modulo \( q \). In this work we prove the following theorem.

**Theorem A.** Suppose \( L(E/K, 1) \neq 0 \). Then

\[
L(E/K, 1) = \Omega \cdot (\#E(K))^{-2} \cdot \#\text{Sha}(E/K) \cdot \prod c_q.
\]

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 \( L(E^d/Q, 1) \neq 0 \), then the full Birch and Swinnerton-Dyer conjecture is true for \( E^d/Q \).

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.

©1997 American Mathematical Society

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
The following is a summary of the paper.

Write \( \psi \) 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

\[
L(E/K, s) = L(\psi, s)L(\overline{\psi}, s).
\]

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

\[
L(\overline{\psi}, 1)/\Omega \sim_q 2^b \cdot (\#E(K))^{-1} \cdot \sqrt{\#\text{III}^\infty}.
\]

where \( \sim_q \) means “equal up to a unit of \( K^\times_q \).”

In this paper we prove (2) for the primes \( q \) that divide \( \#O^\times = 2 \). 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

\[
L(\overline{\psi}, 1)/\Omega \sim_p 2^b \cdot (\#E(K)_2)^{-1} \cdot \#\text{III}_p^\infty
\]

for \( p \mid 2 \). It will then follow that Gross’ refinement [14] of the Birch and Swinnerton-Dyer conjecture for \( E \) is true, i.e.

\[
L(\overline{\psi}, 1)/\Omega = \pm 2^b \cdot (\#E(K))^{-1} \cdot \sqrt{\#\text{III}^\infty}.
\]

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

\[
\#\text{Hom}(X_{\infty}, E_{p^\infty})^G = 2^{b^*} \cdot \#E(K_{\overline{p}})_{p^\infty} \cdot (\#E(K)_2^\infty)^{-1} \cdot \#\text{III}_p^\infty,
\]

where \( b^* = #(B-(p)) \), \( X_{\infty} \) is the Galois group of the maximal abelian 2-extension of \( K_{\infty} = K(E_{p^\infty}) \) which is unramified outside of the primes above \( p \), and \( G = \text{Gal}(K_{\infty}/K) \). 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 \( \text{ord}_p(L(\overline{\psi}, 1)/\Omega) \) when \( p \not| 2 \), as an application of the “main conjecture” of Iwasawa theory for \( K \). In this work we prove a main conjecture for the extension \( K_{\infty}/K \) (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

\[
\#\text{Hom}(X_{\infty}, E_{p^\infty})^G \sim_p 2^{b^*-b} \cdot \#E(K_{p^\infty}) \cdot L(\overline{\psi}, 1)/\Omega.
\]

This formula together with (5) yields (3), thereby completing the verification of the Birch and Swinnerton-Dyer conjecture in the present case.
ON THE CONJECTURE OF BIRCH AND SWINNERTON-DYER

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 $O$ for the ring of integers of $K$. Fix a prime $p$ of $K$ lying above 2, and let $\bar{p}$ denote the complex conjugate of $p$. Then $p \neq \bar{p}$. Now fix an elliptic curve $E$ defined over $K$ with complex multiplication by $O$.

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

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 $p$ and good reduction at all other primes, i.e. if $B = \{p\}$. (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 $\text{Gal}(\bar{F}/F)$, where $\bar{F}$ denotes the algebraic closure of $F$. Further, if $M$ is an $O$-module and $a$ is an ideal of $O$, we will write $M_a$ for the $a$-torsion in $M$ and $M_a^\infty$ for $\bigcup_{n \geq 1} M_{a^n}$. There will be two exceptions to this rule: if $q$ is a prime of $K$, $O_q$ (resp. $K_q$) will denote the completion of $O$ (resp. $K$) at $q$. Also, for convenience, we will write $E_a$ for $E(K_q)$.

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

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

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 $\text{Gal}(K_{\infty}/K_n) \subset 1 + p^nO_p$ is torsion-free if $n \geq 2$. To prove (ii) we note first that $\#E_p = N(p) = 2$, so $G_K$ acts trivially on $E_p$. Thus $E_p \subset E(K)$. Now if we had $E_{p^n} \subset E(K)$, 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 $p$, there is a corresponding result with the prime $p$ replaced by $\bar{p}$, provided $B \neq \{\bar{p}\}$. We will make use of this fact at various places below.

Lemma 2.2. (i) Every prime in $B - \{p\}$ is ramified in $K_2/K$.
(ii) If $2 \leq n \leq \infty$, then $[K_n : K(p^n)] = \#O^\times = 2$. 
Proof. For (i) see [22], Corollary 2 of Theorem 2 (note that the set \( B - \{ p \} \) is non-empty, because \( E \) is non-exceptional). As regards assertion (ii), it is shown in [19] (Lemma 21(iv)) that \([K_n : K(p^n)] \leq \#O^x = 2\) for all \( n < \infty\). On the other hand (i) shows that \( K_n \not\subset K(p^\infty)\) for all \( n \geq 2\), and (ii) follows.

Let \( G = \text{Gal}(K_\infty/K) \) and define an injective map \( \chi_E : G \to O^x_p \) by \( P^o = \chi_E(\sigma)P \) for all \( P \in E_p^\infty \) and all \( \sigma \in G \).

**Proposition 2.3.** The map \( \chi_E \) is an isomorphism.

**Proof.** The theory of complex multiplication shows that \( O^x \chi_E(G) = O^x_p \) (see [23], Theorem 5.4). On the other hand Lemma 2.2(ii) shows that \( G \) contains a subgroup of order 2, namely \( \text{Gal}(K_\infty/K(p^\infty)) \). Consequently \( \{ \pm 1 \} = O^x \subset \chi_E(G) \), which completes the proof.

Define \( \tau = \chi_E^{-1}(-1) \), i.e. \( \tau \) is that element of \( G \) which acts as multiplication by \(-1\) on \( E_p^\infty \). Now let \( (\tau) \) be the cyclic group generated by \( \tau \).

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

**Proof.** Assertion (i) follows from the proof of Proposition 2.3. Now by Proposition 2.3, \( \chi_E \) induces an isomorphism \( \text{Gal}(K_2/K) \cong O^x_p/(1 + p^2O_p) \). Noting that \( O^x_p = 1 + pO_p = \{ \pm 1 \} \times (1 + p^2O_p) \), (ii) follows at once.

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

**Proof.** By Lemma 2.2(i), \( q \) ramifies in \( K_\infty/K \). Further \( q \neq p \), so (i) follows from Corollary 2.4(i). Now if \( E(K_q)^{\infty} = E_p \), then \( q \) splits completely in \( K_\infty/K \). But \( q \) 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 \( q \in B \) let

\[ c_q = [E(K_q) : E_0(K_q)] \]

where \( E_0(K_q) \) is the subgroup of \( E(K_q) \) of points with non-singular reduction modulo \( q \).

**Proposition 2.6.** For every \( q \in B \), \( c_q = 4 \).

**Proof.** If \( q \in B \) and \( q \neq 2 \), then \( c_q = \#E(K_q)^2 \) ([14], Proposition 4.9). Thus by Lemma 2.5(ii) and its analogue for \( \overline{p} \) (see the remark following the proof of Lemma 2.1), we have \( c_q = 4 \) for such \( q \). It remains to show that \( c_p = 4 \) if \( p \in B \) (the equality \( c_p = 4 \) when \( \overline{p} \in B \) is proved similarly).

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

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 \( H^1(G_F,E(F)) \).
Let \( \Gamma = \text{Gal}(K_\infty/K_2) \). Then by Proposition 2.3, \( \Gamma \simeq 1 + p^2O_p \simeq \mathbb{Z}_2 \).
Lemma 2.7. (i) The restriction map induces an isomorphism
\[ H^1(K_2, E_p) \simeq H^1(K_\infty, E_p) \Gamma. \]
(ii) \#H^1(G, E_p) = \#E(K)_p.

Proof. A standard calculation shows that \( H^1(\Gamma, E_p) = 0 \) 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
\[ H^1(G, E_p) \simeq H^1(G_2, E_p^2), \]
where \( G_2 = \text{Gal}(K_2/K) \). Now using Corollary 2.4(ii) and Lemma 2.1(ii), we have
\[ H^1(G_2, E_p^2) \simeq E_p^2/2E_p \simeq E_p = E(K)_p. \]

Lemma 2.8. Let \( \Omega \) be a prime of \( K_\infty \) and let \( \mathfrak{q} \) be the prime of \( K \) lying below \( \Omega \).
Then, if \( \mathfrak{q} \notin B \cup \{\mathfrak{p}\} \),
\[ H^1(\text{Gal}(K_\infty, \Omega/K_\mathfrak{q}), E(K_\infty, \Omega)) = 0. \]

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

Lemma 2.9. Let \( \Omega \) be a prime of \( K_\infty \) and let \( \mathfrak{q} \) be the prime of \( K \) lying below \( \Omega \).
Then, if \( \mathfrak{q} \in B \) and \( \mathfrak{q} \notin 2 \),
\[ \#H^1(\text{Gal}(K_\infty, \Omega/K_\mathfrak{q}), E(K_\infty, \Omega)) = \#E(K_\mathfrak{q}). \]

Proof. \( E \) has good reduction over \( K_2, \Omega \) by Lemma 2.1(i), so \( K_\infty, \Omega/K_2, \Omega \) 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
\[ H^1(\text{Gal}(K_\infty, \Omega/K_\mathfrak{q}), E(K_\infty, \Omega)) \simeq H^1(G_2, \Omega, E(K_2, \Omega)), \]
where \( G_2, \Omega = \text{Gal}(K_2, \Omega/K_\mathfrak{q}) \). Now since \( \Omega \notin \mathfrak{p} \) there is a decomposition \( E(K_2, \Omega) \simeq E(K_2, \Omega)_p \simeq A \), where \( A \) is a uniquely \( p \)-divisible \( \mathcal{O}[G_2, \Omega] \)-module (see §VII.6.3 of [24]). It follows that
\[ H^1(G_2, A, E(K_2, \Omega))_p \simeq H^1(G_2, \Omega, E(K_2, \Omega)_p). \]
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 \( G_2, \Omega \simeq \text{Gal}(K_2/K) \), whence \( H^1(G_2, \Omega, E(K_2, \Omega)_p) \simeq E_p \) (cf. the proof of Lemma 2.7). Finally, using the analogue of Lemma 2.5(ii) for \( \mathfrak{p} \), we have \( \#E_p = \#E_{\mathfrak{p}} = \#E(K_\mathfrak{q})_{p^\infty} \), and the lemma follows.

Lemma 2.10. Suppose \( \mathfrak{p} \in B \). Then there is a unique prime of \( K_\infty \) lying above \( \mathfrak{p} \).

Proof. We must show that the unique prime of \( K_2 \) lying above \( \mathfrak{p} \), say \( \bar{\mathfrak{p}} \), is inert in \( K_\infty/K_2 \). To this end let \( m \leq \infty \) be such that \( \bar{\mathfrak{p}} \) splits completely in \( K_m/K_2 \), so \( E_{p^m} \subset E(K_2, \bar{\mathfrak{p}}) \). Since \( \bar{\mathfrak{p}} \notin \mathfrak{p} \) the reduction-modulo-\( \bar{\mathfrak{p}} \) map sends \( E_{p^m} \) injectively into \( E(\mathcal{O}/\bar{\mathfrak{p}}) \), where \( E \) denotes the reduction of \( E \) modulo \( \bar{\mathfrak{p}} \). As \( \#E(\mathcal{O}/\bar{\mathfrak{p}}) \leq 5 \), 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 $\prod_{p} \approx$ and $S$ denote, respectively, the $p$-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 $p$. Thus

$$\prod_{p} \approx = \ker \left[ H^1(K, E)_{p} \approx \to \bigoplus_{q} H^1(K_q, E)_{p} \approx \right]$$

and

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

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

**Lemma 3.1.** There is an isomorphism

$$\prod_{p} \approx \cong S.$$

**Proof.** Galois cohomology gives us an exact sequence

$$0 \to E(K) \otimes_{\mathbb{Q}} (K_p / \mathcal{O}_p) \to S \to \prod_{p} \approx \to 0.$$

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

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

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

There is a natural exact sequence

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

where $\lambda_{B'}$ is the restriction of $\bigoplus_{q \in B} \lambda_q$ 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 $E^*(F) = \lim \ E(F) / \mathfrak{p}^n E(F)$, where the inverse limit is
taken with respect to the natural maps. Note that $E^*(K) = E(K)_{p} \approx$ injects into
$E^*(K_q)$ for any prime $q$. Now for each $q \in B'$ write $\langle , , \rangle_q$ for the non-degenerate
pairing $E^*(K_q) \times H^1(K_q, E)_{p} \Rightarrow \mathbb{Q}/\mathbb{Z}$ which is induced by the Tate pairing.

**Theorem 3.2.** (Bashmakov) Suppose $\prod_{p} \approx$ is finite. Then a necessary and suf-
ficient condition for an element $(\xi_q) \in \bigoplus_{q \in B'} H^1(K_q, E)_{p}$ to be in the image of
\[ \lambda_{B'} \] is that
\[ \sum_{q \in B'} (x, \xi_q)_q = 0 \]
for every \( x \in E(K)_{\overline{p}} \). In particular,
\[ \#\text{coker}(\lambda_{B'}) = \#E(K)_{\overline{p}}. \]

Proof. See \S 3.3 of [1]. \( \square \)

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

**Corollary 3.3.** \( H^1(K_p, E)_{\overline{p}} \not\subset \text{image}(\lambda_{B'}). \)

Proof. This is immediate from Theorem 3.2 and the non-degeneracy of \( \langle \ , \rangle_p \). \( \square \)

**Lemma 3.4.** Suppose \( q \in B' - \{ \overline{p} \} \). Then
\[ \#H^1(K_q, E)_{\overline{p}} = \#E(K_q)_{\overline{p}} \]

Proof. The groups \( H^1(K_q, E)_{\overline{p}} \) and \( E^*(K_q) \) are dual to one another under \( \langle \ , \rangle_q \). On the other hand, as \( E(K_q) \cong E(K_q)_{\text{torsion}} \oplus \mathcal{O}_q \) (see [24] \S VII.6.3) and \( q \not\equiv \overline{p} \), we have \( E^*(K_q) = E(K_q)_{\overline{p}} \), which proves the lemma. \( \square \)

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

**Proposition 3.5.** Suppose \( E \) has good reduction at \( \overline{p} \), i.e. \( \overline{p} \not\in B' \). Then
\[ \#S(B') = 2^{b^*} \cdot \#E(K_{\overline{p}})_{\overline{p}} \cdot (\#E(K_{\overline{p}})_{\overline{p}})^{-1} \cdot \#\Xi_{\overline{p}} \]
where \( b^* = \#(B - \{ \overline{p} \}) \).

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

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

For any set \( T \) of primes of \( K \), we write \( \overline{T} \) for the set of primes of \( K_\infty \) which lie above the primes in \( T \), and define
\[ S_\infty(T) = \ker \left[ H^1(K_\infty, E_{\overline{p}}) \rightarrow \bigoplus_{\overline{\Omega} \not\in \overline{T}} H^1(K_\infty, \overline{\Omega}, E)_{\overline{p}} \right]. \]

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

**Lemma 3.6.** Let \( X_\infty \) denote the Galois group of the maximal abelian 2-extension of \( K_\infty \) which is unramified outside of the primes above \( p \). Then there is a canonical \( \mathcal{G} \)-isomorphism
\[ S_\infty(p) \cong \text{Hom}(X_\infty, E_{\overline{p}}). \]

Proof. This is well-known. See for example [4], Theorem 12. \( \square \)
Now consider the standard inflation-restriction exact sequence
\[ 0 \to H^1(\mathcal{G}, E_{p^\infty}) \to H^1(K, E_{p^\infty}) \xrightarrow{\text{Res}} H^1(K_\infty, E_{p^\infty})^G. \] (7)

In contrast to the situation prevalent in the case \( p \not| 2 \), the restriction map \( \text{Res} \) is neither injective (see Lemma 2.7(ii)) nor surjective. The following result is all we need, however.

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

**Proof.** Let \( G_2 = \text{Gal}(K_2/K) \), and let \( r : H^1(K, E_{p^\infty}) \to H^1(K_2, E_{p^\infty})^G_2 \) and \( \rho : H^1(K_2, E_{p^\infty})^G_2 \to H^1(K_\infty, E_{p^\infty})^G \) be the natural restriction maps. Then \( \rho \) is an isomorphism by Lemma 2.7(i), and \( \text{Res} \) is the composition of \( r \) and \( \rho \). Thus to prove the lemma it suffices to check that \( \rho^{-1}(S_\infty^*(p)^G) \subset \text{image}(r) \). Choose a prime \( q \in B - \{ p \} \), fix a prime of \( \bar{K} \) lying above \( q \), and write \( I_q \) for the corresponding inertia group. Now recall the automorphism \( \tau \in \mathcal{G} \) which acts as multiplication by \(-1\) on \( E_{p^\infty} \). Since \( \tau \) generates the inertia group of \( q \) in \( K_\infty/K \) (see Lemma 2.5(i)), we can find an element \( \bar{\tau} \in I_q \) whose restriction to \( K_\infty \) is \( \tau \). Then \( \bar{\tau}^2 \in G_{K_\infty} \cap I_q \).

Now using the fact that the elements of \( S_\infty^*(p) \) are unramified outside of \( p \) by Lemma 3.6, it is not difficult to see that every cohomology class \( \{ \xi \} \) in \( \rho^{-1}(S_\infty^*(p)^G) \) satisfies \( \xi(\bar{\tau}^2) = 0 \). It is now a simple matter to check that the map \( c = c_\xi : G_K \to E_{p^\infty} \) 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 \( H^1(K, E_{p^\infty}) \) is mapped to \( \{ \xi \} \) by \( r \).

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

**Proposition 3.8.** The inflation-restriction exact sequence (7) induces an exact sequence
\[ 0 \to H^1(\mathcal{G}, E_{p^\infty}) \to S(B') \xrightarrow{\text{Res}} S_\infty^*(T) \to 0. \]

**Proof.** That the inflation homomorphism maps \( H^1(\mathcal{G}, E_{p^\infty}) \) into \( S(B') \) follows easily from Lemma 2.8. Now for each prime \( \Omega \) of \( K_\infty \) we have a commutative diagram
\[
\begin{array}{ccc}
H^1(K, E_{p^\infty}) & \xrightarrow{\lambda_q} & H^1(K_\infty, E_{p^\infty}) \\
\text{Res} & & \downarrow \text{Res}_\Omega \\
H^1(K_\infty, E_{p^\infty}) & \xrightarrow{\lambda_{\infty, \Omega}} & H^1(K_\infty, E_{p^\infty})
\end{array}
\]
where \( q \) is the prime of \( K \) lying below \( \Omega \), \( \lambda_q \) is the localization map defined before the statement of Lemma 3.1, \( \lambda_{\infty, \Omega} \) is the analogue of \( \lambda_q \) for the field \( K_\infty \), and \( \text{Res}_\Omega \) is the local restriction map.

If \( \Omega \) lies above a prime \( \bar{q} \in B' - T = B - \{ p, \bar{p} \} \), then Lemmas 2.9 and 3.4 show that \( \text{Res}_\Omega \) is the zero map. If \( \Omega \) contains \( q \) with \( q \notin B' \), then Lemma 2.8 shows that \( \text{Res}_\Omega \) is injective. Now let \( c \in S(B') \). Then, using the above diagram,
\[ \lambda_{\infty, \Omega}(\text{Res}(c)) = \text{Res}_\Omega(\lambda_q(c)) = 0 \]
if \( q \notin B' \) (by definition of \( S(B') \)) or if \( q \in B' - T \) (since then \( \text{Res}_\Omega \) is the zero map). Thus \( \text{Res}(S(B')) \subset S_\infty^*(T) \). To prove the reverse inclusion, select an \( f \in S_\infty^*(T) \)
and find an element \( c \in H^1(K, E_{p^\infty}) \) such that \( f = \text{Res}(c) \). Then, for \( \mathfrak{q} \mid q \) with \( q \notin B' \),

\[
\text{Res}_\mathfrak{q}(\lambda_\mathfrak{q}(c)) = \lambda_{\infty, \mathfrak{q}}(f) = 0,
\]

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

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

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

\[
\#\text{Hom}(X_\infty, E_{p^\infty}) = 2^{b^*} \cdot \#E(K_p)_{p^\infty} \cdot (\#E(K)_{2^\infty})^{-1} \cdot \#\mathfrak{I}_p.
\]

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

\[
\#S_\infty(p)^G = 2^{b^*} \cdot \#E(K_p)_{p^\infty} \cdot (\#E(K)_{2^\infty})^{-1} \cdot \#S.
\]

**Case I.** \( E \) has good reduction at \( \mathfrak{p} \).

In this case \( S_\infty(p)^G = S_\infty^*(T) \), and Proposition 3.8 yields

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

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

**Case II.** \( E \) has bad reduction at \( \mathfrak{p} \).

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

\[
\begin{array}{ccc}
S(B') & \xrightarrow{\text{Res}} & S_\infty^*(T) \\
\lambda_{B'} \downarrow & & \lambda_{\tilde{\mathfrak{p}}} \\
\bigoplus_{\mathfrak{q} \in B'} H^1(K_\mathfrak{q}, E_{p^\infty}) & \xrightarrow{\varphi} & H^1(K_{\infty, \tilde{\mathfrak{p}}}, E_{p^\infty})
\end{array}
\]

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

(9) \[
\#H^1(G, E_{p^\infty}) \cdot \#\text{coker}(\lambda_{B'}) \cdot \#S_\infty(p)^G = \#\ker(\varphi) \cdot \#\text{image}(\tilde{\varphi}) \cdot \#S,
\]

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

\[
\ker(\varphi) = H^1(\text{Gal}(K_{\infty, \tilde{\mathfrak{p}}}/K_\mathfrak{p}, E(K_{\infty, \tilde{\mathfrak{p}}}))_{p^\infty}) \bigoplus_{\mathfrak{q} \in B^*} H^1(K_\mathfrak{q}, E_{p^\infty}),
\]

where \( B^* = B' - \{ \tilde{\mathfrak{p}} \} \), may be computed as follows: the proof of Lemma 2.9 shows that \( \#H^1(\text{Gal}(K_{\infty, \tilde{\mathfrak{p}}}/K_\mathfrak{p}), E(K_{\infty, \tilde{\mathfrak{p}}}))_{p^\infty} = \#E_p = 2 \), and Lemmas 3.4 and
2.5(ii) together show that \(#(\bigoplus_{q \in B'} H^1(K_q, E)_{p^\infty}) = 2^{b^* - 1} \cdot \#E(K_p)_{p^\infty}\), where \(b^* = #(B - \{p\})\). Thus

\[\#\ker(\varphi) = 2^{b^*} \cdot \#E(K_p)_{p^\infty}.\]

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

\[\bigoplus_{q \in B'} H^1(K_q, E)_{p^\infty} = \ker(\varphi) + \text{image}(\lambda_{B'}).\]

This must hold since \(\#\text{coker}(\lambda_{B'}) = 2\) by Theorem 3.2 and Lemma 2.1(ii), and \(\ker(\varphi) \not\subseteq \text{image}(\lambda_{B'})\) 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 \(K\), \(p\) is a prime of \(K\) lying above 2, and \(K_n = K(E_{p^n})\) 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 \(a \in I(6)\) define a function

\[\Theta_0(z; a) = \eta(a) \prod_u (\varphi(z; L) - \varphi(u; L))^{-1},\]

where \(\varphi(z; L)\) is the Weierstrass \(\varphi\)-function for the lattice \(L\), the product is taken over representatives of the non-zero classes \(u\) in \((a^{-1}L/L)/\pm 1\), and \(\eta(a) \in K\) is the 12-th root of \(\Delta(L)^{N(a)}/\Delta(a^{-1}L)\) constructed by Robert in [18], where \(\Delta\) is the usual Ramanujan \(\Delta\)-function. This function \(\Theta_0\) is the unique 12-th root of the function \(\Theta(z; L, a)\) used in \(\S\)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-\(p\) part of \(\mathfrak{f}\) and \(\mathfrak{p}^2\) (so \(\mathfrak{f}'\) is prime to \(p\) and \(\mathfrak{f}'\mathfrak{f}' = \#\mathcal{O}^\times\)). Now, for every \(n \leq \infty\), let \(F_n = K(E_{\mathfrak{f}'})K_n\). Further, set \(f_n = \mathfrak{f}' \mathfrak{f}^n\) and fix a point \(v \in \mathcal{C}/L\) of order exactly \(f_n\). Then \(\Theta_0(v; a) \in K(f_n) \subset F_n\) if \((a, 6f) = 1\) ([18], no. 12), and we let \(\mathcal{C}_n\) denote the group generated by all norms \(N_{F_n/K_n}(\Theta_0(v; a)) ((a, 6f) = 1)\) and by all roots of unity in \(K_n\). Then \(\mathcal{C}_n\) is a \(\mathbb{Z}[\text{Gal}(K_n/K)]\)-submodule of the global units of \(K_n\) ([8], \(\S\)II.2.4) whose definition is independent of the choice of \(v\).

We will also need the elliptic units of conductor \(p^n\), whose definition we now recall. Choose a point \(w \in \mathcal{C}/L\) of order exactly \(p^n\). Then \(\Theta_0(w; a) \in K(p^n)\) for all \(a \in I(6)\), and we write \(\mathcal{C}_p^n\) for the group generated by all products \(\prod \Theta_0(w; a)^{m(a)}\) with \(\sum m(a)(N(a) - 1) = 0\) (\(a \in I(6)\)) and by all roots of unity in \(K(p^n)\). Then \(\mathcal{C}_p^n\) is a Galois-stable subgroup of the global units of \(K(p^n)\) 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 $K_n \otimes K_p$ which are congruent to 1 modulo the primes above $p$. Let $\bar{C}_{f,n}$ and $\bar{C}_{p,n}$ denote the closures of $C_{f,n} \cap U_n$ and $C_{p,n} \cap U_n$, respectively, in $U_n$. Define

$$U_\infty = \limleftarrow U_n, \quad \bar{C}'_f = \limleftarrow \bar{C}_{f,n}, \quad \bar{C}_1 = \limleftarrow \bar{C}_{p,n} \quad \text{and} \quad \bar{C}_\infty = \bar{C}'_f \bar{C}_1,$$

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

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

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

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

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

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

It follows from the well-known classification theorem for $\Lambda$-modules that for every finitely generated torsion $\Lambda$-module $Y$ we can find elements $f_i \in \Lambda$ and a finite $\Lambda$-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 $\text{char}(Y)$ for the characteristic ideal $(\prod f_i)\Lambda$ of $Y$.

We can now state the “main conjecture” of Iwasawa theory for the extension $K_\infty/K$ ($E$ non-exceptional).

**Theorem 4.1.** We have

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

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

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

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

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

$$0 \to \bar{E}_\infty / \bar{C}_\infty \to U_\infty / \bar{C}_\infty \to X_\infty \to A_\infty \to 0. \quad (10)$$

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

$$\text{char}(A_\infty) \text{ divides } 2^r \text{ char}(\bar{E}_\infty / \bar{C}_\infty).$$

**Proof.** This result is similar to a theorem of Rubin ([21], Theorem 8.3) and may be proved using methods analogous to those of §§2, 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

$$\text{char}(X_\infty) \text{ divides } 2^r \text{ char}(U_\infty / \bar{C}_\infty).$$

**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 $X_\infty$ and $U_\infty / \bar{C}_\infty$ have the same Iwasawa invariants. This verification is carried out below.
5. The main conjecture: conclusion of the proof

Recall that \( f \) denotes the conductor of the Hecke character of \( K \) attached to \( E \), \( f' \) is the least common multiple of the prime-to-\( p \) part of \( f \) and \( \overline{p}^2 \), and \( F_n = K(E_{f'})K_n \) for \( n \leq \infty \). For each \( n < \infty \), let \( U_n \) be the group of local units of \( F_n \otimes K K_p \) which are congruent to 1 modulo the primes above \( p \), and define
\[
U(f') = \varprojlim U_n \quad \text{and} \quad V_\infty = N_{F_\infty/K_\infty}(U(f')) \subset U_\infty,
\]
ineq
inverse limit with respect to the norm maps. Local class field theory shows that \( U_\infty/V_\infty \) is finite, so \( \text{char}(U_\infty/C_\infty) = \text{char}(V_\infty/C_\infty \cap V_\infty) \).

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

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

Let \( D \) be the ring of integers of the completion of the maximal unramified extension of \( \mathbb{Q}_2 \), and let \( \text{Res} : D[[G(f')]] \to D[[G]] \) be the map induced by the restriction map \( G(f') \to G \). Define \( m(f') \in D[[\Gamma]] \) by the equality
\[
(1 - \tau)m(f') = (1 - \tau)\text{Res}(\nu(f')),
\]
ineq
where \( \nu(f') \in D[[G(f')]] \) 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 \((\gamma - 1)\nu(1) \in D[[G(1)]] \) for every \( \gamma \in G(1) \). Now fix a topological generator \( \gamma_0 \) of \( \Gamma \cong \mathbb{Z}_2 \). Then identifying \( G(1) \) with \( \Gamma \), we define \( m(1) = (\gamma_0 - 1)\nu(1) \in D[[\Gamma]] \).

Now recall that if \( R = \mathbb{Z}_2 \) or \( D \) 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
\[
g = m(f')m(1) \in D[[\Gamma]].
\]
ineq

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

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

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

For each \( n \) with \( 2 \leq n \leq \infty \), let \( \tau_n \) 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 \( n \geq 2 \),
\[
K_n^+ = K(p^n).
\]
ineq

**Proof.** The proposition holds for \( n = \infty \) by Corollary 2.4(i), so \( K_n^+ = K_n \cap K_\infty^+ \supset K(p^n) \) for every \( n \). But \( [K_n : K(p^n)] = [K_n : K_n^+] = 2 \) if \( n \geq 2 \) by Lemma 2.2(ii), and the proposition follows. \( \square \)
Recall $V_\infty = N_{F_{\infty}/K_\infty}(U(f'))$. Let $i(f') : U(f') \to D[[G(f')]]$ be the injective $G(f')$-endomorphism defined in §§II.4.6 and 4.7 of [8] (which is available to us since $f' \not\mid \#O_K^\times = 2$). Since $(1 + \tau)V_\infty = N_{K_{\infty}/K_{\infty}}(V_\infty)$ and $K_{\infty}^+ = K(p_{\infty})$ by the above proposition, we may define, as on p. 100 of [8], maps $i : V_\infty \to D[[G]]$ and $j : (1 + \tau)V_\infty \to D[[G(1)]]$ so that the following diagram commutes:

$$
\begin{CD}
U(f') @> N_{F_{\infty}/K_{\infty}} >> V_\infty @> N_{K_{\infty}/K_{\infty}} >> (1 + \tau)V_\infty \\
i(f') @VVV \downarrow i @VV j V \\
D[[G(f')]] @> \text{Res} >> D[[G]] @> \text{Res}^+ >> D[[G(1)]]
\end{CD}
$$

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

For any $\mathbb{Z}_2$-module $M$, we will write $M \otimes_{\mathbb{Z}_2} D$ for the completion of $M \otimes_{\mathbb{Z}_2} D$.

Now recall the Iwasawa modules $\bar{C}_\ell$ and $\bar{C}_1$ defined in the preceding section.

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

$$
\{(1 - \tau)V_\infty/(1 - \tau)\bar{C}_\ell\} \otimes_{\mathbb{Z}_2} D \simeq A/m(f')B
$$

where $A$ and $B$ are ideals of height 2 in $D[[\Gamma]]$.

(ii) The map $j$ embeds $(1 + \tau)V_\infty \otimes_{\mathbb{Z}_2} D$ in $D[[\Gamma]]$ as an ideal of height 2. Under this embedding,

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

**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

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

**Proof.** This is immediate from part (i) of the above proposition. \[\square\]

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

Recall that $\text{Gal}(K(p_{\infty}^\infty)/K) = G(1) \simeq \Gamma \simeq \mathbb{Z}_2$.

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

**Proof.** Since $K_{\infty}^+ = K(p_{\infty})$ by Proposition 5.2, $K_{\infty}^+ / K$ is a $\mathbb{Z}_2$-extension in which only $p$ 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. \[\square\]

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

**Lemma 5.6.** We have

$$
\bar{C}_1 = \bar{E}_\infty^+.
$$
Proof. Fix an $n$ with $2 \leq n < \infty$. Noting that $K(p^n) = K_n^+$ is a cyclic extension of $K$, one can easily see that the group of elliptic units of $K(p^n)$ defined by Gillard in §6 of [10] agrees with our group $\mathcal{C}_{p^n}$. Then Théorème 5 of [10] gives

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

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

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

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

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

**Lemma 5.7.** (i) $X(K_n^+) = 0$.

(ii) $\bar{\mathcal{E}}_{\infty}^+ = U_{\infty}^+$. 

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

$$X(K_n^+)/I(G^+)X(K_n^+) = \text{Gal}(M_1/K_n^+),$$

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

**Proposition 5.8.** (i) $m(1)$ is a unit of $D[[T]]$.

(ii) $\text{char}(1 - \tau)V_\infty/(1 - \tau)\bar{\mathcal{C}}_\tau = \text{char}(V_\infty/\bar{\mathcal{C}}_\tau \cap V_\infty)$.

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 $m(1)D[[T]]$ contains an ideal of height 2, which gives (i). Now $U_{\infty}^+ \subset \bar{\mathcal{C}}_\tau \bar{\mathcal{C}}_1 = \bar{\mathcal{C}}_\lambda$, so the natural map

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

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

It is immediately clear from the above proposition and Corollary 5.4 that $g = m(f)m(1)$ and $\text{char}(V_\infty/\bar{\mathcal{C}}_\lambda \cap V_\infty)$ generate the same ideal in $D[[T]]$. 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 $\# \text{Hom}(X_\infty, E_{p^\infty})$ to $L(\psi, 1)/\Omega$ 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 $\psi$ 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 $X_\infty = \text{Gal}(M_\infty/K_\infty)$, where $M_\infty$ is the maximal abelian 2-extension of $K_\infty$ which is unramified outside of the primes above $p$.

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

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Proposition 6.1. If \( L(\overline{\psi}, 1) \neq 0 \) then
\[
\#\text{Hom}(X_\infty, E_{p^{\infty}}) \cong (1 - \psi(p)/N(p))L(\overline{\psi}, 1)/\Omega.
\]

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 \( \text{char}(V_\infty/\mathcal{C} \cap V_\infty) \),
\[
\#\text{Hom}(X_\infty, E_{p^{\infty}}) \cong \kappa(g).
\]

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

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

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 \( X_\infty^+ \) is finite, hence zero because \( X_\infty \) 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 \( X_\infty \) on which \( \tau \) acts trivially,
\[
X_\infty/(1 - \tau)X_\infty = \text{Gal}(L/K_\infty),
\]
where \( L \) is the maximal extension of \( K_\infty \) in \( M_\infty \) which is abelian over \( K_\infty^+ \). We will now show that \( \text{Gal}(L/K_\infty^+) \) is finite. By Lemma 5.7(i) there is no non-trivial abelian 2-extension of \( K_\infty^+ \) which is unramified outside of \( p \), so
\[
\text{Gal}(L/K_\infty^+) = \prod_{v \notin p} I_v,
\]
where the product extends over all primes \( v \) of \( K_\infty^+ \) not lying above \( p \) and \( I_v \) is the inertia group of \( v \) in \( \text{Gal}(L/K_\infty^+) \). Since \( L/K_\infty \) is unramified outside of \( p \), \( I_v \) injects into the inertia group of \( v \) in \( \text{Gal}(K_\infty/K_\infty^+) \) for each \( v \notin \mathfrak{p} \). 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 \( p \) are finitely decomposed in \( K_\infty^+ = K(p^\infty) \), and the proposition follows.

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

Lemma 6.3. We have
\[
1 - \psi(p)/N(p) \sim 2^{b^* - b} \cdot \#E(K_p)_{p^{\infty}}.
\]

Proof. When \( E \) has good reduction at \( p \) this follows from Lemma 1 of [4]. If \( E \) has bad reduction at \( p \) then \( \psi(p) = 0 \) and \( \#E(K_p)_{p^{\infty}} = 2 \) by Lemma 2.5(ii) for \( p \), 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 $\Sha_p$ denote the $p$-power torsion in the Tate-Shafarevich group of $E$ over $K$. Then, if $L(\psi, 1) \neq 0$,

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

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

$$2^{b-} \cdot \#E(K_p)_{\infty} \cdot L(\psi, 1)/\Omega \sim \#\Hom(X_{\infty}, E_{\infty})^G.$$ 

On the other hand, Theorem 3.9 gives

$$\#\Hom(X_{\infty}, E_{\infty})^G = 2^{b-} \cdot \#E(K_p)_{\infty} \cdot (\#E(K)_{2\infty})^{-1} \cdot \#\Sha_p,$$

which completes the proof. \qed

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

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

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

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 $L(E_{d_Q}, 1) \neq 0$. In this section we will show that Birch and Swinnerton-Dyer’s conjectural formula for $L(E_{d_Q}, 1)$ is valid, i.e. we will show that

$$(11) \quad L(E_{d_Q}, 1) = W_d \cdot (\#E_d(\mathbb{Q}))^{-2} \cdot \#\Sha_{E_{d_Q}} \cdot \prod c_p^{(d)}$$

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

$$\Sha_{E_{d_Q}} = \ker \left[ H^1(\mathbb{Q}, E_d) \to \bigoplus_v H^1(\mathbb{Q}_v, E_d) \right],$$

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 $L(E_{d_Q}, s) = d/|d|$ ([13] §19), so $L(E_{d_Q}, 1) = 0$ if $d < 0$.

So let $d$ be positive and prime to 7, and let $D_d$ and $L_d$ denote, respectively, the discriminant ideal and period lattice of a minimal model of $E_d$ over $\mathbb{Q}$. Define

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

Then $(2^{m_d})^{12}D_d = (-2^{12}7^3d^6)$ 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 $d > 0$)

$$(12) \quad L_d = \left(2^{m_d-1}/\sqrt{d}\right)L^1.$$
Lemma 7.1. (i) $W_d = W_{-7d}$.
(ii) For any $d$, $E_{/K}^d$ 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 $\text{Gal}(\mathbb{Q}(\sqrt{-7})/\mathbb{Q})$. Thus $D_d$ and $D_{-7d}$ differ by a power of (7) (see [7]). In particular, $\text{ord}_2(D_d) = \text{ord}_2(D_{-7d})$, so $m_d = m_{-7d}$. On the other hand formula 241.00 of [2] shows that $L_{1} = \sqrt{7} I_{1}$, so $I_d = I_1/\sqrt{d} = L_{-1}/\sqrt{7d} = L_{-7d}$. This proves (i). Assertion (ii) is clear since $\text{ord}_{\sqrt{-7}}(-2_{12}^73^6d^6) \equiv 0 \pmod{12}$. Finally, (iii) is known to hold for $d = 1$ ([13], p. 82). This fact together with (12) gives (iii) for all $d > 0$.

Lemma 7.2. Let $b$ denote the number of primes of $K$ where $E_{/K}^d$ 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 $E_{/\mathbb{Q}}$ 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 $b$.

Let $\psi_d$ denote the Hecke character of $K$ attached to $E^d$.

Lemma 7.3. (i) $L(E_{/\mathbb{Q}}^d, s) = L(\psi_d, s) = L(\bar{\psi}_d, s)$.
(ii) For any $d$, $E_{/\mathbb{Q}}^d \simeq \mathbb{Z}/2\mathbb{Z}$ 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.

Proposition 7.4. We have

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

Proof. If $B$ denotes the set of primes of $K$ where $E_{/K}^d$ has bad reduction, then $B \neq \{p\}$ by Lemma 7.1(ii). Thus $E_{/K}^d$ in a non-exceptional curve, so formula (3) of the Introduction is valid for the prime $p$ (see Theorem 6.4 above). Similarly $B \neq \{\bar{p}\}$, so (3) is valid at the prime $\bar{p}$ 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.

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

$$(13) \quad \#\mathbb{I}E_{/K}^d \equiv \left(\#\mathbb{I}E_{/\mathbb{Q}}^d \right)^2.$$  

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

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
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. ☐

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

$$\text{III}(E^d_{/\mathbb{Q}}) \simeq \text{III}(E^d_K)^{G_K/\mathbb{Q}}.$$ 

Proof. It suffices to check that if $v$ is a place of $\mathbb{Q}$ and $\wp$ is a place of $K$ lying above $v$, then the local restriction map $H^1(\mathbb{Q}_v, E^d) \to H^1(K_v, E^d)$ is injective. The kernel of this map is $H^1(\text{Gal}(K_v/\mathbb{Q}_v), E^d(K_v))$, which is clearly zero if $K_v = \mathbb{Q}_v$ or if $v$ is a prime of good reduction for $E^d_{/\mathbb{Q}}$ (since then $v \neq 7$, so $K_v/\mathbb{Q}_v$ 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 $\text{Gal}(K_v/\mathbb{Q}_v)$ with $G_{K/\mathbb{Q}}$.

There is an isomorphism $E^d(K_v) \simeq E^d(K_v)_{2^\infty} \oplus A$, 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 $E^d(K_v)_{2^\infty} = E^d_2$. It follows that there is an isomorphism

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

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 $H^1(G_{K/\mathbb{Q}}, E^d(\mathbb{C})) = 0$. ☐

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 $\mathfrak{p} \mathfrak{p}$ with $\mathfrak{p} \neq \mathfrak{p}$ ($\mathfrak{p} = \mathfrak{p}^c$). We have $\# \text{III}(E^d_{/\mathbb{Q}})_{2^\infty} = (\# \text{III}(E^d_K)_{2^\infty})^2$, and multiplication by $(1 + c)$ on $\text{III}(E^d_{/\mathbb{Q}})_{2^\infty}$ induces an isomorphism

$$\text{III}(E^d_{/\mathbb{Q}})_{2^\infty} \simeq \text{III}(E^d_K)_{2^\infty}.$$ 

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

Case II. $p \neq 2$.

Writing $\text{III}(E^d_{/\mathbb{Q}})_{p^\infty}$ for $(1 - c)\text{III}(E^d_K)_{p^\infty}$, we have the decomposition

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

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

$$\# \text{III}(E^d_{/\mathbb{Q}})_{p^\infty} = \# \text{III}(E^d_{/\mathbb{Q}})_{p^\infty} \cdot \# \text{III}(E^d_{/\mathbb{Q}})_{p^\infty}.$$
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

\[
\#\text{III}(E_{/\mathbb{Q}})_{p^\infty} = \#\text{III}(E^d_{/\mathbb{Q}})_{p^\infty}
\]

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 \( p \) and good reduction at all other primes. In this section we will check formula (3) of the Introduction for these curves.

As before, write \( K_\infty = K(E_p^\infty) \) and \( G = \text{Gal}(K_\infty/K) \). Keep the rest of the notation from \( \S \S 2–6 \) as well.

**Lemma 8.1.** (i) \( K_\infty = K(p^\infty) \).

(ii) \( H^1(G, E_{p^\infty}) = 0 \) for all \( i \geq 1 \).

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

**Proposition 8.2.** We have \( \text{III}_{p^\infty} = 0 \).

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

Recall that if \( a, b \in K^\times \) then \( a \sim b \) means that \( a/b \) is a unit at \( p \).

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

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

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

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

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

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 \( \bar{p} \), we have

\[
L(\bar{\psi}, 1)/\Omega \sim (\#E(K)_{p^\infty})^{-1} = 2 \cdot (\#E(K)_{2^\infty})^{-1} = 2^h \cdot (\#E(K)_{2^\infty})^{-1} \#\text{III}_{p^\infty},
\]

as desired.
REFERENCES


Facultad de Ciencias, Universidad de Chile, Casilla 653, Santiago, Chile
E-mail address: cgonzale@abello.dic.uchile.cl