The Tate–Shafarevich group for elliptic curves with complex multiplication

J. Coates\textsuperscript{a}, Z. Liang\textsuperscript{b}, R. Sujatha\textsuperscript{c,}\textsuperscript{*}

\textsuperscript{a} DPMMS, University of Cambridge, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, England, UK
\textsuperscript{b} School of Mathematical Sciences, Capital Normal University, Beijing, China
\textsuperscript{c} School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Bombay 400 005, India

\textbf{Article info}

Article history:
Received 4 November 2008
Available online 26 May 2009
Communicated by John Cremona

To John Cannon and Derek Holt

Keywords:
Elliptic curves
Algebraic number theory

\textbf{Abstract}

Let \(E\) be an elliptic curve over \(\mathbb{Q}\) with complex multiplication. We give an explicit upper bound for the number of copies of \(\mathbb{Q}_p/\mathbb{Z}_p\) which can occur in the Tate–Shafarevich group of \(E\) for all sufficiently large good ordinary primes \(p\).

© 2009 Elsevier Inc. All rights reserved.


\section{Introduction}

Let \(E\) be an elliptic curve over \(\mathbb{Q}\) and put \(g_{E/\mathbb{Q}} = \text{rank of } E(\mathbb{Q})\). Let

\[ \Sha(E/\mathbb{Q}) = \ker \left( H^1(\mathbb{Q}, E) \to \bigoplus_v H^1(\mathbb{Q}_v, E) \right), \]

where \(v\) ranges over all places of \(\mathbb{Q}\) and \(\mathbb{Q}_v\) is the completion of \(\mathbb{Q}\) at \(v\), denote its Tate–Shafarevich group. As usual, \(L(E/\mathbb{Q}, s)\) is the complex \(L\)-function of \(E\) over \(\mathbb{Q}\). Since \(E\) is now known to be modular, Kolyvagin's work \cite{10} shows that \(\Sha(E/\mathbb{Q})\) is finite if \(L(E/\mathbb{Q}, s)\) has a zero at \(s = 1\) of order \(\leq 1\), and that \(g_{E/\mathbb{Q}}\) is equal to the order of the zero of \(L(E/\mathbb{Q}, s)\) at \(s = 1\). His proof relies heavily on the theory of Heegner points and the work of Gross and Zagier. However, when \(L(E/\mathbb{Q}, s)\) has a zero at \(s = 1\) of order \(\geq 2\), all is shrouded in mystery. It is unknown whether or not \(L(E/\mathbb{Q}, s)\) has

\* Corresponding author.
E-mail addresses: jh.coates@dpmms.cam.ac.uk (J. Coates), liangzhb@gmail.com (Z. Liang), sujatha@math.tifr.res.in (R. Sujatha).
a zero at \( s = 1 \) of order \( \geq g_{E/Q} \), and no link between \( L(E/Q, s) \) and \( \mu(E/Q) \) has ever been proven. In particular, the finiteness of \( \mu(E/Q) \) is unknown for a single elliptic curve \( E/Q \) with \( g_{E/Q} \geq 2 \). This state of affairs is particularly galling for number theorists, since the conjecture of Birch and Swinnerton–Dyer even gives an exact formula for the order of \( \mu(E/Q) \), which predicts that in the vast majority of numerical examples \( \mu(E/Q) \) is zero when \( g_{E/Q} \geq 2 \). We also stress that in complete contrast to the situation for finding \( g_{E/Q} \), it is impossible to calculate \( \mu(E/Q) \) by classical descent methods, except for its \( p \)-primary subgroup for small primes \( p \), usually with \( p \leq 5 \).

By contrast, in the \( p \)-adic world, it has long been known that the main conjectures of Iwasawa theory provide a precise link between the \( \mathbb{Z}_p \)-corank of the \( p \)-primary subgroup of \( \mu(E/Q) \) and the multiplicity of the zero of certain \( p \)-adic \( L \)-functions at the point \( s = 1 \) in the \( p \)-adic plane, at least when \( E \) has potential good ordinary reduction at \( p \). However, it seems that little effort has been made so far to exploit this deep connexion for theoretical purposes, and the only numerical applications to date are given in the recent paper [16], see also [13,14] for the case of supersingular reduction at \( p \). The aim of this paper is to make some modest first steps in this direction in the special case of elliptic curves with complex multiplication. We begin with a theoretical result. For each prime \( p \), let \( t_{E/Q,p} \) denote the \( \mathbb{Z}_p \)-corank of the \( p \)-primary subgroup of \( \mu(E/Q) \). While we cannot prove the vanishing of \( t_{E/Q,p} \) for infinitely many \( p \) in any new cases, we can at least establish the following rather general weak upper bound for \( t_{E/Q,p} \) for sufficiently large good ordinary primes \( p \).

**Theorem 1.1.** Assume that \( E/Q \) admits complex multiplication. For each \( \epsilon > 0 \), there exists an explicitly computable number \( c(E, \epsilon) \), depending only on \( E \) and \( \epsilon \), such that

\[
t_{E/Q,p} \leq (1 + \epsilon)p - g_{E/Q}
\]

for all primes \( p \geq c(E, \epsilon) \) where \( E \) has good ordinary reduction.

We remark that a much stronger form of Theorem 1.1 is known in the geometric analogue (i.e. the case of an elliptic curve over a function field in one variable over a finite field), thanks to the work of Artin and Tate [20]. Indeed, their work shows that, in the geometric analogue, the number of copies of \( \mathbb{Q}_p/\mathbb{Z}_p \) occurring in the Tate–Shafrarevich group has an absolute upper bound which is independent of \( p \). We also note in passing that, after many special cases were established by earlier authors, the Dokchitser brothers [7] have finally proven that, for all elliptic curves \( E \) over \( \mathbb{Q} \) and all primes \( p \), the parity of \( g_{E/Q} + t_{E/Q,p} \) is equal to the parity of the order of zero at \( s = 1 \) of the complex \( L \)-function of \( E/Q \); in particular, the parity of \( t_{E/Q,p} \) does not depend on \( p \).

In the second part of the paper, we show that the \( p \)-adic methods of Iwasawa theory enable one to push numerical calculations of \( t_{E/Q,p} \) over a much larger range of \( p \) where \( E \) admits good ordinary reduction than is possible by classical methods. We consider the elliptic curves

\[
y^2 = x^3 - 17x
\]

and

\[
y^2 = x^3 + 14x.
\]

Both curves admit complex multiplication by the ring of Gaussian integers \( \mathbb{Z}[i] \), and have \( g_{E/Q} = 2 \). The conjecture of Birch and Swinnerton–Dyer predicts that \( \mu(E/Q) = 0 \) for both curves.

**Theorem 1.2.** For the elliptic curves (2) and (3), we have \( t_{E/Q,p} = 0 \) for all primes \( p \) with \( p \equiv 1 \mod 4 \) and \( p < 13500 \), excluding \( p = 17 \) for (2). Moreover \( \mu(E/Q)(p) = 0 \) for all such primes \( p \).

It is surprising that, for the curve (2), the \( p \)-adic \( L \)-function we consider has no other zeroes beyond the zero of order 2 arising from the fact that \( E(\mathbb{Q}) \) has rank 2, for all primes \( p < 13500 \) with
2. \( p \)-Adic \( L \)-functions and the main conjecture

In this section, we briefly explain the theoretical aspects of the Iwasawa theory of elliptic curves with complex multiplication, which underlie the proof of Theorem 1.1, and the computational work described in Section 3. For a systematic account of the Iwasawa theory for curves with complex multiplication, see the forthcoming book [4].

Let \( K \) be an imaginary quadratic field, and write \( \mathcal{O}_K \) for the ring of integers of \( K \). We fix an embedding of \( K \) in \( \mathbb{C} \). Let \( E \) be an elliptic curve defined over \( K \) such that \( \text{End}_K(E) \otimes \mathbb{Z} \mathbb{Q} \) is isomorphic to \( K \) such that \( \text{End}_K(E) \) denotes the ring of \( K \)-endomorphisms of \( E \). It is well known that \( E \) is isogenous over \( K \) to a curve whose ring of \( K \)-endomorphisms is isomorphic to \( \mathcal{O}_K \). As the results we shall discuss depend only on the isogeny class of \( E \), we shall assume henceforth that

\[
\text{End}_K(E) \simeq \mathcal{O}_K. \tag{4}
\]

The existence of such an elliptic curve defined over \( K \) implies, by the classical theory of complex multiplication, that \( K \) has class number 1. We choose a global minimal Weierstrass equation for \( E \)

\[
y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6
\]

whose coefficients \( a_i \) belong to \( \mathcal{O}_K \). Write \( \psi_E \) for the Grössencharacter of \( K \) attached to \( E \) by the theory of complex multiplication. Recall that if \( v \) is a finite place of \( K \) such that \( E \) has good reduction at \( v \), and if \( k_v \) denotes the residue field of \( v \), then the theory of complex multiplication shows that there is a unique element \( \pi_v \) of \( \text{End}_K(E) \) such that the reduction of \( \pi_v \) modulo \( v \) is the Frobenius endomorphism of the reduction of \( E \) modulo \( v \), relative to \( k_v \). The Grössencharacter \( \psi_E \) is then given by \( \psi_E(v) = \pi_v \). We write \( \mathfrak{f} \) for the conductor of \( \psi_E \). It is well known that the prime factors of \( \mathfrak{f} \) are precisely the primes of \( K \) where \( E \) has bad reduction. For each integer \( n \geq 1 \), we define

\[
L_{\mathfrak{f}}(\psi_E^n, s) = \prod_{(v, f) = 1} \left( 1 - \frac{\psi_E^n(v)}{(Nv)^s} \right)^{-1}.
\]

Further, \( L(\psi_E^n, s) \) will denote the primitive Hecke \( L \)-function of \( \psi_E^n \).

Let \( \mathcal{L} \) be the period lattice of the Néron differential

\[
\sigma^* = \frac{dx}{2y + a_1x + a_3},
\]

and let

\[
\Phi(z, \mathcal{L}) : \mathbb{C}/\mathcal{L} \simeq E(\mathbb{C})
\]

be the isomorphism given by

\[
\Phi(z, \mathcal{L}) = \left( \Phi(z, \mathcal{L}) - \frac{a_1^2 + 4a_2}{12}, \frac{1}{2} \left( \Phi'(z, \mathcal{L}) - a_1 \left( \Phi(z, \mathcal{L}) - \frac{a_1^2 + 4a_2}{12} \right) - a_3 \right) \right),
\]

where \( \Phi(z, \mathcal{L}) \) denotes the period lattice of the Néron differential.
where \( \wp(z, \mathcal{L}) \) denotes the Weierstrass \( \wp \)-function attached to \( \mathcal{L} \). Since \( \mathcal{O}_K \) has class number 1, there exists \( \Omega_{\infty} \) in \( \mathbb{C}^\times \) such that

\[ \mathcal{L} = \Omega_{\infty} \mathcal{O}_K. \]

As we shall explain below (see (24)), it is well known that

\[ \Omega_{\infty}^{-n} L(\bar{\psi}_E^n, n) \in K \]

for all integers \( n \geq 1 \). Moreover,

\[ L(\bar{\psi}_E^n, n) \neq 0 \quad \text{for} \quad n \geq 3, \]

since the Euler product converges when \( n \geq 3 \) (in fact, (8) also holds for \( n = 2 \), but the proof is more complicated). Put

\[ c_p(E) = \Omega_{\infty}^{-p} L(\bar{\psi}_E^p, p). \]

If \( h \) is any integral ideal of \( K \), we define

\[ E_h = \text{Ker}(E(\bar{K}) \twoheadrightarrow E(\bar{K})). \]

where \( h \) is any generator of \( h \). Define \( E_{p^n} = \bigcup_{n \geq 1} E_{p^n} \). Let \( \mathcal{M} \) be any Galois extension of \( K \). For each non-archimedean place \( w \) of \( \mathcal{M} \), let \( \mathcal{M}_w \) be the union of the completions at \( u \) of all finite extensions of \( K \) contained in \( \mathcal{M} \). We recall that the classical \( p^\infty \)-Selmer group of \( E \) over \( \mathcal{M} \) is defined by

\[ \text{Sel}_{p^\infty}(E/\mathcal{M}) = \text{Ker}(H^1(\text{Gal}(\bar{\mathcal{M}}/\mathcal{M}), E_{p^n}) \twoheadrightarrow \prod_w H^1(\text{Gal}(\bar{\mathcal{M}}_w/\mathcal{M}_w), E(\bar{\mathcal{M}}_w))). \]

where \( \mathcal{M}_w \) runs over all non-archimedean places of \( \mathcal{M} \). The Galois group of \( \mathcal{M} \) over \( K \) operates on \( \text{Sel}_{p^\infty}(E/\mathcal{M}) \) in the natural fashion. If \( A \) is any \( \mathcal{O}_K \)-module, \( A(p) \) will denote the submodule consisting of all elements which are all annihilated by some power of a generator of \( p \). Then we have the exact sequence

\[ 0 \rightarrow E(\mathcal{M}) \otimes_{\mathcal{O}_K} (K_p/\mathcal{O}_p) \twoheadrightarrow \text{Sel}_p(E/\mathcal{M}) \rightarrow \text{\texttt{W}(E/\mathcal{M})(p)} \rightarrow 0, \]

where \( \text{\texttt{W}(E/\mathcal{M})} \) denotes the Tate–Shafarevich group of \( E \) over \( \mathcal{M} \). We will also need to consider the compact \( \mathbb{Z}_p \)-module

\[ X_p(E/\mathcal{M}) = \text{Hom}(\text{Sel}_p(E/\mathcal{M}), \mathbb{Q}_p/\mathbb{Z}_p). \]

When \( \mathcal{M} \) is any finite extension of \( K \), classical arguments from Galois cohomology show that \( X_p(E/\mathcal{M}) \) is a finitely generated \( \mathbb{Z}_p \)-module. In particular, we define

\[ s_p = \mathbb{Z}_p \text{-rank of } X_p(E/K), \quad t_p = \mathbb{Z}_p \text{-corank of } \text{\texttt{W}(E/K)(p)}. \]

It is clear from (11) that we have

\[ s_p = t_p + n_{E/K}, \]

where \( n_{E/K} = \mathcal{O}_K \text{-rank of } E(K) \). We denote the number of roots of unity in \( K \) by \( w \).
Theorem 2.1. Let \( p \) be a prime number such that (i) \( (p, f) = 1 \), (ii) \( (p, w) = 1 \), and (iii) \( p \) splits in \( K \), say \( p \mathcal{O}_K = pb^\ast \). Let \( m_p \) (resp. \( m_p^\ast \)) denote \( \text{ord}_p(c_p(E)) \) (resp. \( \text{ord}_p^\ast(c_p(E)) \)). Then we always have

\[
m_p \geq s_p, \quad m_p^\ast \geq s_p^\ast.
\]

Moreover, if either \( m_p = n_{E/K} \) or \( m_p^\ast = n_{E/K}^\ast \), then \( \mu(E/K)(p) \) is finite.

In fact, a stronger form of the theorem holds if \( E \) is defined over \( \mathbb{Q} \). Assume therefore that \( E \) is defined over \( \mathbb{Q} \), and write \( L(E/\mathbb{Q}, s) \) for the Hasse–Weil \( L \)-function of \( E \) over \( \mathbb{Q} \). By the theorem of Deuring–Weil, we have

\[
L(E/\mathbb{Q}, s) = L(\psi_E, s),
\]

where the \( L \)-function on the right is the complex \( L \)-function attached to the Grössencharacter \( \psi_E \). Put

\[
g_{E/\mathbb{Q}} = \mathbb{Z}\text{-rank of } E(\mathbb{Q}), \quad r_{E/\mathbb{Q}} = \text{order of zero at } s = 1 \text{ of } L(E/\mathbb{Q}, s).
\]

As \( E \) is defined over \( \mathbb{Q} \), it has real periods, and we define \( \Omega_{\infty}^+ \) to be its smallest positive real period. Thus

\[
\Omega_{\infty}^+ = \Omega_{\infty} \alpha(E),
\]

where \( \alpha(E) \) is some non-zero element of \( \mathcal{O}_K \). Put

\[
c_p^+(E) = (\Omega_{\infty}^+)^{-p} L(\psi_E^p, p).
\]

Let \( \bar{E}_p \) denote the reduction of \( E \) modulo \( p \).

Theorem 2.2. Assume that \( E \) is defined over \( \mathbb{Q} \). Then \( c_p^+(E) \in \mathbb{Q} \). Let \( p \) be a prime number such that (i) \( E \) has good reduction at \( p \), (ii) \( (p, w) = 1 \), (iii) \( p \) splits in \( K \), and (iv) \( (p, \alpha(E)) = 1 \). Assume also that \( r_{E/\mathbb{Q}} \equiv g_{E/\mathbb{Q}} \mod 2 \). If we have

\[
\text{ord}_p(c_p^+(E)) < g_{E/\mathbb{Q}} + 2,
\]

then \( \mu(E/K)(p) \) is finite. Moreover, if

\[
\text{ord}_p(c_p^+(E)) = g_{E/\mathbb{Q}},
\]

and \( \bar{E}_p(\overline{\mathbb{F}_p}) \) has order prime to \( p \) with \( (p, 6) = 1 \), then \( \mu(E/K)(p) = 0 \).

We shall say a prime \( p \) satisfying (i)–(iv) of Theorem 2.2 is exceptional for \( E \) if

\[
\text{ord}_p(c_p^+(E)) > g_{E/\mathbb{Q}}.
\]

For example, for the curve (3), with \( g_{E/\mathbb{Q}} = 2 \), the primes \( p = 29, 277 \) are the only exceptional primes congruent to 1 mod 4 for \( p < 13500 \). However, for \( p = 29, 277 \), our calculations show that \( \text{ord}_p(c_p^+(E)) = 3 \), and so \( \mu(E/K)(p) \) is finite. For these two exceptional primes, C. Wuthrich computed the Mazur–Swinnerton–Dyer \( p \)-adic \( L \)-function for the curve \( E \) defined by (3), and showed in this way that we have also that \( \mu(E/K)(p) = 0 \) for both primes. It is surprising that there are no exceptional primes \( p \) congruent to 1 mod 4 for the curve (2) with \( p < 13500 \).
For all integers \( n \geq 1 \), let \( \mathcal{E}_n^*(z, L) \) denote the Eisenstein series of \( L \), as defined by Eisenstein (see Weil [19] or [9]). In particular, for \( n \geq 3 \), we have

\[
\mathcal{E}_n^*(z, L) = \frac{(-1)^n}{(n-1)!} \left( \frac{d}{dz} \right)^{n-2} \left( \wp(z, L) \right).
\]

The following fundamental formula, which will be the basis of our subsequent work, is proven in [5].

**Theorem 2.3.** Let \( f \) be any generator of the conductor \( \mathcal{f} \) of \( \psi_E \). Then, for all integers \( n \geq 1 \), we have \( \mathcal{E}_n^*(\mathcal{f}^p, L) \in K(E_f) \), and

\[
w\mathcal{L}^{-n}_\infty L_\mathcal{f}(\bar{\psi}_E^p, n) = f^{-n} \text{Trace}_{K(E_f)/K} \left( \mathcal{E}_n^* \left( \frac{\mathcal{L}_\infty}{f} \right), L \right).
\]

Note that (7) is an immediate consequence of this result.

We now fix a prime number \( p \) satisfying \((p, \mathcal{f}) = (p, w) = 1\) and \( pO_K = pp^* \), where \( p, p^* \) are distinct ideals of \( K \). We pick one of these primes, say \( p \), and an embedding

\[
i_p : \hat{K} \hookrightarrow \bar{\mathbb{Q}}_p,
\]

which induces \( p \) on \( K \). For simplicity, we shall usually omit \( i_p \) from subsequent formulae. As was shown in [6], (see also [4]), there exists a \( p \)-adic \( L \)-function which essentially interpolates the image of the \( L \)-values (7). We only state the precise result for the branch of this \( p \)-adic \( L \)-function which is needed for the proof of Theorem 1.1.

Let \( \hat{E}^p \) be the formal group of \( E \) at \( p \), so that we can take \( t = -x/y \) to be a parameter of \( \hat{E}^p \). Let \( \hat{G}_m \) be the formal multiplicative group, and write \( u \) for its parameter. Denote by \( \mathcal{I} \) the ring of integers of the completion of the maximal unramified extension of \( \mathbb{Q}_p \). If \( t \) is a variable, then \( \mathcal{I}[T] \) will denote, as usual, the ring of formal power series in \( T \) with coefficients in \( \mathcal{I} \). As \( \hat{E}^p \) is a formal group of height 1 (in fact, it is even a Lubin–Tate group over \( \mathbb{Z}_p \) attached to the parameter \( \psi_E(p) \)), it is well known that there is an isomorphism over \( \mathcal{I} \)

\[
\delta_p : \hat{G}_m \cong \hat{E}^p,
\]

which is given by a formal power series \( t = \delta_p(u) \) in \( \mathcal{I}[u] \). We can then define the \( p \)-adic period \( \Omega_p \) in \( \mathcal{I}^\times \) by

\[
\Omega_p = \frac{\delta_p(u)}{u} \bigg|_{u=0}.
\]

**Proposition 2.4.** Assume \( \mathcal{L}_\infty \) and \( \Omega_p \) are fixed. Then there exists a unique power series \( H_p(T) \) in \( \mathcal{I}[T] \) such that, for all integers \( n \geq 1 \) with \( n \equiv 1 \bmod (p-1) \), we have

\[
\mathcal{L}_p^{-n} H_p((1+p)^n - 1) = \mathcal{L}_\infty^{-n} (n-1)! L(\bar{\psi}_E^p, n) \left( 1 - \frac{\psi_E^p(p)}{Np} \right).
\]

For a proof of the existence of this \( p \)-adic \( L \)-function \( H_p(T) \), see [6] or [4]. Note that when \( n \equiv 1 \bmod (p-1) \), \( \mathcal{f} \) is the exact conductor of \( \bar{\psi}_E^p \), and so \( L_\mathcal{f}(\bar{\psi}_E^p, s) \) coincides with the primitive \( L \)-function \( L(\bar{\psi}_E^p, s) \).

This \( p \)-adic \( L \)-function is related to descent theory on \( E \) via the so-called “one variable main conjecture” for the Iwasawa theory of \( E \) over the unique \( \mathbb{Z}_p \)-extension of \( K \) unramified outside \( p \). Define
\[ F_\infty = K(E_\infty), \quad G = \text{Gal}(F_\infty/K). \]

The action of \( G \) on \( E_\infty \) defines a homomorphism

\[ \chi_p : G \to \text{Aut}(E_\infty) = \mathbb{Z}_p^\times \]

which is an isomorphism because \( \hat{E}_p \) is a Lubin–Tate group. Let \( K_\infty \) be the unique \( \mathbb{Z}_p \)-extension contained in \( F_\infty \) (class field theory shows that \( K_\infty \) is the unique \( \mathbb{Z}_p \)-extension of \( K \) unramified outside \( p \)). Put

\[ \Gamma = \text{Gal}(K_\infty/K), \quad \Lambda(\Gamma) = \lim_{\leftarrow} \mathbb{Z}_p[\Gamma/U], \]

where \( U \) runs over the open subgroups of \( \Gamma \). There is a natural continuous action of \( \Gamma \) on \( X_p(E/K_\infty) \), and this extends to an action of the Iwasawa algebra \( \Lambda(\Gamma) \). Since it is known that \( X_p(E/K_\infty) \) is a finitely generated torsion \( \Lambda(\Gamma) \)-module (see [4,6]), it follows from the structure theory for such modules that there is an exact sequence of \( \Lambda(\Gamma) \)-modules

\[ 0 \to \bigoplus_{i=1}^r \Lambda(\Gamma)/f_i \Lambda(\Gamma) \to X_p(E/K_\infty) \to D \to 0, \]

where \( f_1, \ldots, f_r \) are non-zero elements of \( \Lambda(\Gamma) \) and \( D \) is a finite \( \Lambda(\Gamma) \)-module. We now pick the unique topological generator \( \gamma_p \) of \( \Gamma \) such that \( \chi_p(\gamma_p) = 1 + p \), and write

\[ j : \Lambda(\Gamma) \to \mathbb{Z}_p[[T]] \]

for the unique isomorphism of topological \( \mathbb{Z}_p \)-algebras with \( j(\gamma_p) = 1 + T \). For simplicity, put

\[ B_p(T) = j\left( \prod_{i=1}^r f_i \right). \]

The power series \( B_p(T) \) is uniquely determined up to multiplication by a unit in \( \mathbb{Z}_p[[T]] \), and is called a characteristic power series for \( X_p(E/K_\infty) \). We shall make essential use of the following deep result (see [15], or [4]).

**Theorem 2.5 (One variable main conjecture).**

\[ H_p ((1 + p)(1 + T) - 1)I[[T]] = B_p(T)I[[T]]. \]

In addition, we shall need (see [12, Chapter 4, Corollary 16]).

**Proposition 2.6.** The two groups \( \mu(E/K)(p) \) and \( \mu(E/K)(p^*) \) have the same \( \mathbb{Z}_p \)-corank. In particular, one is finite if and only if the other is also finite.

We can now prove Theorem 2.1. Since \( \chi_p \) is an isomorphism, we have \( E_\infty(K_\infty) = 0 \). It follows that the restriction map from \( S_p(E/K) \) to \( S_p(E/K_\infty) \) is injective, and by duality, we obtain a surjective \( \Gamma \)-homomorphism

\[ X_p(E/K_\infty) \to X_p(E/K). \]
Recall that $s_p$ denotes the $\mathbb{Z}_p$-rank of $X_p(E/K)$. As $\Gamma$ acts trivially on $X_p(E/K)$, it follows from (31) by a well-known property of characteristic ideals of torsion $\Lambda(\Gamma)$-modules, that $T^{sp}$ must divide $B_p(T)$ in $\mathbb{Z}_p[[T]]$. Hence we conclude from Theorem 2.5 that

$$H_p((1 + p)(1 + T) - 1) = T^{sp} h(T)$$

(32)

for some $h(T)$ in $\mathbb{Z}[[T]]$. Evaluating both sides at $(1 + p)^n - 1$ for any $n$ in $\mathbb{Z}$, we conclude that we always have

$$H_p((1 + p)^n - 1) \equiv 0 \mod p^{sp}.$$  

(33)

Taking $n = p$, and noting that $(1 - \frac{\psi_E(p)T}{Np})$ is a unit at $p$, we conclude from (33) and Proposition 2.4 that

$$c_p(E) \equiv 0 \mod p^{sp}.$$ 

(34)

Replacing $p$ by $p^*$, the same argument shows that

$$c_p(E) \equiv 0 \mod (p^*)^{sp^*}.$$  

(35)

Hence (15) follows. Moreover, if $m_p = n_{E/K}$, then $t_p = 0$ and so $t_p^* = 0$ by Proposition 2.6. A similar argument holds if $m_p^* = n_{E/K}$. This completes the proof of Theorem 2.1.

**Corollary 2.7.** We have $m_p = n_{E/K}$ if and only if the characteristic power series of $X_p(E/K_{\infty})$ can be taken to be $T^{n_{E/K}}$.

**Proof.** If $m_p = n_{E/K}$, the above argument shows that we must have $s_p = n_{E/K}$, and $h(0)$ a $p$-adic unit. It follows from Theorem 2.5 that $B_p(T)$ must be of the form $T^{n_{E/K}}$ times a unit in $\mathbb{Z}_p[[T]]$. Conversely, if the characteristic power series of $X_p(E/K_{\infty})$ can be taken to be $T^{n_{E/K}}$, then Theorem 2.5 shows that $H_p(T)$ is equal to $T^{n_{E/K}}$ times a unit in $\mathbb{Z}[[T]]$, whence it is plain that $m_p = n_{E/K}$. This completes the proof. \qed

Our numerical calculations show that, for the elliptic curve

$$y^2 = x^3 - 17x, \quad \text{with } n_{E/K} = 2,$$

we have $m_p = 2$ for all primes $p$ with $p \equiv 1 \mod 4$, $p \neq 17$, and $p < 13500$. Thus the characteristic power series of $X_p(E/K_{\infty})$ is $T^2$ for all such primes. On the other hand, for the elliptic curve

$$y^2 = x^3 + 14x, \quad \text{with } n_{E/K} = 2,$$

we have $m_p = 2$ for all primes $p$ with $p \equiv 1 \mod 4$ and $p < 13500$, except $p = 29, 277$. Thus for all such primes, with the exception of these two, the characteristic power series of $X_p(E/K_{\infty})$ is $T^2$.

We now establish Theorem 2.2. Assuming that $E$ is defined over $\mathbb{Q}$, we have

$$\tilde{\ell} = \ell, \quad \text{and} \quad \psi_E(\tilde{a}) = \overline{\psi_E(a)}$$  

(36)

for all integral ideals $a$ of $K$ with $(a, \ell) = 1$. Hence

$$L(\psi_E^P, s) = L(\tilde{\psi}_E^P, s).$$
Evaluating at \( s = p \), we conclude that

\[
L(\tilde{\psi}_E^p, p) \in \mathbb{R}.
\]

As \( \Omega_\infty^K \) is real, it follows that

\[
c_p^+(E) \in K \cap \mathbb{R} = \mathbb{Q}.
\]

As before, let \( t_p \) (resp. \( t_p^* \)) be the \( \mathbb{Z}_p \)-corank of \( \mathbb{u}(E/K)(p) \) (resp. \( \mathbb{u}(E/K)(p^*) \)), and let \( t_{E/Q, p} \) be the \( \mathbb{Z}_p \)-corank of \( \mathbb{u}(E/Q)(p) \). Then we claim that

\[
t_{E/Q, p} = t_p = t_p^*.
\]

Indeed, the second equality is just Proposition 2.6. To prove the first equality, note that \( E \) is isogenous over \( \mathbb{Q} \) to the twist \( E' \) of \( E \) by the quadratic character of \( K \) (see, for example, [8]). Thus, \( \mathbb{u}(E/Q)(p) \) and \( \mathbb{u}(E'/Q)(p) \) have the same \( \mathbb{Z}_p \)-corank, and hence the \( \mathbb{Z}_p \)-corank of \( \mathbb{u}(E/K)(p) \) is equal to \( 2t_{E/Q, p} \). On the other hand, the \( \mathbb{Z}_p \)-corank of \( \mathbb{u}(E/K)(p) \) is clearly equal to \( t_p + t_p^* = 2t_{E/Q, p} \), by Proposition 2.6. Hence \( t_{E/Q, p} = t_p \), thereby proving (37).

Assume now that \( \mathbb{u}(E/K)(p) \) is infinite, so that \( t_{E/Q, p} > 0 \). The parity theorem for \( E/Q \) and the prime \( p \) (due to Greenberg in this case, but see the more general results of [7,11]) asserts that

\[
g_{E/Q} + t_{E/Q, p} \equiv t_{E/Q} \mod 2.
\]

By our hypothesis that \( g_{E/Q} \) and \( t_{E/Q} \) have the same parity, it follows that \( t_{E/Q, p} \) must be even, and therefore \( t_{E/Q, p} \geq 2 \), in particular. Hence by (37) \( t_p \geq 2 \). Noting that \( g_{E/Q} = n_{E/K} \), and that \( (p, \alpha(E)) = 1 \), we conclude from (34) that

\[
\text{ord}_p(c_p^+(E)) \geq g_{E/Q} + 2.
\]

Hence, if (20) holds, then we must have \( \mathbb{u}(E/K)(p) \) is finite.

Assume now that \( \text{ord}_p(c_p^+(E)) = g_{E/Q} \). We deduce easily from Theorem 2.5 and (32), that

\[
B_p(T) = T^{n_{E/K}} R_p(T),
\]

where \( R_p(T) \) is a unit in \( \mathbb{Z}_p[[T]] \), so that \( R_p(0) \) is a unit in \( \mathbb{Z}_p \). Hence, by an important general theorem of Perrin-Riou [12], it follows that the canonical \( p \)-adic height pairing

\[
\langle,\rangle_p : E(K) \otimes_{\mathcal{O}} \mathbb{Z}_p \times E(K) \otimes_{\mathcal{O}} \mathbb{Z}_p \to \mathbb{Q}_p,
\]

where \( \mathcal{O} \) is embedded in \( \mathbb{Z}_p \) via \( i_p \), is non-degenerate. Further, we have that

\[
\#(\mathbb{u}(E/K)(p)) \times \det(\langle,\rangle_p) \times \left( 1 - \frac{\psi_{E/K}(p)}{N_p} \right)
\]

is also a \( p \)-adic unit, where \( \det \) denotes the determinant of the height pairing; for this last assertion, we need our hypothesis that \( (p, 6) = 1 \). However, if \( \hat{E}_p(\mathbb{F}_p) \) has order prime to \( p \) and \( (p, 6) = 1 \), then it follows from the results of [12] that \( \det(\langle,\rangle_p) \) is a \( p \)-adic integer. Hence we conclude from (38) that \( \mathbb{u}(E/K)(p) \) is trivial. A similar argument proves the corresponding statement for \( \mathbb{u}(E/K)(p^*) \) and this completes the proof of Theorem 2.2.

We next establish an upper bound for \( t_p \) and \( t_{p^*} \) when \( p \) is a sufficiently large prime which splits in \( K \) as \( p \mathcal{O}_K = pp^* \).
**Theorem 2.8.** For each $\epsilon > 0$, there exists an explicitly computable number $c(E, \epsilon)$, depending only on $E$ and $\epsilon$, such that

$$t_p \leq (1 + \epsilon)p - n_{E/K}, \quad t_p^* \leq (1 + \epsilon)p - n_{E/K},$$

for all primes $p \geq c(E, \epsilon)$ which split in $K$ as $pO_K = pp^*$.

We note that, when $E$ is defined over $\mathbb{Q}$, Theorem 1.1 is an immediate consequence of this result, since, thanks to (37), we then have $t_E/\mathbb{Q}, p = t_p, n_{E/K} = g_E/\mathbb{Q}$.

We now give the proof of Theorem 2.8 which is a simple application of the formula (24), and the fact that $L(\bar{\psi}^p_E, s) \neq 0$ (recall that the latter assertion is true because the Euler product for $L(\bar{\psi}^p_E, s)$ converges for $s = p$). Put

$$\Theta_p = \text{Trace}_{K(E_1)/K} \left( E_p^n \left( \frac{\Omega_{\infty f}}{f}, L \right) \right).$$

We emphasize that in the proof $E$ is fixed and $p$ is varying over all sufficiently large prime numbers which split in $K$.

**Lemma 2.9.** We have $|\Theta_p| \leq d_1^p$, where $d_1 > 1$ is a real number depending only on $E$ and not on $p$.

**Proof.** We may assume $p \geq 3$. By (23), we have

$$E_p^n \left( \frac{\Omega_{\infty f}}{f}, L \right) = \frac{(-1)^p}{(p-1)!} \left( \frac{d}{dz} \right)^{p-2} (\varphi(z, L)) \bigg|_{z=\Omega_{\infty f}}.$$

Let $B$ denote a set of integral ideals of $K$, prime to $f$, such that the Galois group of $K(E_1)/K$ consists precisely of the Artin symbols $\sigma_b$ of the ideals $b$ in $B$. From the definition of the Grössencharacter $\psi_E$ and (41), we have

$$E_p^n \left( \frac{\Omega_{\infty f}}{f}, L \right)_{\sigma_b} = E_p^n \left( \psi_E(b) \frac{\Omega_{\infty f}}{f}, L \right).$$

Thus, by Cauchy’s integral formula, we obtain

$$E_p^n \left( \frac{\Omega_{\infty f}}{f}, L \right)_{\sigma_b} = \frac{(-1)^p}{(p-1)!} \int_{C_b} \frac{\varphi(z, L) dz}{(z - \psi_E(b)\Omega_{\infty f})^{p-1}},$$

where $C_b$ is a circle with centre $\frac{\psi_E(b)\Omega_{\infty f}}{f}$ and sufficiently small radius so that no element of $L$ lies in or on $C_b$. Estimating the integral, it is plain that

$$\left| E_p^n \left( \frac{\Omega_{\infty f}}{f}, L \right)_{\sigma_b} \right| \leq d_2^p,$$

where $d_2 > 1$ depends only on $E$. Summing over all $b$ in $B$, the assertion of the lemma follows. □
Lemma 2.10. There exists a rational integer $d_3 > 1$, depending only on $E$ and not on $p$, such that

$$d_3^p(p - 1)!\xi_p^* \left( \frac{\Omega_{\infty}}{f}, L \right)$$

is an algebraic integer.

Proof. We may assume that $p \geq 5$. Since

$$\xi_p^*(\lambda z, \lambda L) = \lambda^{-p} \xi_p^*(z, L)$$

for any complex number $\lambda$, it suffices to prove the lemma when our generalized Weierstrass equation (5) for $E$ has the property that $g_2(L)/2$ and $g_3(L)$ both belong to $O_K$; here $g_2(L)$ and $g_3(L)$ denote the usual Weierstrass invariants attached to (5). Now the differential equation

$$\left( \wp'(z, L) \right)^2 = 4\wp(z, L)^3 - g_2(L)\wp(z, L) - g_3(L)$$

implies that

$$\wp^{(2)}(z, L) = 6\wp(z, L)^2 - \frac{g_2(L)}{2}.$$ 

A simple recurrence argument on $n$ then shows that, for all $n \geq 1$, we have

$$\wp^{(2n)}(z, L) = D_n(\wp(z, L)),$$

where $D_n(X)$ is a polynomial in $O_K[X]$ of degree $n + 1$. It follows immediately that

$$\wp^{(2n+1)}(z, L) = B_n(\wp(z, L))\wp'(z, L),$$

where $B_n(X) = \frac{d}{dx}(D_n(X))$ is a polynomial of degree $n$ in $O_K[X]$. Taking $n = \frac{p-3}{2}$, the assertion the lemma is now clear from (41), on taking $d_3$ to be a positive integer such that

$$d_3\wp\left( \frac{\Omega_{\infty}}{f}, L \right), \quad d_3\wp'\left( \frac{\Omega_{\infty}}{f}, L \right)$$

are algebraic integers. \(\square\)

We can now complete the proof of Theorem 2.8. We may assume that $(p, f) = (p, w) = 1$. By (24), we then have

$$|\Omega_{\infty, E}^{-p}L(\overline{\psi}_E^p, p)|_p = |\Theta_p|_p = |(p - 1)!\Theta_p|_p,$$

and similarly for $p^*$. Moreover, in view of Lemmas 2.9 and 2.10,

$$d_3^p(p - 1)!\Theta_p$$

is an element of $O_K$ whose complex absolute value is at most $d_4^p(p - 1)!$, where $d_4 > 1$ does not depend on $p$. Since $\Theta_p \neq 0$ because $L(\overline{\psi}_E^p, p) \neq 0$, we conclude from the product formula that
\[ |d_3^p(p - 1)!\bar{\theta}_p|_p \times |d_3^p(p - 1)!\bar{\theta}_p|_{p^*} \geq d_4^{-2p}((p - 1)!)^{-2}. \] (43)

It follows that, we conclude that for each \( \epsilon > 0 \), we have

\[ |\theta_p|_p \times |\theta_p|_{p^*} \geq p^{-2(1+\epsilon)p} \]

for all \( p \geq c(E, \epsilon) \). On the other hand, by Theorem 2.1, and (42), we have

\[ |\theta_p|_p \times |\theta_p|_{p^*} \leq p^{-(s_p + s_{p^*})}. \]

Thus

\[ s_p + s_{p^*} \leq 2(1 + \epsilon)p \]

when \( p \geq c(E, \epsilon) \). As \( s_p = s_{p^*} \), the proof of the theorem is complete.

Define the \( p \)-adic \( L \)-functions

\[ \Lambda_{E,p}(s) = H_p((1 + p)^s - 1), \quad \Lambda_{E,p^*}(s) = H_{p^*}((1 + p)^s - 1), \]

where \( s \) is now a variable in \( \mathbb{Z}_p \). Put

\[ r_{E,p} = \text{ord}_{s=1}\Lambda_{E,p}(s), \quad r_{E,p^*} = \text{ord}_{s=1}\Lambda_{E,p^*}(s). \]

We end this section by remarking that exactly the same argument which establishes Theorem 2.8 proves the following result.

**Theorem 2.11.** For each \( \epsilon > 0 \), there exists an explicitly computable number \( c(E, \epsilon) \) such that

\[ r_{E,p} + r_{E,p^*} \leq 2(1 + \epsilon)p \]

for all primes \( p \geq c(E, \epsilon) \) with \( p \) splitting in \( K \) as \( p\mathcal{O}_K = pp^* \).

3. **Computations for** \( y^2 = x^3 - Dx \)

The goal of this section is to explain how one can use formula (24) to compute

\[ c_p(E) = \Omega_{\infty}^{-p}L(\tilde{\psi}_{E^p}, p) \]

in practice, for the family of curves

\[ E: y^2 = x^3 - Dx, \]

where \( D \) is a fourth-power free non-zero rational integer. For this family of curves, \( K = \mathbb{Q}(i) \) and the isomorphism (4) is given explicitly by mapping \( i \) to the endomorphism which sends \((x, y)\) to \((-x, iy)\). See [1] for earlier computational work on the Iwasawa theory of this family of curves.

We begin by analysing the Galois theory of the fields \( K(E_f) \) where \( f \) again denotes the conductor of \( \psi_E \). If \( \mathfrak{h} \) is any integral ideal of \( K \), we write

\[ \phi(\mathfrak{h}) = \#((\mathbb{Z}[i]/\mathfrak{h})^\times). \]
The next lemma is a very easy consequence of the existence of the Grössencharacter \( \psi_E \) (see [5, Lemma 3], or [3, Lemma 7]) and the fact that no non-trivial root of unity in \( K \) is \( \equiv 1 \mod \mathfrak{h} \), when \( \mathfrak{h} \) is a multiple of \( f \).

**Lemma 3.1.** Let \( \mathfrak{h} \) be any integral ideal of \( K \) which is divisible by the conductor \( f \) of \( \psi_E \). Then \( K(E_{\mathfrak{h}}) \) coincides with the ray class field of \( K \) modulo \( \mathfrak{h} \). In particular, the degree of \( K(E_{\mathfrak{h}})/K \) is equal to \( \phi(\mathfrak{h})/4 \).

The following well-known lemma computes \( f \) for the curve \( E \).

**Lemma 3.2.** Let \( \Delta \) be the product of the distinct prime factors of \( D \). Then \( f = 4\Delta\mathbb{Z}[i] \) if \( D \not\equiv 1 \mod 4 \) and \( f = (1+i)^2\Delta\mathbb{Z}[i] \) if \( D \equiv 1 \mod 4 \).

Let \( E' \) denote the elliptic curve in our family with \( D = 1 \), i.e.

\[
E': \ y^2 = x^3 - x. \tag{44}
\]

**Lemma 3.3.** Assume that \( E = E^D \) with \( D \) divisible by an odd power of an odd prime. Then the extension \( K(E_{(1+i)^k}) \) is equal to \( K \) when \( k = 1 \), to \( K(D^{1/2}) \) when \( k = 2 \), and to \( K(D^{1/4}) \) when \( k = 3 \). For \( k \geq 3 \), we have

\[
K(E_{(1+i)^k}) = K(D^{1/4}, E'_{(1+i)^k})
\]

and this field has degree \( 2^{k-1} \) over \( K \), and degree 4 over \( K(E'_{(1+i)^k}) \).

**Proof.** The assertions for \( k = 1 \) and \( k = 2 \) are readily verified. Put \( \alpha = D^{1/4} \). Over \( K(\alpha) \), we have an isomorphism

\[
E \simeq E'
\]

given by mapping the point \((x, y)\) on \( E \) to the point \((x/\alpha^2, y/\alpha^3)\) on \( E' \). Now \( E' \) has conductor \((1+i)^2\), and \( K(E'_{(1+i)^1}) = K \), whence it follows from (45) that \( K(E_{(1+i)^3}) = K(\alpha) \). Similarly, if \( k \geq 3 \), then (45) implies that \( K(E_{(1+i)^k}) = K(\alpha, E'_{(1+i)^k}) \). Now Lemma 3.1 applied to \( E' \) shows that the degree of \( K(E'_{(1+i)^k}) \) over \( K \) is \( 2^{k-3} \) when \( k \geq 3 \). Moreover, as \( E' \) has good reduction outside the prime \((1+i)\mathbb{Z}[i] \), this is the only prime of \( K \) which can ramify in the extension \( K(E'_{(1+i)^k}) \). Hence \( K(\alpha) : K \) = 4, and \( K(\alpha) \cap K(E'_{(1+i)^k}) = K \) because of the existence of the odd prime factor dividing \( D \) to an odd power. This completes the proof of the lemma. \( \square \)

**Lemma 3.4.** Assume that \( D \) is odd. Then the degree of \( K(E_D)/K \) is \( \phi(D\mathbb{Z}[i]) \).

**Proof.** We can assume \( D \not\equiv 1 \). By the Weil pairing, \( K(E'_D) \) contains the field generated over \( K \) by the \( |D| \)th roots of unity. Hence \( K(E'_D) \) contains \( \sqrt{D} \) (the sign of \( D \) is irrelevant since \( K \) contains the fourth roots of unity). As above, let \( \alpha = D^{1/4} \). Thus \( K(E'_D, \alpha) \) has degree at most 2 over \( K(E'_D) \).

Let \( R_D \) denote the ray class field of \( K \) modulo \( D\mathbb{Z}[i] \). Let \((u, v)\) be a primitive \( D \)-division point on \( E \). Then the classical theory of complex multiplication shows that \( R_D = K(u^2) \), and that \( [R_D : K] = \phi(D\mathbb{Z}[i])/4 \). To prove the lemma, it therefore suffices to show that there exists an element \( \tau \) of \( \text{Gal}(K(E_D)/K) \) such that \( \tau \) fixes \( R_D \), and \( \tau \) is of exact order 4. We do this as follows. As remarked in the previous paragraph, \( K(E'_D) \) has degree \( \phi(D\mathbb{Z}[i]) \) over \( K \) because \( D \) is odd. Moreover, a primitive \( D \)-division point on \( E' \) is given by \((u', v')\), where \( u' = u/\alpha^2 \), \( v' = v/\alpha^3 \). Recalling that multiplication by \( i \) on \( E' \) is given by sending \((x, y)\) to \((-x, iy)\), it follows that there exists \( \sigma \) in \( \text{Gal}(K(E'_D)/K) \) such that
\[ \sigma(u', v') = (-u', iv'). \] (46)

Now let \( \sigma \) denote any extension of \( \sigma \) to the field \( K(E'_D, \alpha) = K(E_D, \alpha) \). Since this field has degree at most 2 over \( K(E'_D) \), we must have that either \( \sigma(\alpha) = -\alpha \) or \( \sigma(\alpha) = \alpha \). Applying \( \sigma \) to \( (u', v') \), we conclude from (46) that

\[ \sigma u = -u, \quad \sigma v = -iv \quad \text{or} \quad \sigma u = -u, \quad \sigma v = iv. \]

It follows from these formulae that \( \sigma^4 \) fixes \( K(E'_D) \), but \( \sigma^2 \) does not. Also \( \sigma \) fixes \( R_D \). Hence we may take \( \tau \) to be restriction of \( \sigma \) to \( \text{Gal}(K(E'_D)/K) \), and the proof of the lemma is complete. \( \Box \)

**Lemma 3.5.** Let \( D = 2^a M \), where \( a = 1 \) or 3, and \( M \) is odd. Then \( K(E_M) \) has degree \( \phi(M\mathbb{Z}[i]) \) over \( K \), and \( K(E_M, D^{1/4}) \) has degree \( 4\phi(M\mathbb{Z}[i]) \) over \( K \).

**Proof.** As remarked earlier, \( K(E'_M) \) has degree \( \phi(M\mathbb{Z}[i]) \) over \( K \) because \( M \) is odd. Also, by Lemma 3.1, \( K(E'_8M) \) is the ray class field of \( K \) modulo \( 8 \), and hence we have

\[ \left[ K(E'_8M) : K \right] = 8\phi(M\mathbb{Z}[i]). \]

Since \( [K(E'_8) : K] = 8 \) by Lemma 3.1, we conclude that

\[ K(E'_M) \cap K(E'_8) = K. \] (47)

By the Weil pairing, \( K(E'_M) \) contains the field of \( |M| \)th roots of unity, and hence also \( \sqrt{M} \). Similarly, \( K(E'_8) \) contains the eighth roots of unity, and so also \( \sqrt{2} \). But \( K(\sqrt{2})/K \) is an extension of degree 2, and thus, by (47), \( \sqrt{2} \) does not belong to \( K(E'_M) \). It follows that \( \sqrt{D} \) does not belong to \( K(E'_M) \) since \( a = 1 \) or 3. Hence

\[ \left[ K(E'_M, \alpha) : K \right] = 4\phi(M\mathbb{Z}[i]). \]

But \( E \) and \( E' \) are isomorphic over \( K(\alpha) \), whence

\[ K(E'_M, \alpha) = K(E_M, \alpha). \]

On the other hand, it is clear that \( [K(E_M, \alpha) : K] \) divides \( 4\phi(M\mathbb{Z}[i]) \). It follows that

\[ [K(E_M) : K] = \phi(M\mathbb{Z}[i]), \quad [K(E_M, \alpha) : K(E_M)] = 4, \]

and the proof of the lemma is complete. \( \Box \)

We now briefly describe the theoretical steps underlying our numerical calculations of \( \text{ord}_p(c^+_p(E)) \) for the curve \( E \) when \( D \) is divisible by at least one odd prime. The Weierstrass equation associated to \( E \) is

\[ y'(z, \mathcal{L})^2 = 4\wp(z, \mathcal{L})^3 - 4D\wp(z, \mathcal{L}). \] (48)

Write \( J = J\mathbb{Z}[i] \) for the conductor of \( \psi_E \), and define
\( u = \varphi\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right) \), \quad \nu = \left(\varphi\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right)\right)/2. \tag{49} \\

By Lemma 3.1, \( K(E) \) is the ray class field of \( K \) modulo \( f \). Hence

\[ K(E) = K(u^2) = K(u), \quad \nu \in K(u), \tag{50} \]

and the degree of \( K(E) \) over \( K \) is \( d = \phi(f)/4 \). As \( f \) is divisible by at least two distinct primes of \( K \), a theorem of Cassels [2] shows that both \( u \) and \( v \) are algebraic integers. Moreover, we can compute explicitly the monic irreducible polynomial of \( u \) over \( \mathbb{Z}[i] \), which has degree \( d \), and which we denote by \( G(X) \). Once we have computed this polynomial \( G(X) \), we can determine

\[ s_m = \text{Trace}_{K(E) / K}(u^m) \quad (m = 1, 2, \ldots, d - 1) \tag{51} \]

recursively, using the following classical formula. Let

\[ G(X) = (X - u_1) \ldots (X - u_d) = X^d - \sigma_1 X^{d-1} + \cdots + (-1)^d \sigma_d, \]

where \( \sigma_1, \ldots, \sigma_d \) are the elementary symmetric functions in \( u_1, \ldots, u_d \). Then we have (see for example, [18, Vol. I, p. 81]),

\[ s_m = (-1)^{m-1} m \sigma_m + \sum_{h=1}^{m-1} (-1)^{h-1} s_{m-h} \sigma_h \quad (m \leq d). \tag{52} \]

Now we recall that, by virtue of formulae (23) and (24), we have

\[ c_p^+ (E) = -w^{-1}(f \alpha(E))^{-p} ((p - 1)!)^{-1} \mathcal{E}_p, \tag{53} \]

where \( \alpha(E) \) is as in (18), and

\[ \mathcal{E}_p = \text{Trace}_{K(E) / K}\left(\frac{\varphi^{(p-2)}\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right)}{f}\right) \]

for all odd primes \( p \). For our curve \( E = E_D \), we have \( w = 4 \). Moreover, we have

\[ \Omega_\infty^+ = \Omega / D^{1/4} \quad \text{if} \ D > 0, \quad \Omega_\infty^- = \Omega / (-D/4)^{1/4} \quad \text{if} \ D < 0, \]

where \( \Omega = 2.622058 \ldots \) is the least positive real period of the curve \( E' \) (44). Hence \( \alpha(E) = 1 \) when \( D > 0 \), and \( \alpha(E) = (1 + i) \) when \( D < 0 \). We now fix the value of \( f \) following the four cases: (i) \( D > 0 \) and \( D \equiv 1 \mod 4 \), (ii) \( D < 0 \) and \( D \equiv 1 \mod 4 \), (iii) \( D > 0 \) and \( D \equiv 1 \mod 4 \), and (iv) \( D < 0 \) and \( D \equiv 1 \mod 4 \). Following these four cases, we take \( f \) to be \( 2(1 + i) \Delta, (1 + i)^3 \Delta, 4 \Delta, \) and \( 4 \Delta \), so that the respective values of \( f \alpha(E) \) are given by \( 2(1 + i) \Delta, -4 \Delta, 4 \Delta, \) and \( 4 \Delta(1 + i) \).

As explained in the proof of Lemma 2.10, we have

\[ \varphi^{(p-2)}\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right) = B_{p-3} \left(\varphi\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right)\right) \frac{\varphi'}{\varphi}\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right), \tag{54} \]

where \( B_{p-3}(X) \) is a polynomial in \( \mathbb{Z}[X] \) of degree \( (p - 3)/2 \). This polynomial can easily computed recursively, using the differential equation (48) (see the explicit examples below when \( D = 17 \) and \( D = -14 \)).
As the theory tells us that \( v \in K(u) \), there exists a polynomial \( J(X) \) in \( K[X] \) such that
\[
\wp'(\frac{\Omega_\infty}{f}, L) = J\left(\wp\left(\frac{\Omega_\infty}{f}, L\right)\right). \tag{55}
\]
In fact, in the numerical examples we have considered, it is always the case that \( J(X) \) belongs to \( \mathbb{Z}[i][1/f][X] \), and we shall assume henceforth that this is the case. Hence, multiplying together \( B_{p-3}(X) \) and \( J(X) \), and using the fact that \( G(\wp(\Omega_\infty/f, L)) = 0 \), we deduce that
\[
\wp'(p-2)\left(\frac{\Omega_\infty}{f}, L\right) = A_p\left(\wp\left(\frac{\Omega_\infty}{f}, L\right)\right),
\]
where \( A_p(X) \) is a polynomial in \( \mathbb{Z}[i][1/f][X] \) of degree at most \( d - 1 \). Writing \( A_p(X) = \sum_{j=0}^{d-1} a_{j,p}X^j \), it follows that
\[
\Xi_p = \sum_{j=0}^{d-1} a_{j,p}^{s_j},
\]
and we can then compute \( c_p^+(E) \) using the formula (53). The machine then calculates \( \text{ord}_p(c_p^+(E)) \) (which our theory shows is always \( \geq 0 \)), followed by
\[
c_p^+(E) \mod p^k, \quad \text{where } k = \text{ord}_p(c_p^+(E)) + 1.
\]
Finally, we note that \( \tilde{E}_p(F_p) \) has order prime to \( p \) for all \( p > 5 \) with \( (p, D) = 1 \). This is clear when \( p \equiv 3 \mod 4 \), since then \( \tilde{E}_p \) is supersingular. For \( p \equiv 1 \mod 4 \), say \( p\mathbb{Z}[i] = p.p^* \), we have \( a_p = \text{Trace}_{K/Q}(\psi_E(p)) \) must be even because 2 is ramified in \( \mathbb{Q}(i) \), from which it follows that we cannot have \( a_p = 1 \), which clearly implies the assertion for these primes \( p \).

The computations described above have been carried out for the two curves \( D = 17 \) and \( D = -14 \) for all primes \( p \) with \( p \equiv 1 \mod 4 \) and \( p < 13,500 \) (the prime \( p = 17 \) is excluded when \( D = 17 \)). We have
\[
D = 17, \quad f = 2(1+i)17, \quad d = 256
\]
\[
D = -14, \quad f = 56, \quad d = 384.
\]
For both cases, the polynomials \( G(X), J(X), B_{p-3}(X), A_p(X) \) have been computed explicitly, and are given at [17], as they are too elaborate to include here. However, as an illustrative example where the coefficients are still not too enormous, we give now the polynomials \( B_{13}(X) \), which occur for \( p = 29 \),
\[
D = -14,
\]
\[
B_{13}(X) = 7496723869173 \times 2^{24}(431525237696X + 3877463640960X^3
+ 5545863414000X^5 + 2565173520000X^7 + 490959787500X^9
+ 4072477500X^{11} + 1212046875X^{13}),
\]
\[
D = 17,
\]
For these two curves, and our range of \(p\), our computations show that \(\text{ord}_p(c_p(E)) = 2\), except for the two primes \(p = 29, 277\) for the curve with \(D = -14\). Table 1 gives the value of \(c_p(E) \mod p^3\) for both curves and our \(p\) in the range \(5 \leq p < 1000\), while Table 2 gives the analogous data for \(p\) in the range \(11000 < p < 12000\). Again the values for all our \(p\) in the range \(p < 13500\) can be found at [17].

Finally, for the curve \(y^2 = x^3 + 14x\) and the two exceptional primes \(p = 29, 277\), we have

\[
c_{29}^+(E) \equiv 27 \cdot 29^3 \mod 29^4,
\]
\[
c_{277}^+(E) \equiv 155 \cdot 277^3 \mod 277^4.
\]

### Table 1

\(c_p(E) \cdot p^{-2} \mod p\) for \(5 \leq p < 1000\) and \(p \equiv 1 \mod 4\).

<table>
<thead>
<tr>
<th>(p)</th>
<th>(D = 17)</th>
<th>(D = -14)</th>
<th>(p)</th>
<th>(D = 17)</th>
<th>(D = -14)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>3</td>
<td>13</td>
<td>8</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>17</td>
<td>not valid</td>
<td>7</td>
<td>29</td>
<td>22</td>
<td>2</td>
</tr>
<tr>
<td>37</td>
<td>20</td>
<td>9</td>
<td>41</td>
<td>29</td>
<td>12</td>
</tr>
<tr>
<td>53</td>
<td>45</td>
<td>42</td>
<td>61</td>
<td>26</td>
<td>60</td>
</tr>
<tr>
<td>73</td>
<td>26</td>
<td>56</td>
<td>89</td>
<td>21</td>
<td>65</td>
</tr>
<tr>
<td>97</td>
<td>83</td>
<td>90</td>
<td>101</td>
<td>59</td>
<td>53</td>
</tr>
<tr>
<td>109</td>
<td>34</td>
<td>68</td>
<td>113</td>
<td>36</td>
<td>47</td>
</tr>
<tr>
<td>137</td>
<td>107</td>
<td>126</td>
<td>149</td>
<td>60</td>
<td>111</td>
</tr>
<tr>
<td>157</td>
<td>145</td>
<td>48</td>
<td>173</td>
<td>44</td>
<td>149</td>
</tr>
<tr>
<td>181</td>
<td>70</td>
<td>157</td>
<td>193</td>
<td>115</td>
<td>11</td>
</tr>
<tr>
<td>197</td>
<td>145</td>
<td>54</td>
<td>229</td>
<td>178</td>
<td>109</td>
</tr>
<tr>
<td>233</td>
<td>34</td>
<td>174</td>
<td>241</td>
<td>141</td>
<td>7</td>
</tr>
<tr>
<td>257</td>
<td>199</td>
<td>9</td>
<td>269</td>
<td>188</td>
<td>139</td>
</tr>
<tr>
<td>277</td>
<td>235</td>
<td>0</td>
<td>281</td>
<td>129</td>
<td>107</td>
</tr>
<tr>
<td>293</td>
<td>250</td>
<td>133</td>
<td>313</td>
<td>69</td>
<td>245</td>
</tr>
<tr>
<td>317</td>
<td>237</td>
<td>191</td>
<td>337</td>
<td>19</td>
<td>151</td>
</tr>
<tr>
<td>349</td>
<td>113</td>
<td>263</td>
<td>353</td>
<td>143</td>
<td>15</td>
</tr>
<tr>
<td>373</td>
<td>75</td>
<td>236</td>
<td>389</td>
<td>257</td>
<td>300</td>
</tr>
<tr>
<td>397</td>
<td>78</td>
<td>68</td>
<td>401</td>
<td>349</td>
<td>340</td>
</tr>
<tr>
<td>409</td>
<td>11</td>
<td>313</td>
<td>421</td>
<td>152</td>
<td>244</td>
</tr>
<tr>
<td>433</td>
<td>432</td>
<td>152</td>
<td>449</td>
<td>423</td>
<td>140</td>
</tr>
<tr>
<td>457</td>
<td>288</td>
<td>376</td>
<td>461</td>
<td>133</td>
<td>37</td>
</tr>
<tr>
<td>509</td>
<td>103</td>
<td>407</td>
<td>521</td>
<td>106</td>
<td>423</td>
</tr>
<tr>
<td>541</td>
<td>33</td>
<td>422</td>
<td>557</td>
<td>276</td>
<td>84</td>
</tr>
<tr>
<td>569</td>
<td>423</td>
<td>209</td>
<td>577</td>
<td>39</td>
<td>212</td>
</tr>
<tr>
<td>593</td>
<td>523</td>
<td>18</td>
<td>601</td>
<td>373</td>
<td>508</td>
</tr>
<tr>
<td>613</td>
<td>429</td>
<td>590</td>
<td>617</td>
<td>133</td>
<td>536</td>
</tr>
<tr>
<td>641</td>
<td>285</td>
<td>489</td>
<td>653</td>
<td>96</td>
<td>540</td>
</tr>
<tr>
<td>661</td>
<td>20</td>
<td>330</td>
<td>673</td>
<td>630</td>
<td>197</td>
</tr>
<tr>
<td>677</td>
<td>332</td>
<td>185</td>
<td>701</td>
<td>105</td>
<td>95</td>
</tr>
<tr>
<td>709</td>
<td>437</td>
<td>108</td>
<td>733</td>
<td>260</td>
<td>462</td>
</tr>
<tr>
<td>757</td>
<td>357</td>
<td>672</td>
<td>761</td>
<td>363</td>
<td>596</td>
</tr>
<tr>
<td>769</td>
<td>751</td>
<td>343</td>
<td>773</td>
<td>13</td>
<td>369</td>
</tr>
<tr>
<td>797</td>
<td>123</td>
<td>93</td>
<td>809</td>
<td>443</td>
<td>212</td>
</tr>
<tr>
<td>821</td>
<td>6</td>
<td>347</td>
<td>829</td>
<td>645</td>
<td>823</td>
</tr>
<tr>
<td>853</td>
<td>48</td>
<td>635</td>
<td>857</td>
<td>5</td>
<td>502</td>
</tr>
<tr>
<td>877</td>
<td>132</td>
<td>603</td>
<td>881</td>
<td>82</td>
<td>591</td>
</tr>
<tr>
<td>929</td>
<td>845</td>
<td>766</td>
<td>937</td>
<td>341</td>
<td>100</td>
</tr>
<tr>
<td>941</td>
<td>253</td>
<td>642</td>
<td>953</td>
<td>794</td>
<td>866</td>
</tr>
<tr>
<td>977</td>
<td>548</td>
<td>98</td>
<td>997</td>
<td>302</td>
<td>401</td>
</tr>
</tbody>
</table>
Table 2

c^p_p(E) \cdot p^{−2} \mod p \text{ for } 11000 < p < 12000 \text{ and } p \equiv 1 \mod 4.

<table>
<thead>
<tr>
<th>p</th>
<th>D = 17</th>
<th>D = −14</th>
<th>p</th>
<th>D = 17</th>
<th>D = −14</th>
</tr>
</thead>
<tbody>
<tr>
<td>11057</td>
<td>3236</td>
<td>10336</td>
<td>11069</td>
<td>7768</td>
<td>6637</td>
</tr>
<tr>
<td>11093</td>
<td>9234</td>
<td>5437</td>
<td>11113</td>
<td>832</td>
<td>9242</td>
</tr>
<tr>
<td>11117</td>
<td>6204</td>
<td>7965</td>
<td>11149</td>
<td>8885</td>
<td>1364</td>
</tr>
<tr>
<td>11161</td>
<td>1292</td>
<td>1636</td>
<td>11173</td>
<td>587</td>
<td>10503</td>
</tr>
<tr>
<td>11177</td>
<td>6184</td>
<td>4427</td>
<td>11197</td>
<td>8804</td>
<td>6750</td>
</tr>
<tr>
<td>11213</td>
<td>6409</td>
<td>8508</td>
<td>11257</td>
<td>192</td>
<td>1839</td>
</tr>
<tr>
<td>11261</td>
<td>700</td>
<td>6850</td>
<td>11273</td>
<td>5932</td>
<td>510</td>
</tr>
<tr>
<td>11317</td>
<td>1969</td>
<td>2892</td>
<td>11321</td>
<td>5451</td>
<td>10042</td>
</tr>
<tr>
<td>11329</td>
<td>5635</td>
<td>9145</td>
<td>11353</td>
<td>3322</td>
<td>7820</td>
</tr>
<tr>
<td>11369</td>
<td>6790</td>
<td>11276</td>
<td>11393</td>
<td>4532</td>
<td>358</td>
</tr>
<tr>
<td>11437</td>
<td>10570</td>
<td>3120</td>
<td>11489</td>
<td>8715</td>
<td>10941</td>
</tr>
<tr>
<td>11497</td>
<td>4837</td>
<td>6424</td>
<td>11549</td>
<td>7265</td>
<td>2757</td>
</tr>
<tr>
<td>11593</td>
<td>225</td>
<td>369</td>
<td>11597</td>
<td>8864</td>
<td>7113</td>
</tr>
<tr>
<td>11617</td>
<td>10691</td>
<td>1052</td>
<td>11621</td>
<td>7500</td>
<td>6521</td>
</tr>
<tr>
<td>11633</td>
<td>293</td>
<td>5463</td>
<td>11657</td>
<td>10665</td>
<td>4770</td>
</tr>
<tr>
<td>11677</td>
<td>10365</td>
<td>11566</td>
<td>11681</td>
<td>6023</td>
<td>5351</td>
</tr>
<tr>
<td>11689</td>
<td>11553</td>
<td>3152</td>
<td>11701</td>
<td>5851</td>
<td>11618</td>
</tr>
<tr>
<td>11717</td>
<td>10185</td>
<td>8521</td>
<td>11777</td>
<td>10882</td>
<td>3487</td>
</tr>
<tr>
<td>11789</td>
<td>6221</td>
<td>3509</td>
<td>11801</td>
<td>10632</td>
<td>3148</td>
</tr>
<tr>
<td>11813</td>
<td>2123</td>
<td>3767</td>
<td>11821</td>
<td>7340</td>
<td>128</td>
</tr>
<tr>
<td>11833</td>
<td>1715</td>
<td>9412</td>
<td>11897</td>
<td>8766</td>
<td>10281</td>
</tr>
<tr>
<td>11909</td>
<td>6032</td>
<td>11519</td>
<td>11933</td>
<td>1190</td>
<td>1783</td>
</tr>
<tr>
<td>11941</td>
<td>5023</td>
<td>6379</td>
<td>11953</td>
<td>10988</td>
<td>1162</td>
</tr>
<tr>
<td>11969</td>
<td>11669</td>
<td>11573</td>
<td>11981</td>
<td>1742</td>
<td>8384</td>
</tr>
</tbody>
</table>

Acknowledgment

We are grateful to C. Wuthrich for his comments on our work, and some independent numerical calculations based on [16].

References