The Tate-Shafarevich group for elliptic curves with complex multiplication II

J. Coates, Z. Liang, R. Sujatha

May 28, 2010

1 Introduction

Let $E$ be an elliptic curve over $\mathbb{Q}$. Put $g_{E/\mathbb{Q}} = \text{rank of } E/\mathbb{Q}$, and

$$\Sha(E/\mathbb{Q}) = \text{Ker} \left( H^1(\mathbb{Q}, E) \to \bigoplus_v H^1(\mathbb{Q}_v, E) \right),$$

where $v$ runs over all places of $\mathbb{Q}$, with $\mathbb{Q}_v$ the completion of $\mathbb{Q}$ at $v$. Although no algorithm has ever been proven to work infallibly, the group $E(\mathbb{Q})$ is, in fact, easy to determine in practice. By contrast, $\Sha(E/\mathbb{Q})$ is extremely difficult to study either theoretically or numerically. The aim of the present paper is to strengthen the theoretical and numerical results of [1], assuming $E$ has complex multiplication.

For each prime $p$, let $t_{E/\mathbb{Q}, p}$ denote the $\mathbb{Z}_p$-corank of the $p$-primary subgroup of $\Sha(E/\mathbb{Q})$.

**Theorem 1.1.** Assume that $E/\mathbb{Q}$ admits complex multiplication. For each $\epsilon > 0$, there exists an explicitly computable number $c(E, \epsilon)$ such that

$$t_{E/\mathbb{Q}, p} \leq (1/2 + \epsilon)p - g_{E/\mathbb{Q}}$$

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

Of course, this result is a far cry from the standard conjecture that $t_{E/\mathbb{Q}, p} = 0$ for every prime $p$. Our method of proof is similar to that given in [1], but we obtain the stronger result by employing an interesting observation of Katz [2] about the divisibility of the relevant $L$-values by primes where $E$ has good supersingular reduction. However, we stress that Katz’s work is used to obtain information about the Iwasawa theory at good ordinary primes $p$, and we have no idea at present how to prove a result like (1) for all sufficiently large primes $p$ where $E$ has good supersingular reduction.

Secondly, we extend the numerical computations of $t_{E/\mathbb{Q}, p}$ given in [1] for certain $E$ with $g_{E/\mathbb{Q}} \geq 2$. Let

$$E : y^2 = x^3 - 82x.$$
Then \( g_{E/Q} = 3 \) and \( E(Q) \) modulo torsion is generated by the points
\((-9, 3), (-8, 12), (-1, 9).\)

The conjecture of Birch and Swinnerton-Dyer predicts that \( \III(E/Q) = 0 \) for this curve, but of course this is unproven, and we do not know whether \( \III(E/Q) \) is even finite.

1.2 Theorem 1.2. For the elliptic curve (2), we have \( \III(E/Q)(p) = 0 \) for all primes \( p \equiv 1 \mod 4 \) with \( p \neq 41 \) and \( p < 30,000 \).

In fact, a different and more subtle technique than that used in [1] is required to carry out these computations, because this earlier method relies on calculating traces from the field of 328-division points on the curve (2). This field has the enormous degree 12,800 over \( Q(i) \) (the integer 328 occurs here because the conductor of the Grössencharacter of the curve is \( 328Z[i] \)), and we have been unable to find the minimal equation over \( Q(i) \) of the \( x \)-coordinate of a 328-division point. By some curious arguments in Galois theory (see Lemma 4.4 and (74)), we show that it suffices to work with a subfield of degree 6,400 over \( Q(i) \), and, with the help of MAGMA, we have succeeded in explicitly computing the minimal polynomial of a natural generator for this subfield over \( Q(i) \) (the \( x \)-coordinate of a 328/(1 + i)-division point).

Moreover, using the same technique of calculation, we have also carried out computations on the five curves of rank 2 given by
\[ E_i : y^2 = x^3 - D_ix, \] with \( D_1 = -14, D_2 = 17, D_3 = -33, D_4 = -34, D_5 = -39, \)

extending the numerical results given in [1] for the curves \( E_1 \) and \( E_2 \).

1.3 Theorem 1.3. For each of the curves \( E_i \) \( (i = 1, \cdots, 5) \), \( \III(E_i/Q)(p) \) is finite for all primes \( p \) of good reduction with \( p \equiv 1 \mod 4 \) and \( p < 30,000 \). Moreover, \( \III(E_i/Q)(p) = 0 \) for all such \( p \), except possibly in the four exceptional cases given by \( p = 29 \) and 277 for the curve \( E_1 \), \( p = 577 \) for the curve \( E_4 \), and \( p = 17 \) for the curve \( E_5 \).

In fact the conjecture of Birch and Swinnerton-Dyer predicts that \( \III(E_i/Q) = 0 \) for \( i = 1, \cdots, 5 \). We ourselves have not successfully carried out the calculations of \( p \)-adic heights to verify that \( \III(E_i/Q)(p) = 0 \) in the four exceptional cases of Theorem 1.3 (our claim to have done this for the primes \( p = 29 \) and 277 for \( E_1 \) in [1] is not correct). However, we are very grateful to C. Wuthrich for computing the \( p \)-adic heights for the three exceptional primes \( p = 17, 29, \) and 277, thereby confirming that \( \III(E_i/Q)(p) = 0 \) for the relevant curves for these primes (the remaining exxceptional prime of 577 for the curve \( E_4 \) remains unsettled).

Finally, we would like to thank Allan Steel and Mark Watkins for their help in factoring polynomials.
2 Divisibility of \( L \)-values by supersingular primes

As Katz has pointed out in [2], the special values of complex \( L \)-functions attached to elliptic curves with complex multiplication tend to be highly divisible by supersingular primes. In this section, we use his method to establish the precise version of his results needed to prove Theorem 1.1.

The following notation will be used throughout the rest of this paper. Let \( K \) be an imaginary quadratic field embedded in the field \( \mathbb{C} \) of complex numbers, and \( \mathcal{O}_K \) its ring of integers. Let \( E \) be an elliptic curve defined over \( K \) such that \( \text{End}_K(E) \simeq \mathcal{O}_K \).

The existence of such a curve implies that \( K \) necessarily has class number 1. We fix a global minimal Weierstrass equation for \( E \)

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

whose coefficients belong to \( \mathcal{O}_K \). Let \( \psi_E \) denote the Grössencharacter of \( E \) over \( K \), and write \( f \) for the conductor of \( \psi_E \). For each integer \( n \geq 1 \), define

\[
L_f(\overline{\psi}_E^n, s) = \prod_{(v,f)=1} \left( 1 - \frac{\overline{\psi}_E^n(v)}{(Nv)^s} \right)^{-1}.
\]

This \( L \)-function is not, in general, primitive, and we write \( L(\overline{\psi}_E^n, s) \) for the primitive Hecke \( L \)-function of \( \overline{\psi}_E^n \).

Let \( \mathcal{L} \) be the period lattice of the Néron differential of the equation (3), and let

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

be the isomorphism given by

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

where \( \varphi(z, \mathcal{L}) \) denotes the Weierstrass \( \varphi \)-function attached to \( \mathcal{L} \). We also fix \( \Omega_\infty \) in \( \mathcal{L} \) such that \( \mathcal{L} = \Omega_\infty \mathcal{O}_K \).

As we shall see in the proof of the next theorem, the numbers

\[
\Omega_\infty^{-n}L(\overline{\psi}_E^n, n) \ (n = 1, 2, ...)
\]

all belong to \( K \). Our goal is to use Katz’s method to establish the following specific result. If \( b \) is a real number, \( \lfloor b \rfloor \) will denote as usual the largest integer \( \leq b \).
Theorem 2.1. Let $q$ be an odd prime number which is inert in $K$. Assume that $E$ has good reduction at $v = q\mathcal{O}_K$. Then, for all integers $n \geq 3$, which are not congruent to $1 + q$ modulo $(q^2 - 1)$, we have

$$\text{ord}_v((n - 1)!\Omega_{\infty}^{-n}L_f(\tilde{\psi}_E^{n}, n)) \geq \left\lfloor \frac{nq}{(q^2 - 1)} \right\rfloor - 1.$$ 

The proof of this theorem will take up the rest of this section. The initial arguments, although subsequently used for supersingular primes, are motivated by the well known construction of the $p$-adic $L$-functions of $E$ in the ordinary case (see [3], [4]). If $\alpha$ is any non-zero element of $\mathcal{O}_K$, let $E_\alpha$ denote the kernel of multiplication by $\alpha$ on $E(K)$. Fix for the rest of the paper an element $f$ of $\mathcal{O}_K$ such that $f = f\mathcal{O}_K$. The field

$$F = K(E_f)$$

will play an important role in both our theoretical and numerical arguments. It is an abelian extension of $K$, which is ramified precisely at the bad primes of $E$ over $K$, and it coincides with the ray class field of $K$ modulo $f$ (see, for example, [4], Chap. 2). Moreover, if $w$ is any good prime of $E/K$, we have

$$\psi_E(w)(U) = U^\tau_w$$

for all $U$ in $E_f$, where $\tau_w$ denotes the Artin symbol of $w$ for $F/K$. Put

$$G = \text{Gal}(F/K).$$

Let $\lambda$ be any element of $\mathcal{O}_K$, which is not a unit, and which is relatively prime to $6fq$. Let $J_\lambda$ denote the set of all non-zero elements in $E_f$. Define

$$R_\lambda(P) = c_E(\lambda)\prod_U(x(P) - x(U))^{-1},$$

where $U$ runs over any set of representatives of $J_\lambda$ modulo the action of the group $\mu_2$ of square roots of unity, and $c_E(\lambda)$ is the unique non-zero element of $K$, whose existence is established in [6] (see Proposition 1 of the Appendix). Thus $R_\lambda(P)$ is a rational function on $E$ with coefficients in $K$. Let $V = \Phi(\Omega_{\infty}/f, \mathcal{L})$, and define

$$\mathcal{R}_\lambda(P) = \prod_{\tau \in G} R_\lambda(P \oplus V^\tau),$$

where $\oplus$ denotes the group law on $E$. Thus $\mathcal{R}_\lambda(P)$ is also a rational function on $E$, with coefficients in $K$. In view of (8) and Theorem 3 of the Appendix of [6], we have

$$\mathcal{R}_\lambda(\psi_E(w)(P)) = \prod_{S \in E_w} \mathcal{R}_\lambda(P \oplus S)$$
for each prime \( w \) of \( K \), where \( E \) has good reduction for \( E/K \). Hence, defining

\[
\Psi_\lambda(P) = \mathcal{R}_\lambda(P)^{N_v} / \mathcal{R}_\lambda(\psi_E(v)(P)),
\]

it follows from (12) with \( w = v \) that

\[
\prod_{S \in E_q} \Psi_\lambda(P \oplus S) = 1.
\]

The following result shows that the function \( \Psi_\lambda(P) \) is related to \( L \)-values. For each integer \( n \geq 1 \), put

\[
L_n = (n-1)! \Omega_\infty^{-n} L_{f}(\psi^n_E, n).
\]

**Proposition 2.2.** For all integers \( n \geq 1 \), we have

\[
(Nv)^{-1} \left( \frac{d}{dz} \right)^n \log \Psi_\lambda(\Phi(z, L))_{z=0} = (-1)^{n-1} f^n (N \lambda - \psi_E((\lambda))^n) \left( 1 - \frac{\psi_E(v)^n}{Nv} \right) L_n.
\]

**Proof.** This is a very classical calculation (see for example [3]), and we only sketch the main points in the proof. Put \( \pi = \psi_E(v) \). Since \( \pi(\Phi(z, L)) = \Phi(\pi z, L) \), we conclude from (13) that it suffices to prove that, for all integers \( n \geq 1 \),

\[
\left( \frac{d}{dz} \right)^n \log \mathcal{R}_\lambda(\Phi(z, L))_{z=0} = (-1)^{n-1} f^n (N \lambda - \psi_E((\lambda))^n) L_n.
\]

Let

\[
\theta(z, L) = \exp \left( -s_2(L) z^2 / 2 \right) \sigma(z, L),
\]

where \( \sigma(z, L) \) is the Weierstrass \( \sigma \)-function of \( L \) and, as usual,

\[
s_2(L) = \lim_{s \to 0} \sum_{w \in L(0)} w^{-2} |w|^{-2s}.
\]

Then we have (see, for example, [3, Theorem 1.9])

\[
\mathcal{R}_\lambda(\Phi(z, L))^2 = c_E(\lambda)^{2d} \prod_{b \in B} \theta^2(z + \psi_E(b) \frac{\Omega_\infty}{f}, L)^{N_L} / \theta^2(z + \psi_E(b) \frac{\Omega_\infty}{f}, \lambda^{-1} L),
\]

where \( B \) is any set of integral ideals of \( K \) whose Artin symbols for \( F/K \) give precisely the elements of the Galois group \( G \), and \( d = [F : K] \).

For each integer \( n \geq 1 \), let \( E_n^T(z, L) \) be the value at \( s = n \) of the analytic continuation of the Kronecker series

\[
H_n(z, s, L) = \sum_{w \in L} \frac{(\bar{z} + \bar{w})^n}{|z + w|^{2s}}.
\]
As usual, let \( A(\mathcal{L}) = (uv - v\bar{u})/2\pi i \), where \( u, v \) is any \( \mathbb{Z} \)-basis of \( \mathcal{L} \) with \( v/u \) having positive imaginary part. Then we have (see \([5, \text{Corollary 1.7}]\)), for any \( \rho \) in \( \mathbb{C} \setminus \mathcal{L} \),

\[
\frac{d}{dz} \log(\theta(z + \rho, \mathcal{L})) = \frac{\bar{\rho}}{A(\mathcal{L})} + \sum_{n=1}^{\infty} (-1)^{n-1} E_n^*(\rho, \mathcal{L}) z^{n-1}.
\]

Since \( A(\lambda^{-1} \mathcal{L}) = A(\mathcal{L})/N\lambda, \ E_n^*(z, \lambda^{-1} \mathcal{L}) = \psi_E((\lambda))^n E_n^*(\psi_E((\lambda))z, \mathcal{L}) \), it follows easily from (18) and (19), on putting

\[
\mathcal{D}_\lambda = \left( \frac{d}{dz} \right)^n \log \Re(\Phi(z, \mathcal{L}))_{|z=0},
\]

that

\[
\mathcal{D}_\lambda = (-1)^{n-1} (n-1)! \sum_{b \in B} \left( N\lambda E_n^*(\psi_E(b) \frac{\Omega_\infty}{f}, \mathcal{L}) - \psi_E((\lambda))^n E_n^*(\psi_E(b \cdot (\lambda)) \frac{\Omega_\infty}{f}, \mathcal{L}) \right).
\]

On the other hand, it is easily seen that, for all integers \( n \geq 1 \), we have

\[
L_f(\psi_E^n, s) = \frac{|\Omega_\infty/f|^2 s}{(\Omega_\infty/f)^n} \sum_{b \in B} \left( \psi_E(b) \frac{\Omega_\infty}{f}, s, \mathcal{L} \right).
\]

This completes the proof of (17), and so also of Proposition 2.2. \( \square \)

We now turn to the \( v \)-adic properties of our function \( \Psi_\lambda(P) \). Let \( \hat{E}^v \) be the formal group of \( E \) at \( v \), which is defined over \( \mathcal{O}_v \), and has parameter \( t = -x/y \). It can be shown that the action of \( \mathcal{O}_K \) on \( E \) extends to an action of \( \mathcal{O}_v \) on \( \hat{E}^v \). If \( a \) is any element of \( \mathcal{O}_v \), we write \([a](t)\) for the formal power series in \( \mathcal{O}_v[[t]] \) giving the corresponding endomorphism of \( \hat{E}^v \). As before, put \( \pi = \psi_E(v) \). Since the reduction modulo \( v \) of the endomorphism \( \pi \) of \( E \) gives the Frobenius endomorphism of the reduced curve, we plainly have

\[
[t](t) \equiv t^{N_v} \mod q.
\]

As \([a](t) = at + \cdots \) for all \( a \in \mathcal{O}_v \), it follows from (22) that \( \hat{E}^v \) is in fact a Lubin-Tate group over \( \mathcal{O}_v \) for the local parameter \( \pi \).

**Lemma 2.3.** Let \( A_\lambda(t) \) be the \( t \)-expansion of \( \Psi_\lambda(P) \). Then \( A_\lambda(t) \) belongs to \( 1 + q\mathcal{O}_v[[t]] \).

**Corollary 2.4.** Defining

\[
C_\lambda(t) = (Nv)^{-1} \log A_\lambda(t),
\]

we have \( qC_\lambda(t) \) belongs to \( \mathcal{O}_v[[t]] \).
Proof. Let $B_{\lambda}(t)$ be the $t$-expansion of $R_{\lambda}(P)$. A standard argument (see the proof of Lemma 8 in [6]), based on the explicit expression (10), shows that $B_{\lambda}(t)$ is a unit in $O_v[[t]]$. It follows that $B_{\lambda}(\pi(t))$ is also a unit in $O_v[[t]]$, whence we conclude from (13) that $A_{\lambda}(t)$ belongs to $O_v[[t]]$. Moreover, writing $B_{\lambda}(t) = \sum_{n=0}^{\infty} b_n t^n$, we deduce from (22) that

$$B_{\lambda}(\pi(t)) = \sum_{n=0}^{\infty} b_n (\pi(t))^n \equiv \sum_{n=0}^{\infty} b_n t^{nN_v} \mod q.$$  

(24)

On the other hand, as $b_n^{N_v} \equiv b_n \mod q$, one has

$$B_{\lambda}(t)^{N_v} \equiv \sum_{n=0}^{\infty} b_n t^{nN_v} \mod q.$$  

(25)

It follows immediately from (24) and (25) that $A_{\lambda}(t) \equiv 1 \mod q$, completing the proof of Lemma 2.3. The corollary is immediate since $\log A_{\lambda}(t)$ then belongs to $qO_v[[t]]$, since $q$ is odd.

Define

$$C_{\lambda}^*(t) = qC_{\lambda}(t).$$  

(26)

By Corollary (2.4), $C_{\lambda}^*(t)$ belongs to $O_v[[t]]$, and, by (14),

$$\sum_{R \in E_q} C_{\lambda}^*(t[+])t(R) = 0,$$  

(27)

where $[+]$ denotes the formal group law on $\hat{E}^q$. Here $t(R)$ runs over the $q$-division points on $\hat{E}^q$ as $R$ runs over $E_q$. Katz’s argument applies to any power series in $O_v[[t]]$ satisfying (27).

2.5 Proposition 2.5. (Katz [K]) Let $g(t)$ be any power series in $O_v[[t]]$ satisfying

$$\sum_{R \in E_q} g(t[+])t(R) = 0.$$  

(28)

Then, for all integers $n \geq 1$, we have

$$\left( \frac{d}{dz} \right)^n g(t) \in q^{\frac{nq}{q^2-1}} O_v[[t]].$$

We now briefly describe Katz’s proof. It is convenient to replace $\hat{E}^q$ by an isomorphic Lubin-Tate group. Let $E$ be the Lubin-Tate group over $O_v$ attached to the local parameter $\pi$, and satisfying

$$[\pi](w) = \pi w + w^{N_v},$$  

(29)

where $[\pi](w)$ now denotes the endomorphism of $E$ defined by $\pi$. By Lubin-Tate theory, there exists an $O_v$-isomorphism

$$\eta : E \simeq \hat{E}^q.$$  

(30)
which is given by a formal power series \( t = \eta(w) \) in \( \mathcal{O}_v[[w]] \). Defining \( h(w) = g(\eta(w)) \), we then have

\[
\sum_{u \in \mathcal{E}_q} h(w[u]) = 0,
\]

where \([+]\) also denotes the formal group law on \( \mathcal{E} \), and \( \mathcal{E}_q \) is the group of \( q \)-division points on \( \mathcal{E} \). The isomorphism \( \xi \) enables us to write \( z = \varepsilon(t) \), where \( \varepsilon(t) \) is a power series in \( K_v[[t]] \). It is then easy to see that

\[
z = \nu(w), \quad \text{where } \nu(w) = \varepsilon(\eta(w))
\]
is the logarithm map of \( \mathcal{E} \), and that it suffices to show that, for all integers \( n \geq 1 \),

\[
\left( \frac{d}{dz} \right)^n h(w) \in q^{\left\lfloor \frac{n}{2} \right\rfloor} \mathcal{O}_v[[w]].
\]

Note that the operator

\[
\frac{d}{dz} = \frac{1}{\nu'(w)} \frac{d}{dw}
\]
maps \( \mathcal{O}_v[[w]] \) into itself, since \( \nu'(w) \) is a unit in \( \mathcal{O}_v[[w]] \) by a well known property of formal groups.

For each \( r(w) \) in \( \mathcal{O}_v[[w]] \), we define \( D_n r(w) \) \((n \geq 0)\) in \( \mathcal{O}_v[[w]] \) by the expansion

\[
r(w[u]) = \sum_{n=0}^{\infty} D_n r(w) u^n,
\]

where \( u \) is an independent variable.

**2.6 Lemma 2.6.** For \( n = 0, 1, \ldots, Nv - 1 \), we have

\[
D_n r(w) = \frac{1}{n!} \left( \frac{d}{dz} \right)^n r(w).
\]

**Proof.** Since \( r(w[u]u_1[u]u_2) = r(w[u]u_2[u]u_1) \), we obtain

\[
D_{n_1}(D_{n_2} r(w)) = D_{n_2}(D_{n_1} r(w)) \quad (n_1, n_2 \geq 0).
\]

Also, as \( \nu(w[u]) = \nu(w) + \nu(u) \), we have

\[
\frac{\partial}{\partial u} (w[u]) = \nu'(u)/\nu'(w[u]),
\]
and hence

\[
\frac{\partial}{\partial u} r(w[u]) = r'(w[u])\nu'(u)/\nu'(w[u]).
\]
Putting \( u = 0 \) in this equation, and noting that \( \nu'(0) = 1 \), it follows that \( D_1 r(w) = r'(w)/\nu'(w) \). Thus the above equation can be rewritten as

\[
\frac{\partial}{\partial u} r(w[+]u) = \nu'(u)(D_1 r)(w[+]u).
\]

Recalling \((37)\), this then gives the identity

\[
\sum_{n=1}^{\infty} n D_n r(w) u^{n-1} = \nu'(u) \sum_{n=0}^{\infty} D_n r((w)) u^n.
\]

Also, as \( \nu([\pi](w)) = \pi \nu(w) \), one easily deduces from \((29)\) that

\[
\nu'(w) \equiv 1 \mod w^{Nv-1}.
\]

Combining \((39)\) and \((40)\), we immediately obtain \( D_n r = D_1(D_{n-1} r)/n \) for \( n = 1, \ldots, Nv-1 \), and the assertion of the lemma follows by induction on \( n \).

Since \( \text{ord}_q((Nv-1)!)) = q-1 \), it follows immediately from Lemma \(2.6\) that, for each \( r(w) \) in \( \mathcal{O}_v[[w]] \), \( (\frac{d}{dz})^{Nv-1} r(w) \) belongs to \( q^{q-1} \mathcal{O}_v[[w]] \). The next lemma establishes a stronger result, provided \( r(w) \) satisfies \((41)\).

2.7 Lemma 2.7. Let \( r(w) \) be any power series in \( \mathcal{O}_v[[w]] \) satisfying \((41)\). Then

\[
\left( \frac{d}{dz} \right)^{Nv-1} r(w) \in q^q \mathcal{O}_v[[w]].
\]

Proof. Combining \((35)\) and \((41)\) gives

\[
\sum_{n=0}^{\infty} \left( \sum_{\eta \in \mathcal{E}_q} \eta^n \right) D_n r(w) = 0.
\]

By \((29)\), we see that the non-zero elements of \( \mathcal{E}_q \) are given by the \( \alpha \zeta \), where \( \zeta \) runs over the \((Nv-1)\)-th roots of unity, and \( \alpha^{Nv-1} = -\pi \). Thus the \( n \)-th term in \((43)\) is zero unless \( Nv-1 \) divides \( n \), and, when \( Nv-1 \) does divide \( n \), we have

\[
\sum_{\eta \in \mathcal{E}_q} \eta^n = (Nv-1)\alpha^n (n > 0).
\]

Hence \((43)\) can be written as

\[
q^2 r(w) + \sum_{m=1}^{\infty} (Nv-1)(-\pi)^m D_m(Nv-1) r(w) = 0.
\]

But this last equation clearly implies that

\[
D_{Nv-1} r(w) \in q \mathcal{O}_v[[w]],
\]

and the assertion of the lemma now follows from Lemma \(2.6\) and the remarks made immediately before \((41)\). \( \square \)
Lemma 2.8. Let \( r(w) \) be any element of \( \mathcal{O}_v[[w]] \) satisfying (41). Then, for all integers \( n \geq 0 \), we have

\[
\left( \frac{d}{dz} \right)^n r(w) \in q^{\left\lfloor \frac{nq}{Nv} \right\rfloor} \mathcal{O}_v[[w]].
\]

Proof. Assume \( n \geq 1 \), and write \( n = (Nv - 1)b + a \), where \( b \geq 0 \) and \( 0 \leq a < Nv - 1 \). Now

\[
\left\lfloor \frac{nq}{Nv - 1} \right\rfloor = \left\lfloor \frac{aq}{Nv - 1} \right\rfloor + bq,
\]

and

\[
\left\lfloor \frac{aq}{Nv - 1} \right\rfloor = \text{ord}_q(a!).
\]

The assertion of the lemma is now plain from (36) and (42).

We can now complete the proof of Theorem 2.1. Proposition 2.5 follows immediately from applying Lemma 2.8 to the function \( h(w) \). In turn, applying Proposition 2.5 to the power series \( C_\lambda(t) \) given by (26), and recalling that \( (f, v) = 1 \), we conclude from Proposition 2.2 that, for all integers \( n \geq 1 \),

\[
\text{ord}_v \left( (N\lambda - \psi_E((\lambda))^n \left( 1 - \frac{\psi_E(v)^n}{Nv} \right) L_n \right) \geq \left\lfloor \frac{nq}{Nv - 1} \right\rfloor - 1.
\]

Assuming that \( n \geq 3 \), it is clear that \( 1 - (\psi_E(v)^n/Nv) \) is a \( v \)-adic unit. Now choose \( \lambda \) to be any element of \( \mathcal{O}_K \) such that \( (\lambda, 6) = 1 \), \( \lambda \equiv 1 \mod f \), and \( \lambda \mod v \) is a generator of \( (\mathcal{O}_K/v\mathcal{O}_K)^\times \). As \( \lambda \equiv 1 \mod f \), \( \psi_E((\lambda)) = \lambda \), and thus

\[
N\lambda - \psi_E((\lambda))^n = \lambda(\bar{\lambda} - \lambda^{n-1}) \equiv \lambda(\lambda^q - \lambda^{n-1}) \mod v.
\]

Since \( \lambda \mod v \) is a generator of \( (\mathcal{O}_K/v\mathcal{O}_K)^\times \), it follows that (46) is prime to \( q \) provided \( n \) is not congruent to 1 + \( q \mod Nv - 1 \). This completes the proof of Theorem 2.1.

3 Application to the Tate-Shafarevich group

In this section, we combine Theorem 2.1 with Iwasawa theory to prove Theorem 1.1. Throughout the section, \( c_1, c_2, \ldots \) will denote positive integers which depend only on the coefficients of the equation (3), and which could be made explicit if desired. Also, \( J \) will denote the set of all prime numbers \( q \) such that \( q \) is inert in \( K \), and \( E \) has good reduction at \( q\mathcal{O}_K \).

For the moment, let \( p \) be any odd prime number. Put

\[
P(p) = \prod_{q | p} q^{\nu_q}, \text{ where } \nu_q = \left\lfloor \frac{pq}{q^2 - 1} \right\rfloor - 1.
\]
Lemma 3.1. For each odd prime $p$, we have

\[ \mathcal{P}(p) \geq p^{n/2}/c_1^p. \]

Proof. Clearly

\[ \nu_q \geq \left[ \frac{p}{q} \right] - 1 \geq \frac{p}{q} - 2, \]

and so

\[ \log \mathcal{P}(p) \geq p \sum_{q \leq p, q \in J} \frac{\log q}{q} - 2 \sum_{q \leq p} \log q. \]

By a weak form of the prime number theorem, we have

\[ \sum_{q \leq p} \log q < \sum_{q \leq p} \log q \leq c_2 p. \]

Let $\chi$ be the Dirichlet character corresponding to the extension $K/\mathbb{Q}$, and let $t$ be its conductor. Define

\[ \mathcal{M}(p) = \sum_{\chi(q) = -1, q \leq p} \frac{\log q}{q}, \]

where the sum is taken over all primes $q \leq p$ with $\chi(q) = -1$. Plainly

\[ 0 \leq \mathcal{M}(p) - \sum_{q \leq p} \frac{\log q}{q} \leq c_3. \]

Combining (49), (50), and (52), we obtain

\[ \log \mathcal{P}(p) \geq p\mathcal{M}(p) - c_4 p. \]

Now a well known equivalent form of Dirichlet’s theorem on primes in arithmetic progressions asserts that, for any real $x \geq 2$, and each integer $q$ with $(a, t) = 1$, we have

\[ \left| \sum_{q \equiv a \mod t, q \leq x} \frac{\log q}{q} - \frac{1}{e(t)} \log x \right| \leq c_5, \]

where the sum on the left is over all prime numbers $q \leq x$ with $q \equiv a \mod t$, and $e(t)$ denotes the order of the group of units of $\mathbb{Z}/t\mathbb{Z}$. Now precisely half of the classes $a \mod t$ with $(a, t) = 1$ satisfy $\chi(a) = -1$. Taking $x = p$, we conclude from (54) that

\[ \left| \mathcal{M}(p) - \frac{\log p}{2} \right| \leq c_6. \]
The assertion of the lemma now follows immediately on combining (53) and (55). □

The proof of Theorem 1.1 now proceeds exactly as in the proof of Theorem 2.8 of [1], except we exploit Katz’s divisibility assertion (6). Thus we now take \( p \) to be any odd prime with \( \mathcal{O}_K = \mathcal{O}_K^{\mathbb{P}} \) and \( \mathbb{P} \neq \mathbb{P}^* \), such that \( E \) has good reduction at both \( \mathbb{P} \) and \( \mathbb{P}^* \).

Then there exists a positive rational integer \( c_7 \), depending only on the equation (3), such that

\[
\xi(p) = c_7(p-1)! \Omega_{\infty}^{\mathbb{P}} L_{l}(\psi_{E/K},p) / P(p)
\]

remains a non-zero algebraic integer in \( K \). In view of Lemma 3.1 and [1, Lemma 2.9], we have

\[
|\xi(p)| \leq c_7^p p^{p/2}.
\]

Thus, using the product formula for \( K \), we conclude that

\[
|\xi(p)|_p \cdot |\xi(p)|_{p^*} \geq c_7^{2p} p^{-p} \geq p^{-(1+\epsilon)p};
\]

here the last inequality holds for any \( \epsilon > 0 \), provided \( p \) is sufficiently large. On the other hand, applying the main conjectures of Iwasawa theory (which are in fact proven theorems) for \( E \) over the unique \( \mathbb{Z}_p \)-extensions of \( K \) which are unramified outside \( \mathbb{P} \) and \( \mathbb{P}^* \), respectively, it follows that (see the proof of Theorem 2.1 in [1])

\[
|\xi(p)|_p \cdot |\xi(p)|_{p^*} \leq p^{-2(n_{E/K}+t_p)},
\]

where \( n_{E/K} \) is the \( \mathcal{O}_K \)-rank of \( E(K) \), and \( t_p \) is the \( \mathbb{Z}_p \)-corank of III(\( E/K \))(\( p \)) (which can be shown to be equal to the \( \mathbb{Z}_p \)-corank of III(\( E/K \))(\( p^* \))). Thus, combining (58) and (59), we have proven the following stronger form of Theorem 2.8 of [1]:

**Theorem 3.2.** Let \( \epsilon \) be any positive number. Then, for all sufficiently large odd primes \( p \) such that \( p \mathcal{O}_K = \mathcal{O}_K^{\mathbb{P}} \), \( t_p \) is bounded above by \( (1/2 + \epsilon)p - n_{E/K} \).

Finally, we note that Theorem 1.1 is an immediate corollary of this result, because, when \( E \) is defined over \( \mathbb{Q} \) we have \( n_{E/K} = g_{E/\mathbb{Q}} \) and \( t_p = t_{E/\mathbb{Q},p} \). This completes the proof of Theorem 1.1. □

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

We explain in this section the improvements in the computational technique of [1], which enables us to prove Theorem 1.2 and Theorem 1.3. As in [1], we consider the family of curves

\[
E : y^2 = x^3 - Dx,
\]
where $D$ is a fourth power free non-zero rational integer. For these curves, $K = \mathbb{Q}(i)$ and the isomorphism from $\mathbb{Z}[i]$ to $\text{End}_K(E)$ is given by mapping $i$ to the endomorphism which sends $(x, y)$ to $(-x, iy)$.

As earlier, let $f$ be the conductor of the Gr"ossencharacter $\psi_E$, and fix some $f$ in $\mathcal{O}_K$ such that $f = f\mathcal{O}_K$. The explicit value of $f$ is well-known, and is given by Lemma 3.2 of \cite{H}. In particular, $f$ is always divisible by $(1 + i)\mathcal{O}_K$, and we define

$$f_1 = f/(1 + i), \quad f_1 = f_1\mathcal{O}_K.$$  

Recall that $G$ denotes the Galois group of $K(E_i)$ over $K$. If $\mathfrak{g}$ is an integral ideal of $K$, we denote the order of the multiplicative group of units of $\mathcal{O}_K/\mathfrak{g}$ by $\phi(\mathfrak{g})$. Also the symbol $\ominus$ will denote subtraction in the group law of $E$.

**Lemma 4.1.** Assume that $D$ is divisible by an odd prime. Let $H_{f_1}$ be the ray class field of $K$ modulo $f_1$. Then $H_{f_1} = K(u)$, where $u$ is the $x$-coordinate of any primitive $f_1$-division point on $E$. Moreover, $[K(E_i) : H_{f_1}] = 2$, and

$$\sigma(Q) = \ominus Q \text{ for all } Q \text{ in } E_{f_1}.$$  

where $\sigma$ denotes the non-trivial element of the Galois group of $K(E_i)$ over $H_{f_1}$.

**Proof.** Since $D$ is odd, $f_1$ is divisible by a prime of $K$ distinct from $(1 + i)\mathcal{O}_K$, and thus if $\zeta$ is a root of unity in $K$ with $\zeta \equiv 1 \mod f_1$, then we must have $\zeta = 1$. It follows that $[H_{f_1} : K] = \phi(f_1)/4$. On the other hand, since $f$ is the conductor of $\psi_E$, $K(E_i)$ coincides with the ray class field of $K$ modulo $f$ (see \cite{H} Lemma 7), and so $[K(E_i) : K] = \phi(f)/4$, whence

$$[K(E_i) : H_{f_1}] = 2.$$  

Let $(u, v)$ be any primitive $f_1$-division point on $E$. By the classical theory of complex multiplication, $H_{f_1} = K(u^2)$. Let $\sigma$ denote the non-trivial element of $\text{Gal}(K(E_i)/H_{f_1})$. Since $H_{f_1} = K(u^2)$, we must have $\sigma u = \pm u$. But $\sigma u = -u$ is impossible, since it would imply that $\sigma v = \pm iv$, which would in turn imply that $\sigma^2$ is not the identity element of $G$. Hence $\sigma u = u$. The following argument shows that we cannot have $\sigma v = v$. Assume indeed that $\sigma v = v$, so that

$$H_{f_1} = K(E_{f_1}).$$  

Take $\alpha$ to be any element of $\mathcal{O}_K$ so that $\alpha \equiv 1 \mod f_1$, and put $a = \alpha\mathcal{O}_K$. Note that $a$ is prime to $f$ because $f$ and $f_1$ have the same prime factors. Since the abelian extension $H_{f_1}/K$ has conductor $f_1$, the Artin symbol $\tau_a$ of $a$ for the extension $H_{f_1}/K$ is equal to 1. But by \cite{H}, we have

$$\tau_a(Q) = \psi_E(a)(Q) \text{ for all } Q \text{ in } E_{f_1}.$$  

Hence we must have $\psi_E(a) \equiv 1 \mod f_1$. But $a = \psi_E(a)\mathcal{O}_K$, and so $\psi_E(a) = \zeta\alpha$ where $\zeta$ is a root of unity in $K$. As $\alpha \equiv 1 \mod f_1$, it follows that $\psi_E((\alpha)) = \alpha$ for all $\alpha$ in $\mathcal{O}_K$ with
\( \alpha \equiv 1 \mod f_1 \). This in turn implies that the conductor \( f \) of \( \psi_E \) must divide \( f_1 \), which is a contradiction. Hence we must have

\[
\sigma(u, v) = (u, -v) = \Theta(u, v),
\]

which proves (61). This completes the proof. \( \Box \)

The Weierstrass differential equation associated to \( E \) is

\[
\wp'(z, \mathcal{L})^2 = 4\wp(z, \mathcal{L})^3 - 4D\wp(z, \mathcal{L}). \tag{65}
\]

In general, we write \( \wp^{(n)}(z, \mathcal{L}) \) for the \( n \)-th derivative of \( \wp(z, \mathcal{L}) \) with respect to \( z \). For all integers \( n \geq 0 \), one has

\[
\wp^{(2n+1)}(z, \mathcal{L}) = B_n(\wp(z, \mathcal{L}))\wp'(z, \mathcal{L}), \tag{66}
\]

where \( B_n(X) \) is a polynomial of degree \( n \) in \( \mathbb{Z}[X] \).

4.2 Corollary 4.2. Assume that \( D \) is divisible by an odd prime. Then, for all integers \( n \geq 0 \),

\[
\text{Tr}_{K(E_i)/K}(\wp^{(2n+1)}(\Omega_\infty/f_1, \mathcal{L})) = 0. \tag{67}
\]

Proof. Writing \( \text{Tr}_{K(E_i)/H_{f_1}} \) for the trace map from \( K(E_i) \) to \( H_{f_1} \), it is clear from (61) and (66) that

\[
\text{Tr}_{K(E_i)/H_{f_1}}(\wp^{(2n+1)}(\Omega_\infty/f_1, \mathcal{L})) = 0. \tag{68}
\]

The assertion (67) follows immediately, completing the proof. \( \Box \)

We next introduce the formal expressions

\[
W(z) = \wp(z, \mathcal{L})^{1/2}, \ V(z) = (\wp(z, \mathcal{L})^2 - D)^{1/2}. \tag{69}
\]

Noting that the differential equation (65) can be written as

\[
\wp'(z, \mathcal{L}) = 2W(z)V(z), \tag{70}
\]

one immediately obtains

\[
W''(z) = V(z), \ V'(z) = 2W(z)^3. \tag{71}
\]

The following lemma is then clear by induction on \( n \).

4.3 Lemma 4.3. For all integers \( n \geq 0 \), we have

\[
V^{(2n+1)}(z) = A_n(W(z)),
\]

where \( A_n(X) \) is a polynomial of degree \( 2n + 3 \) in \( \mathbb{Z}[X] \).
Since
\[ \wp((1 + i)z, \mathcal{L}) = \frac{\wp(z, \mathcal{L})^2 - D}{2i\wp(z, \mathcal{L})}, \]
it follows that
\[ \wp(z, \mathcal{L}) = i\wp((1 + i)z, \mathcal{L}) \pm iV((1 + i)z), \]
(72)

Define
\[ \rho = W\left(\frac{\Omega_\infty}{f_1}\right), \]
(73)
so that \(\rho^2 = \wp(\Omega_\infty/f_1, \mathcal{L})\).

**Lemma 4.4.** Assume that \(D\) is divisible by an odd prime. Then \(K(\rho) = H_{f_1}\), where \(H_{f_1}\) is the ray class field of \(K\) mod \(f_1\). In particular, \([K(\rho) : K] = \phi(f)/8\).

**Proof.** Putting \(z = \Omega_\infty/f_1\) in (72), we conclude that \(\gamma = V(\Omega_\infty/f_1)\) belongs to \(F = K(E_i)\). Taking \(z = \Omega_\infty/f_1\) in (70), it then follows that \(\rho\) must also belong to \(F = K(E_i)\). Moreover, as \(F = K(\wp(\Omega_\infty/f_1, \mathcal{L}))\), we see from (72) that \(\gamma\) does not belong to \(H_{f_1}\), whereas its square plainly does. Hence, writing \(\sigma\) for the non-trivial element of \(\text{Gal}(F/H_{f_1})\), it follows that \(\sigma(\gamma) = -\gamma\). We know from (61) that we also have \(\sigma(v) = -v\), when \(v = \wp'(\Omega_\infty/f_1, \mathcal{L})\). It then follows from (70) with \(z = \Omega_\infty/f_1\) that \(\sigma\) must fix \(\rho\), completing the proof. \(\square\)

We continue to assume that \(D\) is divisible by an odd prime. Then, after differentiating (72), and using (67) and the lemma just proven, we conclude that, for all integers \(n \geq 0,
\]
(74)
\[ \text{Tr}_{K(E_i)/K}(\wp^{(2n+1)}(\Omega_\infty/f, \mathcal{L})) = \pm(1 + i)^{2n+3} \text{Tr}_{H_{f_1}/K}(A_n(\rho)). \]
We use the right hand side of this formula to compute the left hand side in our numerical calculations. The great advantage from a numerical point of view is that the equation (74) allows us to avoid knowing the minimal polynomials of both \(\wp(\Omega_\infty/f, \mathcal{L})\) and \(\wp'(\Omega_\infty/f, \mathcal{L})\) over \(K\), and only requires knowledge of the minimal polynomial of \(\rho\) as well as the coefficients of \(A_n(X)\). Indeed, as we shall explain in the next paragraph, we have been able to calculate the minimal polynomial of \(\rho\) over \(K\) for each of the 6 curves discussed in the Introduction.

Let \(H(X)\) be the minimal polynomial of \(\rho\) over \(K\). By Lemma 4.4 \(H(X)\) has degree \(\phi(f)/8\). We succeeded in computing \(H(X)\) when
\[ \begin{align*}
D &= -14, 17, -33, -34, -39, 82,
\end{align*} \]
and the respective degrees of \(H(X)\) are 192, 128, 960, 1024, 576, 64,000. By far the most difficult case was \(D = 82\), and it was only found with the help of the MAGMA programmes. It would take too much space to give these polynomials explicitly here,
although we would be happy to provide an electronic file containing them for any interested reader. We now list the coefficient of largest absolute value for each of the polynomials $H(X)$, together with the power of $X$ where it occurs:

$$D = -14; \text{ coefficient of } X^{40}:$$

$$-17505698603459355436042213669487147582723059629657863703494656.$$

$$D = 17; \text{ coefficient of } X^{18}:$$

$$-323854307090694728597766056638496367408758560.$$

$$D = -33; \text{ coefficient of } X^{107}:$$

$$11136921680773983777658357767268403310078752482356445633679346954236 \text{ (continued)}.$$
$D = 82$; coefficient of $X^{376}$:

16267703436973377213003989713931931718932500126487797045408201501253939
6731694266094747666615530988064086303049611694143030937780501940450482
6148923158148399191147813882230238624119655402654012877646848571872713
2822553302999268257535786699238655250299150648286294022464086021755163
9738764276240402326739779256978620234034249213967253713905896267785931
1389272946311927380327203467553385171814069136924311033952190656371048
8401256493656625338991614392352334979047794680542663138130567100068261
473008075589476896476370514831830605725691202268893937372813267988367
6652353478038859315100790273860531016767864764458583519619890332349983
1711986989627104655179084273340230013821136292556801493781093121612681
4363981856242791856465666624336990116907158556227793717809986779598196
13158735614026642534292325773460349009009263102014156414450768913713516
822227131939890289476123528846055893652489735995479793826504226262779
280734839459970503640698308912766554349258650720767819339393235364804223
64628161940253821727104232110778223725707981779028065842828864503574
798538329317118897738585994175156823915639693931547246990152507384535
032026410562091608138590163788096431000263595522961820142663587238896
1043298009429916985454588056855950483173445938068590086144429016871410

17
We now discuss briefly the computation of the relevant $L$-values. Let $\Omega_{\infty}^+$ be the smallest positive real period of $E$, so that

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

where $\Omega = 2.622058...$ is the least real non-zero period of $y^2 = x^3 - x$. Thus $\Omega_{\infty}^+ = \alpha(E) \Omega_{\infty}$, where $\alpha(E)$ is 1 or $(1 + i)$ according as $D > 0$ or $D < 0$. As in [1], we write

$$c_n^+(E) = (\Omega_{\infty}^+)^{-n} L(\overline{\psi}_E, n) \ (n \geq 1),$$

where $\overline{\psi}_E$ is the complex conjugate of $\psi_E$. The $L$-values $L(\overline{\psi}_E, n)$ are computed using the functional equation and the $L$-function values at the central point $s = 1/2$. The computation involves the use of the Tate curve and the theory of complex multiplication.
so that \( c_n^+ (E) \) is in \( \mathbb{Q} \).

Now take \( p \) to be any prime with \( p \equiv 1 \mod 4 \) and \((p, D) = 1\). Using the full force of the main conjectures of Iwasawa theory, it is proven in [1, Theorem 2.2] that (i) \( \text{ord}_p (c_p^+ (E)) \geq g_{E/Q} \), (ii) if \( \text{ord}_p (c_p^+ (E)) = g_{E/Q} \), then \( \text{III}(E/Q)(p) = 0 \), and (iii) if \( \text{ord}_p (c_p^+ (E)) \leq g_{E/Q} + 1 \), then \( \text{III}(E/Q)(p) \) is finite. We calculate \( \text{ord}_p (c_p^+ (E)) \) as follows. Putting \( n = p \) in (15), one has

\[
c_p^+ (E) = \frac{1}{\alpha(E)^p(p-1)!} L_p,
\]

and, by a classical formula,

\[
L_p = -f^{-p} \text{Tr}_{K(E_f)/K} \left( \varphi^{(p-2)} \left( \frac{\Omega_{\infty}^{(p-2)}}{f}, \mathcal{L} \right) \right).
\]

Combining this with (74) for \( n = (p - 3)/2 \), we obtain

\[
(77)
\]

\[
c_p^+ (E) = \pm \frac{1}{\beta(E)^p(p-1)!} \text{Tr}_{H_1/K} \left( A_{E_f/2}(\rho) \right),
\]

where

\[
(78)
\]

\[
\beta(E) = f \alpha(E)/(1 + i).
\]

Of course, \( c_p^+ (E) \) is obviously positive, and we choose the sign in (77) accordingly. This formula (77) is the key one for the computations. Indeed, the expression on the right of (77) can readily be calculated when we know explicitly the minimal polynomial of \( \rho \) over \( K \).

For the six values of \( D \) given by (75), we make use of the following respective values of \( f \):

\[
(79)
\]

\[
f = 2^3 \cdot 7, \ 2(1 + i)17, \ 2^2 \cdot 3 \cdot 11, \ 2^3 \cdot 17, \ 2(1 + i) \cdot 3 \cdot 13, \ 2^3 \cdot 41.
\]

Tables I and II give the values of \( c_p^+ (E)^p-g_{E/Q} \mod p \) in the two ranges \( p < 1000 \) and \( 29000 < p < 30000 \), with \( p \) congruent to 1 mod 4, for our six curves. We have placed a * in the Tables in the relevant column whenever \( p \) divides \( D \).

Finally, we must point out that the values of \( c_p^+ (E)^p-g_{E/Q} \mod p \) given in Tables 1 and 2 of [1] should be corrected by multiplying each entry with the factor 4. This is because the formulae (24) and (53) of [1] are incorrect, and only become valid if the factor \( w \) occurring in each formula is omitted (and \( w = 4 \) when \( K = \mathbb{Q}(i) \)). Of course, the correct values are given in Tables 1 and 2 below.
| $p$ | case 82 | case −33 | case −34 | case −39 | case 17 | case −14 |
|-----|--------|----------|----------|----------|---------|---------|
| 5   | 3      | 4        | 4        | 1        | 2       | 1       |
| 13  | 4      | 10       | 9        | *        | 6       | 3       |
| 17  | 14     | 13       | *        | 0        | *       | 11      |
| 29  | 20     | 8        | 2        | 20       | 1       | 0       |
| 37  | 21     | 12       | 26       | 16       | 6       | 36      |
| 41  | *      | 37       | 7        | 37       | 34      | 7       |
| 53  | 1      | 10       | 14       | 8        | 21      | 9       |
| 61  | 11     | 1        | 33       | 18       | 43      | 57      |
| 73  | 42     | 15       | 40       | 44       | 31      | 5       |
| 89  | 77     | 13       | 76       | 74       | 84      | 82      |
| 97  | 92     | 57       | 10       | 92       | 41      | 69      |
| 101 | 31     | 61       | 43       | 92       | 34      | 10      |
| 109 | 37     | 43       | 31       | 3        | 27      | 54      |
| 113 | 64     | 29       | 30       | 98       | 31      | 75      |
| 137 | 6      | 136      | 8        | 7        | 17      | 93      |
| 149 | 146    | 21       | 89       | 119      | 91      | 146     |
| 157 | 101    | 100      | 147      | 31       | 109     | 35      |
| 173 | 158    | 156      | 61       | 3        | 3       | 77      |
| 181 | 20     | 78       | 45       | 177      | 99      | 85      |
| 193 | 48     | 72       | 122      | 125      | 74      | 44      |
| 197 | 110    | 109      | 76       | 14       | 186     | 19      |
| 229 | 206    | 19       | 51       | 132      | 25      | 207     |
| 233 | 178    | 140      | 18       | 212      | 136     | 230     |
| 241 | 114    | 54       | 89       | 108      | 82      | 28      |
| 257 | 32     | 203      | 41       | 136      | 25      | 36      |
| 269 | 127    | 261      | 243      | 169      | 214     | 18      |
| 277 | 50     | 130      | 272      | 267      | 109     | 0       |
| 281 | 145    | 171      | 50       | 64       | 235     | 147     |
| 293 | 187    | 232      | 49       | 215      | 121     | 239     |
| 313 | 65     | 72       | 179      | 123      | 276     | 41      |
| 317 | 212    | 108      | 14       | 137      | 314     | 130     |
| 337 | 241    | 104      | 80       | 35       | 76      | 267     |
| 349 | 114    | 336      | 344      | 85       | 103     | 5       |
| 353 | 61     | 104      | 78       | 288      | 219     | 60      |
| 373 | 97     | 195      | 315      | 216      | 300     | 198     |
| 389 | 381    | 13       | 32       | 273      | 250     | 33      |
| 397 | 15     | 205      | 279      | 59       | 312     | 272     |
| $p$ | case 82 | case $-33$ | case $-34$ | case $-39$ | case 17 | case $-14$ |
|-----|--------|----------|----------|----------|--------|--------|
| 401 | 394    | 197      | 308      | 22       | 193    | 157    |
| 409 | 255    | 138      | 95       | 70       | 44     | 25     |
| 421 | 92     | 97       | 369      | 199      | 187    | 134    |
| 433 | 306    | 155      | 417      | 37       | 429    | 175    |
| 449 | 11     | 32       | 345      | 337      | 345    | 111    |
| 457 | 178    | 369      | 159      | 60       | 238    | 133    |
| 461 | 205    | 304      | 250      | 12       | 71     | 148    |
| 509 | 335    | 500      | 411      | 208      | 412    | 101    |
| 521 | 105    | 469      | 172      | 382      | 424    | 129    |
| 541 | 12     | 18       | 162      | 59       | 132    | 65     |
| 557 | 229    | 107      | 38       | 216      | 547    | 336    |
| 569 | 473    | 274      | 566      | 237      | 554    | 267    |
| 577 | 71     | 506      | 0        | 574      | 156    | 271    |
| 593 | 505    | 155      | 524      | 454      | 313    | 72     |
| 601 | 597    | 350      | 515      | 491      | 290    | 229    |
| 613 | 292    | 311      | 363      | 75       | 490    | 521    |
| 617 | 408    | 187      | 188      | 206      | 532    | 293    |
| 641 | 388    | 548      | 186      | 269      | 499    | 33     |
| 653 | 67     | 343      | 170      | 332      | 384    | 201    |
| 661 | 642    | 125      | 382      | 176      | 80     | 659    |
| 673 | 620    | 407      | 102      | 73       | 501    | 115    |
| 677 | 492    | 583      | 22       | 68       | 651    | 63     |
| 701 | 682    | 180      | 211      | 527      | 420    | 380    |
| 709 | 333    | 79       | 707      | 595      | 330    | 432    |
| 733 | 398    | 544      | 276      | 16       | 307    | 382    |
| 757 | 577    | 537      | 519      | 150      | 671    | 417    |
| 761 | 172    | 445      | 554      | 428      | 691    | 101    |
| 769 | 208    | 448      | 45       | 652      | 697    | 603    |
| 773 | 264    | 270      | 685      | 439      | 52     | 703    |
| 797 | 550    | 603      | 33       | 92       | 492    | 372    |
| 809 | 267    | 606      | 196      | 12       | 154    | 39     |
| 821 | 638    | 728      | 789      | 45       | 24     | 567    |
| 829 | 799    | 825      | 430      | 418      | 93     | 805    |
| 853 | 85     | 476      | 473      | 579      | 192    | 834    |
| 857 | 13     | 802      | 25       | 5        | 20     | 294    |
| 877 | 505    | 353      | 734      | 828      | 528    | 658    |
| 881 | 373    | 427      | 355      | 267      | 328    | 602    |
| 929 | 775    | 430      | 923      | 9        | 593    | 277    |
| 937 | 795    | 456      | 829      | 904      | 427    | 400    |
### Table I: Table of $c_p^+(E)/\text{rank}(E) \mod p$ for $p < 1000$ and $p \equiv 1 \mod 4$.

| $p$  | case 82 | case -33 | case -34 | case -39 | case 17 | case -14 |
|------|---------|----------|----------|----------|---------|----------|
| 941  | 5       | 594      | 645      | 558      | 71      | 686      |
| 953  | 35      | 633      | 133      | 819      | 317     | 605      |
| 977  | 587     | 653      | 428      | 915      | 238     | 392      |
| 997  | 839     | 563      | 408      | 882      | 211     | 607      |

### Table II: Table of $c_p^+(E)/\text{rank}(E) \mod p$ for $29000 < p < 30000$ and $p \equiv 1 \mod 4$.

| $p$  | case 82 | case -33 | case -34 | case -39 | case 17 | case -14 |
|------|---------|----------|----------|----------|---------|----------|
| 29009| 25650   | 23127    | 2319     | 23907    | 2335    | 22753    |
| 29017| 2820    | 18581    | 20044    | 17655    | 28801   | 10064    |
| 29021| 11083   | 5690     | 7203     | 16719    | 21473   | 28871    |
| 29033| 28457   | 24461    | 8759     | 24782    | 16202   | 22261    |
| 29077| 14804   | 11706    | 10879    | 27218    | 21375   | 26584    |
| 29101| 8296    | 17887    | 11405    | 3758     | 4867    | 19197    |
| 29129| 25398   | 22104    | 1256     | 15983    | 27700   | 14477    |
| 29137| 11967   | 8087     | 14839    | 2323     | 21504   | 11674    |
| 29153| 21169   | 10422    | 27377    | 3436     | 15374   | 11577    |
| 29173| 9596    | 27126    | 10426    | 14543    | 14146   | 15233    |
| 29201| 27808   | 18751    | 1663     | 26052    | 10329   | 10761    |
| 29209| 17480   | 25574    | 26288    | 23118    | 15890   | 21215    |
| 29221| 10441   | 4222     | 3439     | 15921    | 20174   | 2642     |
| 29269| 4577    | 8091     | 18622    | 2602     | 8749    | 14748    |
| 29297| 302     | 24353    | 11929    | 10928    | 6390    | 24694    |
| 29333| 15913   | 6596     | 6496     | 24112    | 25483   | 17739    |
| 29389| 28936   | 7811     | 3473     | 19903    | 16483   | 4201     |
| 29401| 3675    | 14554    | 27879    | 11800    | 20475   | 13536    |
| 29429| 6780    | 11389    | 26246    | 167      | 24609   | 24452    |
| 29437| 17070   | 14093    | 16470    | 28787    | 6001    | 12774    |
| 29453| 57      | 21091    | 12802    | 17808    | 14024   | 15022    |
| 29473| 11341   | 8907     | 4052     | 12428    | 27500   | 341      |
| 29501| 20384   | 24356    | 12630    | 13100    | 25119   | 13208    |
| 29537| 12361   | 4242     | 3350     | 3811     | 3605    | 15245    |
| 29569| 2147    | 16852    | 14648    | 3185     | 21444   | 18834    |
| 29573| 14394   | 22250    | 1696     | 13205    | 25891   | 6662     |
| 29581| 8560    | 16558    | 21191    | 534      | 29153   | 10018    |
| 29629| 28337   | 18609    | 8370     | 14834    | 26381   | 5673     |
| 29633| 14670   | 5698     | 22556    | 11543    | 19394   | 27146    |
| 29641| 5608    | 20521    | 12418    | 24522    | 7262    | 12119    |
| 29669| 20520   | 7822     | 26359    | 26038    | 3437    | 14200    |
Finally, we consider the special primes. The primes $p = 19$ and $p = 277$ for the curve
with $D = -14$ are already discussed in [1]. For $D = -39$ and $p = 17$, we have that
\[ c_p^+(E) = 3^{11}5^{2}7^{2}13^{4}17^{3}11 \cdot 163 \cdot 42853254446776087. \]
For $D = -34$, and $p = 577$, $c_p^+(E)$ lies in the interval $[10^{2289}, 10^{2290}]$, and is a very large
number, which we have not succeeded in factoring. However, our calculations show that
\[ c_p^+(E) \equiv 69 \cdot 577^3 \mod 577^4. \]
Thus, by Theorem 2.2 of [1], $\text{III}(E/Q)(p)$ is finite in both cases.

References

[1] J. Coates, Z. Liang, R. Sujatha, The Tate-Shafarevich group for elliptic curves
with complex multiplication, Jour. Alg. 322 (2009), 657–674.

[2] N. Katz, Divisibilities, congruences, and Cartier duality, Jour. Fac. Sci. Univ.
Tokyo 28 (1982), 667–678.

[3] J. Coates, A. Wiles, On $p$-adic $L$-functions and elliptic units, J. Austral. Math.
Soc. 26 (1978), 1-25.

[4] J. Coates, R. Sujatha, Elliptic curves with complex multiplication and $L$-values,
book in preparation.

[5] C. Goldstein, N. Schappacher, Series d’Eisenstein e fonctions $L$ des courbes
elliptiques a multiplication complexe, Crelle J. 327 (1981), 184-218.

[6] J. Coates, Elliptic curves with complex multiplication and Iwasawa theory, Bull.
London Math. Soc. 23 (1991) 321-350.
J. Coates  
Emmanuel College  
Cambridge CB2 3AP, England.  
Department of Mathematics,  
POSTECH, Pohang 790-784, Korea.  
e-mail j.h.coates@dpmms.cam.ac

Z. Liang  
School of Mathematical Sciences,  
Capital Normal University,  
Xisanhuanbeilu 105, Haidan District,  
Beijing, China.  
e-mail liangzhb@gmail.com

R. Sujatha  
School of Mathematics, TIFR,  
Homi Bhabha Road, Colaba,  
Mumbai 40005, India.  
e-mail sujatha@math.tifr.res.in