Journal of Algebra 322 (2009) 657–674

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

The Tate–Shafarevich group for elliptic curves with complex multiplication

J. Coates [a], Z. Liang [b], R. Sujatha [c,*]

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

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

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.

1. Introduction

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

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

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 [10] shows that $Ш(E/\mathbb{Q})$ is finite if $L(E/\mathbb{Q}, s)$ has a zero at $s = 1$ of order $\leqslant 1$, 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 $\geqslant 2$, all is shrouded in mystery. It is unknown whether or not $L(E/\mathbb{Q}, s)$ has

* Corresponding author.
E-mail addresses: J.H.Coates@dpmms.cam.ac.uk (J. Coates), liangzhb@gmail.com (Z. Liang), sujatha@math.tifr.res.in (R. Sujatha).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2009.04.039

a zero at $s = 1$ of order $\geqslant g_{E/\mathbb{Q}}$, and no link between $L(E/\mathbb{Q}, s)$ and $Ш(E/\mathbb{Q})$ has ever been proven. In particular, the finiteness of $Ш(E/\mathbb{Q})$ is unknown for a single elliptic curve $E/\mathbb{Q}$ with $g_{E/\mathbb{Q}} \geqslant 2$. 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 $Ш(E/\mathbb{Q})$, which predicts that in the vast majority of numerical examples $Ш(E/\mathbb{Q})$ is zero when $g_{E/\mathbb{Q}} \geqslant 2$. We also stress that in complete contrast to the situation for finding $g_{E/\mathbb{Q}}$, it is impossible to calculate $Ш(E/\mathbb{Q})$ by classical descent methods, except for its p-primary subgroup for small primes p, usually with $p \leqslant 5$.

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 $Ш(E/\mathbb{Q})$ 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 $t_{E/\mathbb{Q},p}$ denote the $\mathbb{Z}_p$-corank of the p-primary subgroup of $Ш(E/\mathbb{Q})$. While we cannot prove the vanishing of $t_{E/\mathbb{Q},p}$ for infinitely many p in any new cases, we can at least establish the following rather general weak upper bound for $t_{E/\mathbb{Q},p}$ for sufficiently large good ordinary primes p.

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

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

for all primes $p \geqslant c(E, \epsilon)$ 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–Shafarevich 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 $g_{E/\mathbb{Q}} + t_{E/\mathbb{Q},p}$ is equal to the parity of the order of zero at $s = 1$ of the complex L-function of $E/\mathbb{Q}$; in particular, the parity of $t_{E/\mathbb{Q},p}$ 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 $t_{E/\mathbb{Q},p}$ over a much larger range of p where E admits good ordinary reduction than is possible by classical methods. We consider the elliptic curves

$$y^2 = x^3 - 17x \tag{2}$$

and

$$y^2 = x^3 + 14x. \tag{3}$$

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

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

$p \equiv 1 \bmod 4$ and p distinct from 17 (more precisely, our computations show that, for this curve and these primes p, the power series $H_{\mathfrak{p}}(T)$ in $\mathcal{I}[\![T]\!]$, whose existence is given by Proposition 2.4, is of the form $T^2.J_{\mathfrak{p}}(T)$, where $J_{\mathfrak{p}}(T)$ is a unit in $\mathcal{I}[\![T]\!]$). For the curve (3), there are additional zeroes for precisely the two primes $p = 29$ and 277 amongst all $p \equiv 1 \bmod 4$ with $p < 13500$.

2. $\mathfrak{p}$-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 $\mathrm{End}_K(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is isomorphic to K, where $\mathrm{End}_K(E)$ 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

$$\mathrm{End}_K(E) \simeq \mathcal{O}_K. \tag{4}$$

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

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{5}$$

whose coefficients a_i belong to $\mathcal{O}_K$. Write ψ_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 π_v of $\mathrm{End}_K(E)$ such that the reduction of π_v modulo v is the Frobenius endomorphism of the reduction of E modulo v, relative to k_v. The Grössencharacter ψ_E is then given by $\psi_E(v) = \pi_v$. We write $\mathfrak{f}$ for the conductor of ψ_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 $n \geqslant 1$, we define

$$L_{\mathfrak{f}}\big(\bar{\psi}_E^n, s\big) = \prod_{(v,\mathfrak{f})=1} \left(1 - \frac{\bar{\psi}_E^n(v)}{(Nv)^s}\right)^{-1}.$$

Further, $L(\bar{\psi}_E^n, s)$ will denote the primitive Hecke L-function of $\bar{\psi}_E^n$.

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

$$\varpi = \frac{dx}{2y + a_1x + a_3},$$

and let

$$\Phi(z, \mathcal{L})\colon \mathbb{C}/\mathcal{L} \simeq E(\mathbb{C})$$

be the isomorphism given by

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

where $\wp(z,\mathcal{L})$ denotes the Weierstrass $\wp$-function attached to $\mathcal{L}$. Since $\mathcal{O}_K$ has class number 1, there exists Ω_∞ in $\mathbb{C}^\times$ such that

$$\mathcal{L} = \Omega_\infty \mathcal{O}_K. \tag{6}$$

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

$$\Omega_\infty^{-n} L\big(\bar{\psi}_E^n, n\big) \in K \tag{7}$$

for all integers $n \geqslant 1$. Moreover,

$$L\big(\bar{\psi}_E^n, n\big) \neq 0 \quad \text{for } n \geqslant 3, \tag{8}$$

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

$$c_p(E) = \Omega_\infty^{-p} L\big(\bar{\psi}_E^p, p\big). \tag{9}$$

If $\mathfrak{h}$ is any integral ideal of K, we define

$$E_{\mathfrak{h}} = \mathrm{Ker}\big(E(\bar{K}) \xrightarrow{h} E(\bar{K})\big), \tag{10}$$

where h is any generator of $\mathfrak{h}$. Define $E_{\mathfrak{p}^\infty} = \bigcup_{n\geqslant 1} E_{\mathfrak{p}^n}$. 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 $\mathfrak{p}^\infty$-Selmer group of E over $\mathcal{M}$ is defined by

$$\mathrm{Sel}_{\mathfrak{p}}(E/\mathcal{M}) = \mathrm{Ker}\big(H^1\big(\mathrm{Gal}(\bar{\mathcal{M}}/\mathcal{M}), E_{\mathfrak{p}^\infty}\big)\big) \to \prod_w H^1\big(\mathrm{Gal}(\bar{\mathcal{M}}_w/\mathcal{M}_w), E(\bar{\mathcal{M}}_w)\big),$$

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

$$0 \to E(\mathcal{M}) \otimes_{\mathcal{O}_K} (K_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}) \to \mathrm{Sel}_{\mathfrak{p}}(E/\mathcal{M}) \to \text{Ш}(E/\mathcal{M})(\mathfrak{p}) \to 0, \tag{11}$$

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

$$X_{\mathfrak{p}}(E/\mathcal{M}) = \mathrm{Hom}\big(\mathrm{Sel}_{\mathfrak{p}}(E/\mathcal{M}), \mathbb{Q}_p/\mathbb{Z}_p\big). \tag{12}$$

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

$$s_{\mathfrak{p}} = \mathbb{Z}_p\text{-rank of } X_{\mathfrak{p}}(E/K), \qquad t_{\mathfrak{p}} = \mathbb{Z}_p\text{-corank of } \text{Ш}(E/K)(\mathfrak{p}). \tag{13}$$

It is clear from (11) that we have

$$s_{\mathfrak{p}} = t_{\mathfrak{p}} + n_{E/K}, \tag{14}$$

where $n_{E/K} = \mathcal{O}_K$-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) $(p, \mathfrak{f}) = 1$, (ii) $(p, w) = 1$, *and* (iii) p *splits in* K, *say* $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$. *Let* $m_{\mathfrak{p}}$ (*resp.* $m_{\mathfrak{p}^*}$) *denote* $\mathrm{ord}_{\mathfrak{p}}(c_p(E))$ (*resp.* $\mathrm{ord}_{\mathfrak{p}^*}(c_p(E))$). *Then we always have*

$$m_{\mathfrak{p}} \geqslant s_{\mathfrak{p}}, \qquad m_{\mathfrak{p}^*} \geqslant s_{\mathfrak{p}^*}. \tag{15}$$

Moreover, if either $m_{\mathfrak{p}} = n_{E/K}$ *or* $m_{\mathfrak{p}^*} = n_{E/K}$, *then* $\text{Ш}(E/K)(p)$ *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

$$L(E/\mathbb{Q}, s) = L(\psi_E, s), \tag{16}$$

where the L-function on the right is the complex L-function attached to the Grössencharacter ψ_E. Put

$$g_{E/\mathbb{Q}} = \mathbb{Z}\text{-rank of } E(\mathbb{Q}), \qquad r_{E/\mathbb{Q}} = \text{order of zero at } s = 1 \text{ of } L(E/\mathbb{Q}, s). \tag{17}$$

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

$$\Omega_\infty^+ = \Omega_\infty \alpha(E), \tag{18}$$

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

$$c_p^+(E) = \bigl(\Omega_\infty^+\bigr)^{-p} L\bigl(\bar{\psi}_E^p, p\bigr). \tag{19}$$

Let $\tilde{E}_p$ 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* $r_{E/\mathbb{Q}} \equiv g_{E/\mathbb{Q}} \bmod 2$. *If we have*

$$\mathrm{ord}_p\bigl(c_p^+(E)\bigr) < g_{E/\mathbb{Q}} + 2, \tag{20}$$

then $\text{Ш}(E/K)(p)$ *is finite. Moreover, if*

$$\mathrm{ord}_p\bigl(c_p^+(E)\bigr) = g_{E/\mathbb{Q}}, \tag{21}$$

and $\tilde{E}_p(\mathbb{F}_p)$ *has order prime to* p *with* $(p, 6) = 1$, *then* $\text{Ш}(E/K)(p) = 0$.

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

$$\mathrm{ord}_p\bigl(c_p^+(E)\bigr) > g_{E/\mathbb{Q}}. \tag{22}$$

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 $\mathrm{ord}_p(c_p^+(E)) = 3$, and so $\text{Ш}(E/K)(p)$ 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 $\text{Ш}(E/K)(p) = 0$ 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 $n \geqslant 1$, let $\mathcal{E}_n^*(z, \mathcal{L})$ denote the Eisenstein series of $\mathcal{L}$, as defined by Eisenstein (see Weil [19] or [9]). In particular, for $n \geqslant 3$, we have

$$\mathcal{E}_n^*(z, \mathcal{L}) = \frac{(-1)^n}{(n-1)!}\left(\frac{d}{dz}\right)^{n-2}\big(\wp(z, \mathcal{L})\big). \tag{23}$$

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 $\mathfrak{f}$ of ψ_E. Then, for all integers $n \geqslant 1$, we have $\mathcal{E}_n^*(\frac{\Omega_\infty}{f}, \mathcal{L}) \in K(E_\mathfrak{f})$, and*

$$w\Omega_\infty^{-n} L_\mathfrak{f}\big(\bar{\psi}_E^n, n\big) = f^{-n}\,\mathrm{Trace}_{K(E_f)/K}\left(\mathcal{E}_n^*\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right)\right). \tag{24}$$

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

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

$$i_\mathfrak{p} : \bar{K} \hookrightarrow \bar{\mathbb{Q}}_p, \tag{25}$$

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

Let $\hat{E}^\mathfrak{p}$ be the formal group of E at $\mathfrak{p}$, so that we can take $t = -x/y$ to be a parameter of $\hat{E}^\mathfrak{p}$. Let $\hat{\mathbb{G}}_m$ 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 $\hat{E}^\mathfrak{p}$ is a formal group of height 1 (in fact, it is even a Lubin–Tate group over $\mathbb{Z}_p$ attached to the parameter $\psi_E(\mathfrak{p})$), it is well known that there is an isomorphism over $\mathcal{I}$

$$\delta_\mathfrak{p} \colon \hat{\mathbb{G}}_m \simeq \hat{E}^\mathfrak{p}, \tag{26}$$

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

$$\Omega_\mathfrak{p} = \left.\frac{\delta_\mathfrak{p}(u)}{u}\right|_{u=0}. \tag{27}$$

Proposition 2.4. *Assume Ω_∞ and $\Omega_\mathfrak{p}$ are fixed. Then there exists a unique power series $H_\mathfrak{p}(T)$ in $\mathcal{I}[\![T]\!]$ such that, for all integers $n \geqslant 1$ with $n \equiv 1 \bmod (p-1)$, we have*

$$\Omega_\mathfrak{p}^{-n} H_\mathfrak{p}\big((1+p)^n - 1\big) = \Omega_\infty^{-n}(n-1)! L\big(\bar{\psi}_E^n, n\big)\left(1 - \frac{\psi_E^n(\mathfrak{p})}{N\mathfrak{p}}\right). \tag{28}$$

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

This $\mathfrak{p}$-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 $\mathfrak{p}$. Define

$$F_\infty = K(E_{\mathfrak{p}^\infty}), \qquad G = \mathrm{Gal}(F_\infty/K).$$

The action of G on $E_{\mathfrak{p}^\infty}$ defines a homomorphism

$$\chi_{\mathfrak{p}} : G \to \mathrm{Aut}(E_{\mathfrak{p}^\infty}) = \mathbb{Z}_p^\times \tag{29}$$

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

$$\Gamma = \mathrm{Gal}(K_\infty/K), \qquad \Lambda(\Gamma) = \varprojlim \mathbb{Z}_p[\Gamma/U],$$

where U runs over the open subgroups of Γ. There is a natural continuous action of Γ on $X_{\mathfrak{p}}(E/K_\infty)$, and this extends to an action of the Iwasawa algebra $\Lambda(\Gamma)$. Since it is known that $X_{\mathfrak{p}}(E/K_\infty)$ 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

$$0 \to \bigoplus_{i=1}^{r} \Lambda(\Gamma)/f_i\Lambda(\Gamma) \to X_{\mathfrak{p}}(E/K_\infty) \to D \to 0,$$

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 $\gamma_{\mathfrak{p}}$ of Γ such that $\chi_{\mathfrak{p}}(\gamma_{\mathfrak{p}}) = 1 + p$, and write

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

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

$$B_{\mathfrak{p}}(T) = j\left(\prod_{i=1}^{r} f_i\right). \tag{30}$$

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

Theorem 2.5 *(One variable main conjecture).*

$$H_{\mathfrak{p}}\big((1+p)(1+T)-1\big)\mathcal{I}[\![T]\!] = B_{\mathfrak{p}}(T)\mathcal{I}[\![T]\!].$$

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

Proposition 2.6. *The two groups* $Ш(E/K)(\mathfrak{p})$ *and* $Ш(E/K)(\mathfrak{p}^*)$ *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 $\chi_{\mathfrak{p}}$ is an isomorphism, we have $E_{\mathfrak{p}^\infty}(K_\infty) = 0$. It follows that the restriction map from $\mathcal{S}_{\mathfrak{p}}(E/K)$ to $\mathcal{S}_{\mathfrak{p}}(E/K_\infty)$ is injective, and by duality, we obtain a surjective Γ-homomorphism

$$X_{\mathfrak{p}}(E/K_\infty) \to X_{\mathfrak{p}}(E/K). \tag{31}$$

Recall that $s_{\mathfrak{p}}$ denotes the $\mathbb{Z}_p$-rank of $X_{\mathfrak{p}}(E/K)$. As Γ acts trivially on $X_{\mathfrak{p}}(E/K)$, it follows from (31) by a well-known property of characteristic ideals of torsion $\Lambda(\Gamma)$-modules, that $T^{s_{\mathfrak{p}}}$ must divide $B_{\mathfrak{p}}(T)$ in $\mathbb{Z}_p[\![T]\!]$. Hence we conclude from Theorem 2.5 that

$$H_{\mathfrak{p}}\big((1+p)(1+T)-1\big) = T^{s_{\mathfrak{p}}} h(T) \tag{32}$$

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

$$H_{\mathfrak{p}}\big((1+p)^n - 1\big) \equiv 0 \bmod p^{s_{\mathfrak{p}}}. \tag{33}$$

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

$$c_p(E) \equiv 0 \bmod \mathfrak{p}^{s_p}. \tag{34}$$

Replacing $\mathfrak{p}$ by $\mathfrak{p}^*$, the same argument shows that

$$c_p(E) \equiv 0 \bmod (\mathfrak{p}^*)^{s_{\mathfrak{p}^*}}. \tag{35}$$

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

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

Proof. If $m_{\mathfrak{p}} = n_{E/K}$, the above argument shows that we must have $s_{\mathfrak{p}} = n_{E/K}$, and $h(0)$ a p-adic unit. It follows from Theorem 2.5 that $B_{\mathfrak{p}}(T)$ must be of the form $T^{n_{E/K}}$ times a unit in $\mathbb{Z}_p[\![T]\!]$. Conversely, if the characteristic power series of $X_{\mathfrak{p}}(E/K_\infty)$ can be taken to be $T^{n_{E/K}}$, then Theorem 2.5 shows that $H_{\mathfrak{p}}(T)$ is equal to $T^{n_{E/K}}$ times a unit in $\mathcal{I}[\![T]\!]$, whence it is plain that $m_{\mathfrak{p}} = n_{E/K}$. This completes the proof. □

Our numerical calculations show that, for the elliptic curve

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

we have $m_{\mathfrak{p}} = 2$ for all primes p with $p \equiv 1 \bmod 4$, $p \neq 17$, and $p < 13500$. Thus the characteristic power series of $X_{\mathfrak{p}}(E/K_\infty)$ 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 $m_{\mathfrak{p}} = 2$ for all primes p with $p \equiv 1 \bmod 4$ and $p < 13500$, except $p = 29, 277$. Thus for all such primes, with the exception of these two, the characteristic power series of $X_{\mathfrak{p}}(E/K_\infty)$ is T^2.

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

$$\bar{\mathfrak{f}} = \mathfrak{f}, \quad \text{and} \quad \psi_E(\bar{\mathfrak{a}}) = \overline{\psi_E(\mathfrak{a})} \tag{36}$$

for all integral ideals $\mathfrak{a}$ of K with $(\mathfrak{a}, \mathfrak{f}) = 1$. Hence

$$L\big(\psi_E^p, s\big) = L\big(\bar{\psi}_E^p, s\big).$$

Evaluating at $s = p$, we conclude that

$$L\big(\bar{\psi}_E^p, p\big) \in \mathbb{R}.$$

As Ω_∞^+ is real, it follows that

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

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

$$t_{E/\mathbb{Q},p} = t_{\mathfrak{p}} = t_{\mathfrak{p}^*}. \tag{37}$$

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, $Ш(E/\mathbb{Q})(p)$ and $Ш(E'/\mathbb{Q})(p)$ have the same $\mathbb{Z}_p$-corank, and hence the $\mathbb{Z}_p$-corank of $Ш(E/K)(p)$ is equal to $2t_{E/\mathbb{Q},p}$. On the other hand, the $\mathbb{Z}_p$-corank of $Ш(E/K)(p)$ is clearly equal to $t_{\mathfrak{p}} + t_{\mathfrak{p}^*} = 2t_{E/\mathbb{Q},p}$, by Proposition 2.6. Hence $t_{E/\mathbb{Q},p} = t_{\mathfrak{p}}$, thereby proving (37).

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

$$g_{E/\mathbb{Q}} + t_{E/\mathbb{Q},p} \equiv r_{E/\mathbb{Q}} \bmod 2.$$

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

$$\operatorname{ord}_p\big(c_p^+(E)\big) \geqslant g_{E/\mathbb{Q}} + 2.$$

Hence, if (20) holds, then we must have $Ш(E/K)(p)$ is finite.

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

$$B_{\mathfrak{p}}(T) = T^{n_{E/K}} R_{\mathfrak{p}}(T),$$

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

$$\langle , \rangle_{\mathfrak{p}} : E(K) \otimes_{\mathcal{O}} \mathbb{Z}_p \times E(K) \otimes_{\mathcal{O}} \mathbb{Z}_p \to \mathbb{Q}_p,$$

where $\mathcal{O}$ is embedded in $\mathbb{Z}_p$ via $i_{\mathfrak{p}}$, is non-degenerate. Further, we have that

$$\#\big(Ш(E/K)(\mathfrak{p})\big) \times \det\langle , \rangle_{\mathfrak{p}} \times \left(1 - \frac{\psi_{E/K}(\mathfrak{p})}{N\mathfrak{p}}\right) \tag{38}$$

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 $\tilde{E}_p(\mathbb{F}_p)$ has order prime to p and $(p, 6) = 1$, then it follows from the results of [12] that $\det\langle , \rangle_{\mathfrak{p}}$ is a p-adic integer. Hence we conclude from (38) that $Ш(E/K)(\mathfrak{p})$ is trivial. A similar argument proves the corresponding statement for $Ш(E/K)(\mathfrak{p}^*)$ and this completes the proof of Theorem 2.2.

We next establish an upper bound for $t_{\mathfrak{p}}$ and $t_{\mathfrak{p}^*}$ when p is a sufficiently large prime which splits in K as $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$.

Theorem 2.8. *For each $\epsilon > 0$, there exists an explicitly computable number $c(E,\epsilon)$, depending only on E and ϵ, such that*

$$t_{\mathfrak{p}} \leqslant (1+\epsilon)p - n_{E/K}, \qquad t_{\mathfrak{p}^*} \leqslant (1+\epsilon)p - n_{E/K}, \tag{39}$$

for all primes $p \geqslant c(E,\epsilon)$ which split in K as $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$.

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 $t_{E/\mathbb{Q},p} = t_{\mathfrak{p}}$, $n_{E/K} = g_{E/\mathbb{Q}}$.

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

$$\Theta_p = \mathrm{Trace}_{K(E_{\mathfrak{f}})/K}\left(\mathcal{E}_p^*\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right)\right). \tag{40}$$

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 $|\Theta_p| \leqslant d_1^p$, where $d_1 > 1$ is a real number depending only on E and not on p.*

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

$$\mathcal{E}_p^*\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right) = \frac{(-1)^p}{(p-1)!}\left(\frac{d}{dz}\right)^{p-2}\big(\wp(z,\mathcal{L})\big)\Big|_{z=\frac{\Omega_\infty}{f}}. \tag{41}$$

Let $\mathcal{B}$ denote a set of integral ideals of K, prime to $\mathfrak{f}$, such that the Galois group of $K(E_{\mathfrak{f}})/K$ consists precisely of the Artin symbols $\sigma_{\mathfrak{b}}$ of the ideals $\mathfrak{b}$ in $\mathcal{B}$. From the definition of the Grössencharacter ψ_E and (41), we have

$$\mathcal{E}_p^*\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right)^{\sigma_{\mathfrak{b}}} = \mathcal{E}_p^*\left(\psi_E(\mathfrak{b})\frac{\Omega_\infty}{f}, \mathcal{L}\right).$$

Thus, by Cauchy's integral formula, we obtain

$$\mathcal{E}_p^*\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right)^{\sigma_{\mathfrak{b}}} = \frac{(-1)^p}{(p-1)2\pi i}\int\limits_{\mathcal{C}_{\mathfrak{b}}} \frac{\wp(z,\mathcal{L})\,dz}{(z - \frac{\psi_E(\mathfrak{b})\Omega_\infty}{f})^{p-1}},$$

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

$$\left|\mathcal{E}_p^*\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right)^{\sigma_{\mathfrak{b}}}\right| \leqslant d_2^p,$$

where $d_2 > 1$ depends only on E. Summing over all $\mathfrak{b}$ in $\mathcal{B}$, 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*

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

is an algebraic integer.

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

$$\mathcal{E}_p^*(\lambda z, \lambda \mathcal{L}) = \lambda^{-p} \mathcal{E}_p^*(z, \mathcal{L})$$

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

$$\big(\wp'(z, \mathcal{L})\big)^2 = 4\wp(z, \mathcal{L})^3 - g_2(\mathcal{L})\wp(z, \mathcal{L}) - g_3(\mathcal{L})$$

implies that

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

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

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

where $D_n(X)$ is a polynomial in $\mathcal{O}_K[X]$ of degree $n+1$. It follows immediately that

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

where $B_n(X) = \frac{d}{dX}(D_n(X))$ is a polynomial of degree n in $\mathcal{O}_K[X]$. 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

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

are algebraic integers. □

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

$$\big|\Omega_\infty^{-p} L\big(\bar{\psi}_E^p, p\big)\big|_{\mathfrak{p}} = |\Theta_p|_{\mathfrak{p}} = \big|(p-1)!\Theta_p\big|_{\mathfrak{p}}, \tag{42}$$

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

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

is an element of $\mathcal{O}_K$ 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 $L(\bar{\psi}_E^p, p) \neq 0$, we conclude from the product formula that

$$\left|d_3^p(p-1)!\Theta_p\right|_{\mathfrak{p}} \times \left|d_3^p(p-1)!\Theta_p\right|_{\mathfrak{p}^*} \geqslant d_4^{-2p}\big((p-1)!\big)^{-2}. \tag{43}$$

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

$$|\Theta_p|_{\mathfrak{p}} \times |\Theta_p|_{\mathfrak{p}^*} \geqslant p^{-2(1+\epsilon)p}$$

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

$$|\Theta_p|_{\mathfrak{p}} \times |\Theta_p|_{\mathfrak{p}^*} \leqslant p^{-(s_{\mathfrak{p}}+s_{\mathfrak{p}^*})}.$$

Thus

$$s_{\mathfrak{p}} + s_{\mathfrak{p}^*} \leqslant 2(1+\epsilon)p$$

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

Define the p-adic L-functions

$$\mathfrak{L}_{E,\mathfrak{p}}(s) = H_{\mathfrak{p}}\big((1+p)^s - 1\big), \qquad \mathfrak{L}_{E,\mathfrak{p}^*}(s) = H_{\mathfrak{p}^*}\big((1+p)^s - 1\big),$$

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

$$r_{E,\mathfrak{p}} = \operatorname{ord}_{s=1}\mathfrak{L}_{E,\mathfrak{p}}(s), \qquad r_{E,\mathfrak{p}^*} = \operatorname{ord}_{s=1}\mathfrak{L}_{E,\mathfrak{p}^*}(s).$$

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*

$$r_{E,\mathfrak{p}} + r_{E,\mathfrak{p}^*} \leqslant 2(1+\epsilon)p$$

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

3. Computations for $y^2 = x^3 - Dx$

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

$$c_p(E) = \Omega_\infty^{-p} L\big(\bar{\psi}_E^p, p\big)$$

in practice, for the family of curves

$$E\colon\ y^2 = x^3 - Dx,$$

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 $K(E_{\mathfrak{f}})$ where $\mathfrak{f}$ again denotes the conductor of ψ_E. If $\mathfrak{h}$ is any integral ideal of K, we write

$$\phi(\mathfrak{h}) = \#\big(\big(\mathbb{Z}[i]/\mathfrak{h}\big)^\times\big).$$

The next lemma is a very easy consequence of the existence of the Grössencharacter ψ_E (see [5, Lemma 3], or [3, Lemma 7]) and the fact that no non-trivial root of unity in K is $\equiv 1 \bmod \mathfrak{h}$, when $\mathfrak{h}$ is a multiple of $\mathfrak{f}$.

Lemma 3.1. *Let $\mathfrak{h}$ be any integral ideal of K which is divisible by the conductor $\mathfrak{f}$ of ψ_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 $\mathfrak{f}$ for the curve E.

Lemma 3.2. *Let Δ be the product of the distinct prime factors of D. Then $\mathfrak{f} = 4\Delta\mathbb{Z}[i]$ if $D \not\equiv 1 \bmod 4$ and $\mathfrak{f} = (1+i)^3\Delta\mathbb{Z}[i]$ if $D \equiv 1 \bmod 4$.*

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

$$E'\colon\ y^2 = x^3 - x. \tag{44}$$

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 $k \geqslant 3$, we have*

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

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

$$E \simeq E' \tag{45}$$

given by mapping the point (x, y) on E to the point $(x/\alpha^2, y/\alpha^3)$ on E'. Now E' has conductor $(1+i)^3$, and $K(E'_{(1+i)^3}) = K$, whence it follows from (45) that $K(E_{(1+i)^3}) = K(\alpha)$. Similarly, if $k \geqslant 3$, 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 $k \geqslant 3$. 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. □

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 $D \neq 1$. 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 τ of $\mathrm{Gal}(K(E_D)/K)$ such that τ fixes R_D, and τ 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 σ in $\mathrm{Gal}(K(E'_D)/K)$ such that

$$\sigma(u', v') = (-u', iv'). \tag{46}$$

Now let σ denote any extension of σ 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 σ 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 σ^4 fixes $K(E_D)$, but σ^2 does not. Also σ fixes R_D. Hence we may take τ to be restriction of σ to $\mathrm{Gal}(K(E_D)/K)$, and the proof of the lemma is complete. □

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 $8M$, and hence we have

$$\big[K\big(E'_{8M}\big) : K\big] = 8\phi\big(M\mathbb{Z}[i]\big).$$

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

$$K\big(E'_M\big) \cap K\big(E'_8\big) = K. \tag{47}$$

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

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

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

$$K\big(E'_M, \alpha\big) = K(E_M, \alpha).$$

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

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

and the proof of the lemma is complete. □

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

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

Write $\mathfrak{f} = f\mathbb{Z}[i]$ for the conductor of ψ_E, and define

$$u = \wp\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right), \qquad v = \left(\wp'\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right)\right)/2. \tag{49}$$

By Lemma 3.1, $K(E_\mathfrak{f})$ is the ray class field of K modulo $\mathfrak{f}$. Hence

$$K(E_\mathfrak{f}) = K\big(u^2\big) = K(u), \quad v \in K(u), \tag{50}$$

and the degree of $K(E_\mathfrak{f})$ over K is $d = \phi(\mathfrak{f})/4$. As $\mathfrak{f}$ 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

$$s_m = \mathrm{Trace}_{K(E_\mathfrak{f})/K}\big(u^m\big) \quad (m = 1, 2, \ldots, d-1) \tag{51}$$

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]),

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

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

$$c_p^+(E) = -w^{-1}\big(f\alpha(E)\big)^{-p}\big((p-1)!\big)^{-1}\Xi_p, \tag{53}$$

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

$$\Xi_p = \mathrm{Trace}_{\mathrm{K}(\mathrm{E}_\mathfrak{f})/\mathrm{K}}\left(\wp^{(p-2)}\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right)\right)$$

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

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

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 $D \equiv 1 \bmod 4$, (ii) $D < 0$ and $D \equiv 1 \bmod 4$, (iii) $D > 0$ and $D \not\equiv 1 \bmod 4$, and (iv) $D < 0$, and $D \not\equiv 1 \bmod 4$. Following these four cases, we take f to be $2(1+i)\Delta$, $(1+i)^3\Delta$, 4Δ, and 4Δ, so that the respective values of $f\alpha(E)$ are given by $2(1+i)\Delta$, -4Δ, 4Δ, and $4\Delta(1+i)$.

As explained in the proof of Lemma 2.10, we have

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

where $B_{\frac{p-3}{2}}(X)$ 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

$$\wp'\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right) = J\left(\wp\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right)\right). \tag{55}$$

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 $B_{\frac{p-3}{2}}(X)$ and $J(X)$, and using the fact that $G(\wp(\frac{\Omega_\infty}{f}, \mathcal{L})) = 0$, we deduce that

$$\wp^{(p-2)}\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right) = A_p\left(\wp\left(\frac{\Omega_\infty}{f}, \mathcal{L}\right)\right),$$

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 $\mathrm{ord}_p(c_p^+(E))$ (which our theory shows is always $\geqslant 0$), followed by

$$c_p^+(E) \bmod p^k, \quad \text{where } k = \mathrm{ord}_p\big(c_p^+(E)\big) + 1.$$

Finally, we note that $\tilde{E}_p(\mathbb{F}_p)$ has order prime to p for all $p > 5$ with $(p, D) = 1$. This is clear when $p \equiv 3 \bmod 4$, since then $\tilde{E}_p$ is supersingular. For $p \equiv 1 \bmod 4$, say $p\mathbb{Z}[i] = \mathfrak{p}.\mathfrak{p}*$, we have $a_p = \mathrm{Trace}_{K/\mathbb{Q}}(\psi_E(\mathfrak{p}))$ 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 $p \equiv 1 \bmod 4$ and $p < 13,500$ (the prime $p = 17$ is excluded when $D = 17$). We have

$$D = 17, \qquad f = 2(1+i)17, \qquad d = 256$$
$$D = -14, \qquad f = 56, \qquad d = 384.$$

For both cases, the polynomials $G(X)$, $J(X)$, $B_{\frac{p-3}{2}}(X)$, $A_p(X)$ 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 $p = 29$,

$$D = -14,$$

$$\begin{aligned} B_{13}(X) = 7496723869173 \times 2^{24}\big(&431525237696X + 3877463640960X^3 \\ &+ 5545863414000X^5 + 2565173520000X^7 + 490959787500X^9 \\ &+ 40724775000X^{11} + 1212046875X^{13}\big), \end{aligned}$$

$$D = 17,$$

$$B_{13}(X) = 7496723869173 \times 2^{24}\big(1383348216959X - 10236515835780X^3 + 12057373443375X^5 - 4592819790000X^7 + 723915196875X^9 - 49451512500X^{11} + 1212046875X^{13}\big).$$

For these two curves, and our range of p, our computations show that $\mathrm{ord}_p(c_p^+(E)) = 2$, except for the two primes $p = 29, 277$ for the curve with $D = -14$. Table 1 gives the value of $c_p^+(E) \bmod p^3$ for both curves and our p in the range $5 \leqslant p < 1000$, 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

$$c_{29}^+(E) \equiv 27 \cdot 29^3 \bmod 29^4,$$
$$c_{277}^+(E) \equiv 155 \cdot 277^3 \bmod 277^4.$$

Table 1
$c_p^+(E) \cdot p^{-2} \bmod p$ for $5 \leqslant p < 1000$ and $p \equiv 1 \bmod 4$.

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

Table 2
$c_p^+(E) \cdot p^{-2} \bmod p$ for $11000 < p < 12000$ and $p \equiv 1 \bmod 4$.

p	$D = 17$	$D = -14$	p	$D = 17$	$D = -14$
11057	3236	10336	11069	7768	6637
11093	9234	5437	11113	832	9242
11117	6204	7965	11149	8885	1364
11161	1292	1636	11173	587	10503
11177	6184	4427	11197	8804	6750
11213	6409	8508	11257	192	1839
11261	700	6850	11273	5932	510
11317	1969	2892	11321	5451	10402
11329	5635	9145	11353	3322	7820
11369	6790	11276	11393	4532	358
11437	10570	3120	11489	8715	10941
11497	4837	6424	11549	7265	2757
11593	225	369	11597	8864	7113
11617	10691	1052	11621	7500	6521
11633	293	5463	11657	10665	4770
11677	10365	11566	11681	6023	5351
11689	11553	3152	11701	5851	11618
11717	10185	8521	11777	10882	3487
11789	6221	3509	11801	10632	3148
11813	2123	3767	11821	7340	128
11833	1715	9412	11897	8766	10281
11909	6032	11519	11933	1190	1783
11941	5023	6379	11953	10988	1162
11969	11669	11573	11981	1742	8384

Acknowledgment

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

References

[1] D. Bernardi, C. Goldstein, N. Stephens, Notes p-adiques sur les courbes elliptiques, Crelle J. 351 (1984) 129–170.
[2] J. Cassels, A note on the division values of $p(u)$, Math. Proc. Cambridge Philos. Soc. 45 (1949) 167–172.
[3] J. Coates, Elliptic curves with complex multiplication and Iwasawa theory, Bull. London Math. Soc. 23 (1991) 321–350.
[4] J. Coates, R. Sujatha, Elliptic Curves with Complex Multiplication and L-Values, book in preparation.
[5] J. Coates, A. Wiles, On the conjecture of Birch and Swinnerton–Dyer, Invent. Math. 39 (1977) 223–251.
[6] J. Coates, A. Wiles, On p-adic L-functions and elliptic units, J. Aust. Math. Soc. 26 (1978) 1–25.
[7] T. Dokchitser, V. Dokchitser, On the Birch Swinnerton–Dyer quotients modulo squares, Ann. Math., in press.
[8] B. Gross, Arithmetic on Elliptic Curves with Complex Multiplication, Lecture Notes in Math., vol. 776, Springer, 1980.
[9] C. Goldstein, N. Schappacher, Séries d'Eisenstein et fonctions L de courbes elliptiques à multiplication complexe, Crelle J. 327 (1981) 184–218.
[10] V. Kolyvagin, Euler systems, in: The Grothendieck Festschrift, vol. II, in: Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.
[11] J. Nekovář, Selmer complexes, Astérisque 310 (2007).
[12] B. Perrin-Riou, Arithmétique des courbes elliptiques et théorie d'Iwasawa, Bull. Soc. Math. France 17 (1984).
[13] D. Bernardi, B. Perrin-Riou, Variante p-adique de la conjecture de Birch et Swinnerton–Dyer (le cas supersingulier), C. R. Acad. Sci. Paris Sr. I Math. 317 (1993) 227–232.
[14] B. Perrin-Riou, Arithmétique des courbes elliptiques à réduction super singuliére en p, Experiment. Math. 12 (2003) 155–186.
[15] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, Invent. Math. 103 (1991) 25–68.
[16] W. Stein, C. Wuthrich, Computations about Tate–Shafarevich groups using Iwasawa theory, preprint, 2008.
[17] http://www.cnu.edu.cn/mathpage/upload/liangzibin/thesis/20081104074048.rar.
[18] B. Van der Waerden, Modern Algebra, vols. I and II, Ungar, 1953.
[19] A. Weil, Elliptic Functions According to Eisenstein and Kronecker, Springer, 1976.
[20] J. Tate, On the conjecture of Birch and Swinnerton–Dyer and a geometric analog, Séminaire Bourbaki 306 (1966).