Advanced Studies in Pure Mathematics 17, 1989
Algebraic Number Theory — in honor of K. Iwasawa
pp. 409–419

# Tate-Shafarevich Groups of Elliptic Curves with Complex Multiplication

**Karl Rubin**

***Dedicated to Professor Kenkichi Iwasawa on his 70th birthday***

If $E$ is an elliptic curve defined over an imaginary quadratic field $K$, with complex multiplication by $K$, and if $L(E_{/K}, 1)\neq 0$, then the Tate-Shafarevich group $\text{Ш}(E_{/K})$ is finite. The proof of this statement in [8] is complicated by the necessity of studying the $\mathfrak{p}$-part of $\text{Ш}(E_{/K})$ for *all* primes $\mathfrak{p}$ of $K$. In fact the above theorem grew out of an earlier weaker result which, because it ignores a finite set of "bad" primes of $K$, is proved much more simply.

The purpose of the present paper is to give the original proof of this simpler result, Theorem 1 below. The proof contains the important ideas of the proof of Theorem A of [8], but is much clearer because many of the technical difficulties of [8] do not arise. Later in this section we will use Theorem 1 to obtain three examples of finite Tate-Shafarevich groups. This paper should be viewed as the predecessor of [8], and one would be well-advised to read this paper first.

Suppose $E$ is an elliptic curve defined over an imaginary quadratic field $K\subset \boldsymbol{C}$, with complex multiplication by the ring of integers $\mathcal{O}$ of $K$. Fix an $\mathcal{O}$-generator $\Omega\in \boldsymbol{C}^{\times}$ of the period lattice of a minimal model of $E$, let $\psi$ denote the Hecke character of $K$ attached to $E$, $L(\psi, s)$ the corresponding Hecke $L$-function, and $L(E_{/K}, s)$ the $L$-function of $E$ over $K$. Then $L(E_{/K}, s)=L(\psi, s)L(\bar{\psi}, s)$, $L(\bar{\psi}, 1)/\Omega\in K$, and $L(E_{/K}, 1)=0\Leftrightarrow L(\psi, 1)=0\Leftrightarrow L(\bar{\psi}, 1)=0$.

**Theorem 1.** *Let $E$ be an elliptic curve defined over an imaginary quadratic field $K$, with complex multiplication by $K$. Let $\mathfrak{p}$ be a prime of $K$ where $E$ has good reduction, and which does not divide $\#(\mathcal{O}^{\times})$. If $\#(E(K)_{\text{torsion}})L(\bar{\psi}, 1)/\Omega\not\equiv 0 \pmod{\mathfrak{p}}$, then the $\mathfrak{p}$-part of $\text{Ш}(E_{/K})$ is zero. In particular if $L(\bar{\psi}, 1)\neq 0$ then the $\mathfrak{p}$-part of $\text{Ш}(E_{/K})$ is zero for all but finitely*

---

Received December 1, 1987.
This work was carried out while the author was an Alfred P. Sloan Fellow at MSRI, Berkeley. Additional support was provided by NSF grant DMS-8501937.

*many primes $\mathfrak{p}$ of K.*

**Remarks.** 1. As in [8], the method of proof of Theorem 1 relies heavily on the ideas of Coates and Wiles [3] and of Thaine [11].

2. If $E$ is defined over $\boldsymbol{Q}$, then $L(E_{/Q}, s)=L(\bar{\psi}, s)$. If $p$ is a rational prime greater than 2, and $\mathfrak{p}$ is any prime of $K$ above $p$, then the inflation-restriction sequence of Galois cohomology shows that the $p$-part of Ш$(E_{/Q})$ is nontrivial if and only if the $\mathfrak{p}$-part of Ш$(E_{/K})$ is nontrivial. This allows us to use Theorem 1 to relate Ш$(E_{/Q})$ and $L(E_{/Q}, 1)$.

3. *Examples of Tate-Shafarevich groups.* In certain cases Theorem 1 can be used to compute Ш exactly. For example:

A) *Let E be the curve* $y^2=x^3-x$. *Then* Ш$(E_{/Q})=0$.

*Proof.* This curve has $CM$ by $\boldsymbol{Z}[i]$, bad reduction only at $(1+i)$, $\#[E(\boldsymbol{Q}(i))_{\text{torsion}}]=8$ and $L(\bar{\psi}, 1)/\Omega=1/4$. Thus Theorem 1 shows that the non-2-part of Ш$(E_{/K})$ is trivial. Using remark 2 above it follows that the non-2-part of Ш$(E_{/Q})$ is trivial as well, and Fermat's proof (circa 1650) that $E(\boldsymbol{Q})$ is finite also shows (see [12], Chap. II, § X and Appendix IV) that Ш$(E_{/Q})_2=0$, so Ш$(E_{/Q})=0$. //

B) *Let E be the Fermat cubic* $x^3+y^3=z^3$. *Then* Ш$(E_{/Q})=0$.

*Proof.* This curve has $CM$ by $\boldsymbol{Z}[(1+\sqrt{-3})/2]$, bad reduction only at $(\sqrt{-3})$, $\#[E(\boldsymbol{Q}(\sqrt{-3}))_{\text{torsion}}]=9$, and $L(\bar{\psi}, 1)/\Omega=1/3$. Thus Theorem 1 and remark 2 above show that Ш$(E_{/Q})_p=0$ for $p>3$. That Ш$(E_{/Q})_2=0$ (resp. Ш$(E_{/Q})_3=0$) follows from a computation of Cassels [1] (resp. Euler and probably also Fermat, see [12], Chap. II, § XVI and Appendix IV). //

C) *Let E be the modular curve* $X_0(49)$: $y^2+xy=x^3-x^2-2x-1$. *Then* Ш$(E_{/Q})=0$.

*Proof.* This curve has $CM$ by $\boldsymbol{Z}[(1+\sqrt{-7})/2]$, bad reduction only at $(\sqrt{-7})$, $\#[E(\boldsymbol{Q}(\sqrt{-7}))_{\text{torsion}}]=4$ and $L(\bar{\psi}, 1)/\Omega=1/2$. Thus Theorem 1 shows that Ш$(E_{/K})_p=0$ for $p\nmid 14$. Gross has shown ([4] § 22) that Ш$(E_{/K})_2$ $=$Ш $(E_{/K})_7=0$ as well, so Ш$(E_{/K})=0$ and another inflation-restriction argument allows us to conclude that Ш$(E_{/Q})=0$. //

4. Theorem 1 can be restated as follows: *If* $L(E_{/K}, 1)\neq 0$, *then the only primes of K of good reduction, not dividing* $\#(\mathcal{O}_K^{\times})$, *which can occur in* Ш$(E_{/K})$ *are the ones predicted by the Birch and Swinnerton-Dyer conjecture* (*in the refinement given in* [5]). Similarly, if $E$ is defined over $\boldsymbol{Q}$ and has $CM$ by $K$, it follows from Theorem 1 (see remark 2 above) that if $L(E_{/Q}, 1)\neq 0$,

then the only rational primes of good reduction not dividing $\sharp(\mathcal{O}_K^\times)$ which can occur in $Ш(E_{/Q})$ are the ones predicted by the Birch and Swinnerton-Dyer conjecture.

If $L(\bar{\psi}, 1)\neq 0$ and one knows the order of Ш it is a simple matter to check the full Birch and Swinnerton-Dyer conjecture for $E$. In each of the three examples given above, the Birch and Swinnerton-Dyer conjecture is true.

## § 1. Preliminaries

Fix an imaginary quadratic field $K\subset \boldsymbol{C}$ and an elliptic curve $E$, defined over $K$, with complex multiplication by the ring of integers $\mathcal{O}$ of $K$. In particular this ensures that $K$ has class number one. Fix once and for all a prime $\mathfrak{p}$ of $K$, not dividing $\sharp(\mathcal{O}^\times)$, where $E$ has good reduction, and write $K_\mathfrak{p}$ and $\mathcal{O}_\mathfrak{p}$ for the completions of $K$ and $\mathcal{O}$ at $\mathfrak{p}$. Let $E_\mathfrak{p}$ denote the subgroup of $E(\bar{K})$ killed by $\mathfrak{p}$, and let $F=K(E_\mathfrak{p})$ be the extension of $K$ generated by the coordinates of these points.

**Lemma 2.** *Over $F$, $E$ has good reduction everywhere.*

*Proof.* See for example [3], Theorem 2. The proof is an application of the criterion of Néron-Ogg-Shafarevich, using the fact that $E$ has potentially good reduction everywhere, and that $\mathrm{Gal}\,(F(E_{\mathfrak{p}^\infty})/F)\subset 1+\mathfrak{p}\mathcal{O}_\mathfrak{p}$ is torsion-free if $\mathfrak{p}\nmid\sharp(\mathcal{O}^\times)$. //

**Lemma 3.** *$F/K$ is a cyclic extension of degree $N\mathfrak{p}$-1, and $\mathfrak{p}$ is totally ramified in $F/K$.*

*Proof.* That $F/K$ is cyclic of degree dividing $N\mathfrak{p}$-1 follows easily from the natural injection

$$\mathrm{Gal}\,(F/K)\to\mathrm{Aut}\,(E_\mathfrak{p})\cong(\mathcal{O}/\mathfrak{p})^\times.$$

That this map is surjective and that $\mathfrak{p}$ is totally ramified is proved in [3] Lemma 5 using the theory of formal groups, and in [10] § 3 using explicit formulas for complex multiplication. In either case one uses the theory of complex multiplication to show that if $(x, y)$ is a nonzero point of order $\mathfrak{p}$ on a Weierstrass model of $E$ which is minimal at $\mathfrak{p}$, then $x/y$ satisfies a polynomial over $K$ of degree $N\mathfrak{p}$-1 which is an Eisenstein polynomial at $\mathfrak{p}$. //

**Lemma 4.** $E(K_\mathfrak{p})/\mathfrak{p}E(K_\mathfrak{p})\cong\mathcal{O}/\mathfrak{p}$.

*Proof.* By Lemma 3, $E(K_\mathfrak{p})$ has no $\mathfrak{p}$-torsion, and by [6], $E(K_\mathfrak{p})$ has a subgroup of finite index which is free of rank one over $\mathcal{O}_\mathfrak{p}$. //

## § 2. The descent

For any field $k$ we will write $\bar{k}$ for an algebraic closure of $k$ and $G_k = \mathrm{Gal}(\bar{k}/k)$. Fix a generator $\pi$ of the prime $\mathfrak{p}$ and consider the exact sequence

$$0 \longrightarrow E_{\mathfrak{p}} \longrightarrow E(\bar{K}) \xrightarrow{\pi} E(\bar{K}) \longrightarrow 0.$$

This gives rise to a cohomology exact sequence

$$(1) \qquad 0 \longrightarrow E(K)/\mathfrak{p}E(K) \longrightarrow H^1(G_K, E_{\mathfrak{p}}) \longrightarrow H^1(G_K, E(\bar{K}))_{\mathfrak{p}} \longrightarrow 0$$

where $H^1(G_K, E(\bar{K}))_{\mathfrak{p}}$ denotes the $\mathfrak{p}$-torsion in $H^1(G_K, E(\bar{K}))$. Recall that the Tate-Shafarevich group $\text{Ш} = \text{Ш}(E_{/K})$ of $E$ over $K$ is defined by

$$\text{Ш} = \ker [H^1(G_K, E(\bar{K})) \longrightarrow \bigoplus_{\substack{\text{places} \\ v \text{ of } K}} H^1(G_v, E(\bar{K}_v))]$$

where $G_v = \mathrm{Gal}(\bar{K}_v/K_v) \subset G_K$. Also define

$$S(\mathfrak{p}) = \ker [H^1(G_K, E_{\mathfrak{p}}) \longrightarrow \bigoplus_{v} H^1(G_v, E(\bar{K}_v))],$$

$$S'(\mathfrak{p}) = \ker [H^1(G_K, E_{\mathfrak{p}}) \longrightarrow \bigoplus_{v \neq \mathfrak{p}} H^1(G_v, E(\bar{K}_v))].$$

Then $S(\mathfrak{p})$ is the usual Selmer group of $E$ relative to $\mathfrak{p}$ and $S'(\mathfrak{p})$ is the larger group consisting of those cocycles which are locally trivial at all places different from $\mathfrak{p}$. By restricting the sequence (1) we obtain (writing $\text{Ш}_{\mathfrak{p}}$ for the $\mathfrak{p}$-torsion in Ш)

$$(2) \qquad 0 \longrightarrow E(K)/\mathfrak{p}E(K) \longrightarrow S(\mathfrak{p}) \longrightarrow \text{Ш}_{\mathfrak{p}} \longrightarrow 0.$$

We now proceed to describe the Selmer group $S(\mathfrak{p})$. The major difference between the descent described here and, for example, the one given in [2], is Step 3 below, where we make use of the local condition at $\mathfrak{p}$ to bound the size of $S(\mathfrak{p})$ rather than $S'(\mathfrak{p})$. This is necessary when $E$ has supersingular reduction at $\mathfrak{p}$, or when $\mathfrak{p}$ is anomalous for $E$ (see [3]).

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

*Step* 1. *Restriction to* $\mathrm{Hom}(G_F, E_{\mathfrak{p}})$.

The inflation-restriction exact sequence of Galois cohomology yields

$$(3) \qquad 0 \longrightarrow H^1(G, E_{\mathfrak{p}}) \longrightarrow H^1(G_K, E_{\mathfrak{p}}) \xrightarrow{r} H^1(G_F, E_{\mathfrak{p}})^G \longrightarrow H^2(G, E_{\mathfrak{p}})$$

where $r$ denotes the restriction map. We have $H^1(G, E_{\mathfrak{p}}) = H^2(G, E_{\mathfrak{p}}) = 0$ since the order of $G$ is prime to the order of $E_{\mathfrak{p}}$ by Lemma 3. Also,

$H^1(G_F, E_\mathfrak{p}) = \mathrm{Hom}\,(G_F, E_\mathfrak{p})$ because $G_F$ acts trivially on $E_\mathfrak{p}$. Therefore $r$ induces an isomorphism $H^1(G_K, E_\mathfrak{p}) \cong \mathrm{Hom}\,(G_F, E_\mathfrak{p})^G$.

*Step* 2. *Image of* $S'(\mathfrak{p})$ *in* $\mathrm{Hom}\,(G_F, E_\mathfrak{p})^G$.

Let $\mathscr{P}$ denote the unique prime of $F$ above $\mathfrak{p}$, and $p$ the rational prime below $\mathfrak{p}$. Write $X = \mathrm{Gal}\,(M/F)$, where $M$ is the maximal abelian $p$-extension of $F$ unramified outside of $\mathscr{P}$.

**Proposition 5.** *The restriction map* $r$ *of* (3) *induces an injection*

$$0 \longrightarrow S'(\mathfrak{p}) \longrightarrow \mathrm{Hom}\,(X, E_\mathfrak{p})^G.$$

*Proof.* Let $c$ be any element of $S'(\mathfrak{p})$, and $\mathfrak{q}$ any prime of $F$ not dividing $\mathfrak{p}$. By Lemma 2, $E_{/F}$ has good reduction at $\mathfrak{q}$, and therefore (see for example the proof of Theorem 4.2 (b), Chap. X of [9]) the restriction of $r(c)$ to the inertia group of $\mathfrak{q}$ in $G_F$ is trivial. This shows that $r(S'(\mathfrak{p})) \subset \mathrm{Hom}\,(X, E_\mathfrak{p})^G$. //

**Remark.** It is not difficult to show that $r$ induces an isomorphism $S'(\mathfrak{p}) \cong \mathrm{Hom}\,(X, E_\mathfrak{p})^G$ (see [2] § 2) but we will not need this.

*Step* 3. *Image of* $S(\mathfrak{p})$ *in* $\mathrm{Hom}\,(X, E_\mathfrak{p})^G$.

Let $\Phi$ denote the completion of $F$ at $\mathscr{P}$, and recall that $G_\mathfrak{p} = \mathrm{Gal}\,(\bar{K}_\mathfrak{p}/K_\mathfrak{p})$. We have the following diagram in which the top row, the analogue of (1) for $K_\mathfrak{p}$, is exact:

$$\begin{array}{ccccccc} 0 \longrightarrow E(K_\mathfrak{p})/\mathfrak{p}E(K_\mathfrak{p}) & \longrightarrow & H^1(G_\mathfrak{p}, E_\mathfrak{p}) & \longrightarrow & H^1(G_\mathfrak{p}, E(\bar{K}_\mathfrak{p}))_\mathfrak{p} \longrightarrow 0 \\ & & \downarrow & & \\ & & H^1(G_\Phi, E_\mathfrak{p})^G & \xrightarrow{\sim} & \mathrm{Hom}\,(\Phi^\times, E_\mathfrak{p})^G \end{array} \qquad (4)$$

(we have used local class field theory to identify $\mathrm{Hom}\,(G_\Phi, E_\mathfrak{p})$ with $\mathrm{Hom}\,(\Phi^\times, E_\mathfrak{p})$). Write

$$\varphi\colon E(K_\mathfrak{p})/\mathfrak{p}E(K_\mathfrak{p}) \longrightarrow \mathrm{Hom}\,(\Phi^\times, E_\mathfrak{p})^G$$

for the map given by (4). Explicitly, $\varphi(x)(v) = (\gamma - 1)\pi^{-1}x$, where $x \in E(K_\mathfrak{p})$, $v \in \Phi^\times$, and $\gamma$ is the local Artin symbol $[v, \Phi^{\mathrm{ab}}/\Phi]$. Since the restriction map from $H^1(G_\mathfrak{p}, E_\mathfrak{p})$ to $H^1(G_\Phi, E_\mathfrak{p})$ is injective (see Step 1), $\varphi$ is injective as well.

Let $A$ denote the $p$-primary part of the ideal class group of $F$, and $A'$ the $p$-part of the ideal class group of $\mathcal{O}_F[1/\pi]$, which we can identify with the quotient of $A$ by the subgroup generated by the projection of the ideal class of $\mathscr{P}$ into $A$. Let $\mathscr{E}'$ denote the group of $\mathscr{P}$-units of $F$, i.e. those elements which are units at all primes different from $\mathscr{P}$, and let $D$ denote the decomposition group of $\mathscr{P}$ in $X$. By class field theory we have

(5) $$0 \longrightarrow D \longrightarrow X \longrightarrow A' \longrightarrow 0$$

and

(6) $$\mathrm{Hom}(D, E_{\mathfrak{p}}) \cong \mathrm{Hom}(\Phi^{\times}/\bar{\mathscr{E}}', E_{\mathfrak{p}}) \subset \mathrm{Hom}(\Phi^{\times}, E_{\mathfrak{p}}),$$

where $\bar{\mathscr{E}}'$ denotes the closure of $\mathscr{E}'$ in $\Phi^{\times}$. Define a subgroup $\mathscr{S}$ of $\mathrm{Hom}(X, E_{\mathfrak{p}})^G$ by

$$\mathscr{S} = \{f \in \mathrm{Hom}(X, E_{\mathfrak{p}})^G : f|_D \in \mathrm{image}(\varphi)\},$$

and define a subgroup $B$ of $E(K_{\mathfrak{p}})/\mathfrak{p}E(K_{\mathfrak{p}})$ by

(7) $$B = \{x \in E(K_{\mathfrak{p}})/\mathfrak{p}E(K_{\mathfrak{p}}) : \varphi(x)|_{\mathscr{E}'} = 0\}.$$

**Theorem 6.** (i) *There is a natural sequence*

$$0 \longrightarrow \mathrm{Hom}(A', E_{\mathfrak{p}})^G \longrightarrow \mathscr{S} \longrightarrow B.$$

(ii) *The restriction map $r$ of* (3) *induces an injection*

$$0 \longrightarrow S(\mathfrak{p}) \longrightarrow \mathscr{S}.$$

*Proof.* Define a map $\beta: \mathscr{S} \longrightarrow E(K_{\mathfrak{p}})/\mathfrak{p}E(K_{\mathfrak{p}})$ by $\beta(f) = \varphi^{-1}(f|_D)$. By (6), for any $f \in \mathscr{S}$, $\varphi(\beta(f)) = f|_D$ is trivial on $\mathscr{E}'$, i.e. $\beta(f) \in B$. By (5) we see

$$\mathrm{Hom}(A', E_{\mathfrak{p}})^G = \ker[\mathrm{Hom}(X, E_{\mathfrak{p}})^G \longrightarrow \mathrm{Hom}(D, E_{\mathfrak{p}})] = \ker(\beta).$$

This proves (i).

Proposition 5 shows that $r$ gives an injection of $S(\mathfrak{p})$ into $\mathrm{Hom}(X, E_{\mathfrak{p}})^G$. Let $c$ be any element of $S(\mathfrak{p})$ and write $c_{\mathfrak{p}}$ for the image of $c$ in $H^1(G_{\mathfrak{p}}, E_{\mathfrak{p}})$. Since $c$ maps to 0 in $H^1(G_{\mathfrak{p}}, E(\bar{K}_{\mathfrak{p}}))_{\mathfrak{p}}$, the image of $c_{\mathfrak{p}}$ in $\mathrm{Hom}(\Phi^{\times}, E_{\mathfrak{p}})$ under (4) lies in the image of $\varphi$. But (using (6)) the image of $c_{\mathfrak{p}}$ in $\mathrm{Hom}(\Phi^{\times}, E_{\mathfrak{p}})$ is precisely the restriction of $r(c)$ to $D$. Therefore $r$ maps $S(\mathfrak{p})$ into $\mathscr{S}$, and (ii) follows. //

**Remark.** Using the fact that $S'(\mathfrak{p}) \cong \mathrm{Hom}(X, E_{\mathfrak{p}})^G$ (see the remark at the end of Step 2) the proof of Theorem 6 (ii) actually shows that $S(\mathfrak{p}) \cong \mathscr{S}$.

## § 3. The reciprocity law map

By Lemma 4 we can fix an isomorphism

(8) $$\lambda: E(K_{\mathfrak{p}})/\mathfrak{p}E(K_{\mathfrak{p}}) \xrightarrow{\sim} \mathcal{O}/\mathfrak{p}.$$

Recall that $\varphi\colon E(K_{\mathfrak{p}})/\mathfrak{p}E(K_{\mathfrak{p}}) \longrightarrow \mathrm{Hom}(\Phi^{\times}, E_{\mathfrak{p}})^{G}$ is the map defined by (4).

**Proposition 7.** *There is a unique G-equivariant map $\delta\colon \Phi^{\times} \to E_{\mathfrak{p}}$ such that $\varphi(x)(v) = \lambda(x)\delta(v)$ for all $x \in E(K_{\mathfrak{p}})$ and $v \in \Phi^{\times}$.*

*Proof.* We can define $\delta$ by

$$\delta\colon \Phi^{\times} \longrightarrow \mathrm{Hom}(E(K_{\mathfrak{p}}), E_{\mathfrak{p}}) \xrightarrow{\sim} \mathrm{Hom}(\mathcal{O}, E_{\mathfrak{p}}) \cong E_{\mathfrak{p}}$$

where the first map is given by sending $v \in \Phi^{\times}$ to $\varphi(\cdot)(v) \in \mathrm{Hom}(E(K_{\mathfrak{p}}), E_{\mathfrak{p}})$, and the second is induced by (8). (Concretely, $\delta(v) = \varphi(\lambda^{-1}(1))(v)$.) The uniqueness is clear. //

Write $\mathscr{P}_{\Phi}$ for the maximal ideal of $\Phi$ and for every $n \geq 1$ define $\mathscr{U}_n = 1 + (\mathscr{P}_{\Phi})^n$. Fix a uniformizing parameter $u$ of $\Phi$. Since $\Phi/K_{\mathfrak{p}}$ is totally ramified (Lemma 3), for every $v \in \mathscr{U}_1$ there is a unique element $d(v) \in \mathcal{O}/\mathfrak{p}$ satisfying $v \equiv 1 + d(v)u \pmod{u^2}$. This map $d$ is a homomorphism from $\mathscr{U}_1$ to $\mathcal{O}/\mathfrak{p}$ with kernel $\mathscr{U}_2$, called the logarithmic derivative homomorphism (with respect to $u$).

**Theorem 8.** *Let $\delta$ be the reciprocity map of Proposition 7. Then* $\ker(\delta) \cap \mathscr{U}_1 = \mathscr{U}_2$.

*Proof.* The explicit reciprocity law of Wiles [13] says that there is a nonzero $\tau \in E_{\mathfrak{p}}$ such that $\delta(v) = d(v)\tau$ for every $v \in \mathscr{U}_1$, and the theorem follows immediately. As we do not need the full strength theorem, we give a simpler proof using the following result of Stark [10].

**Proposition 9.** *Suppose $x \in E(K_{\mathfrak{p}})$ and $x \notin \mathfrak{p}E(K_{\mathfrak{p}})$. Then $\Phi(\pi^{-1}x)/\Phi$ is an abelian extension of conductor $(\mathscr{P}_{\Phi})^2$.*

*Proof.* This is Theorem 1 of [10]. The proof given there is a discriminant calculation using Kronecker's limit formula. //

*Proof of Theorem* 8. Recall that for any $v \in \Phi^{\times}$ and $x \in E(K_{\mathfrak{p}})$, $\varphi(x)(v) = (\gamma - 1)\pi^{-1}x$, where $\gamma$ is the local Artin symbol $[v, \Phi^{\mathrm{ab}}/\Phi]$. By Proposition 9, the image of $\mathscr{U}_2$ under the local Artin map acts trivially on $\Phi(\pi^{-1}E(K_{\mathfrak{p}}))$, so $\mathscr{U}_2 \subset \ker(\delta)$. If $\delta$ were trivial on all of $\mathscr{U}_1$, we would have $\delta \in \mathrm{Hom}(\Phi^{\times}/\mathscr{U}_1, E_{\mathfrak{p}})^G \cong \mathrm{Hom}(\boldsymbol{Z} \times \boldsymbol{\mu}_{N\mathfrak{p}-1}, E_{\mathfrak{p}})^G = 0$. This is impossible since $\varphi$ is injective and therefore not identically zero.

Thus $\delta$ induces a nontrivial $G$-homomorphism from $\mathscr{U}_1/\mathscr{U}_2$ to $E_{\mathfrak{p}}$, which must be surjective because $G$ acts transitively on the nonzero elements of $E_{\mathfrak{p}}$. Since $[\mathscr{U}_1 : \mathscr{U}_2] = \#(E_{\mathfrak{p}}) = N\mathfrak{p}$, this map must be injective as well and the theorem follows. //

## § 4. Elliptic units and $L(\bar{\psi}, 1)$

Write $\mathscr{C}$ for the group of elliptic units of $F$, for example as defined in the Appendix of [8]. (If the residue characteristic of $\mathfrak{p}$ is greater than 3 one can use the group of elliptic units defined in [3], § 5.)

Fix an $\mathcal{O}$-generator $\Omega \in \boldsymbol{C}^\times$ of the period lattice of a minimal model of $E$, and let $\psi$ be the Hecke character of $K$ attached to $E$. Define $\mathscr{L}=\#(E(K)_{\text{torsion}})L(\bar{\psi}, 1)/\Omega$; it is known that $\mathscr{L} \in K$.

Recall that $\pi$ is a generator of $\mathfrak{p}$, and $d$ is the logarithmic derivative homomorphism defined in § 3. The next result, due to Coates and Wiles [3], provides the crucial link between the algebraic and analytic sides of our picture.

**Theorem 10.** *There is an elliptic unit $\xi \in \mathscr{C} \cap \mathscr{U}_1$ such that $d(\xi)=\mathscr{L}$.*

*Proof.* This is a computation using explicit formulas for elliptic units in terms of the sigma function. See [3] § 5 or [10] § 2, or for maximum generality (including the extra factor of $\#(E(K)_{\text{torsion}})$, which can be divisible by $\mathfrak{p}$ only for $N\mathfrak{p} \leq 7$) see [8] Theorem 12.11. //

**Theorem 11.** *Let $\delta$ be the reciprocity map of Proposition 7. If $\mathscr{L} \not\equiv 0$ (modulo $\mathfrak{p}$) then there is an elliptic unit $\xi \in \mathscr{C}$ such that $\delta(\xi) \neq 0$.*

*Proof.* Let $\xi$ be an elliptic unit satisfying Theorem 10. Then $\xi \in \mathscr{U}_1$ and $d(\xi) \neq 0$, so $\xi \notin \mathscr{U}_2$ and by Theorem 8, $\delta(\xi) \neq 0$. //

Recall that $p$ is the rational prime below $\mathfrak{p}$. Define characters of $G_K = \mathrm{Gal}(\bar{K}/K)$

$$\omega\colon G_K \longrightarrow \boldsymbol{\mu}_{p-1} \subset \boldsymbol{Z}_p^\times \qquad \text{by } \zeta^\sigma = \zeta^{\omega(\sigma)} \text{ for all } \zeta \in \boldsymbol{\mu}_p,\ \sigma \in G_K$$

$$\chi\colon G_K \longrightarrow \boldsymbol{\mu}_{N\mathfrak{p}-1} \subset \mathcal{O}_\mathfrak{p}^\times \qquad \text{by } \sigma\nu = \chi(\sigma)\nu \text{ for all } \nu \in E_\mathfrak{p},\ \sigma \in G_K.$$

If $[K_\mathfrak{p}\colon \boldsymbol{Q}_p]=2$ write $*$ for the action of the nontrivial automorphism of $K_\mathfrak{p}/\boldsymbol{Q}_p$. Define an irreducible $\boldsymbol{Z}_p$-representation $\rho$ of $G$ by

$$\rho=\chi \qquad \text{if } \chi \text{ is } \boldsymbol{Z}_p^\times\text{-valued,}$$

$$\rho=\chi \oplus \chi^* \qquad \text{if } \chi \text{ is not } \boldsymbol{Z}_p^\times\text{-valued.}$$

For any $G$-module $M$, we will denote by $M^\rho$ the $\rho$-eigenspace ($\rho$-isotypic component) of the $p$-adic completion $\varprojlim M/p^m M$ of $M$ for the action of $G$.

**Proposition 12.** *If $\mathscr{L} \not\equiv 0$ (modulo $\mathfrak{p}$) then $\mathscr{C}^\rho \not\subset (\Phi^\times)^p$.*

*Proof.* Suppose $\mathscr{C}^\rho \subset (\Phi^\times)^p$. Then $\delta$ would vanish on $\mathscr{C}^\rho$, and therefore also (since $\mathrm{Hom}(\mathscr{C}, E_\mathfrak{p})^G = \mathrm{Hom}(\mathscr{C}^\rho, E_\mathfrak{p})^G$) on all of $\mathscr{C}$. By Theorem 11 this is not the case. //

## § 5. Proof of Theorem 1

To control the size of the Selmer group $S(\mathfrak{p})$, by Theorem 6 it suffices to control $\mathrm{Hom}(A, E_\mathfrak{p})^G$ and $B$, where $A$ is the $p$-primary part of the ideal class group of $F$ and $B$ is the subgroup of $E(K_\mathfrak{p})/\mathfrak{p}E(K_\mathfrak{p})$ defined by (7). Write $\mathcal{O}_F^\times$ for the global units of $F$, and as in § 4 let $\mathscr{L} = \sharp(E(K)_{\mathrm{torsion}}) \times L(\bar{\psi}, 1)/\Omega$.

**Theorem 13.** *If* $\mathscr{L} \not\equiv 0 \pmod{\mathfrak{p}}$ *then* $B=0$.

*Proof.* Fix an elliptic unit $\xi \in \mathscr{C} \subset \mathcal{O}_F^\times$ satisfying Theorem 11, i.e. $\delta(\xi) \neq 0$ in $E_\mathfrak{p}$. If $x \in B$, then $\varphi(x)(\xi) = 0$ by definition of $B$, and so $\lambda(x)\delta(\xi) = 0$ by definition of $\delta$. Therefore $\lambda(x)=0$, and so $x=0$ in $E(K_\mathfrak{p})/\mathfrak{p}E(K_\mathfrak{p})$. //

By Proposition 12.4 of the Appendix of [8], the group of elliptic units $\mathscr{C}$ is contained in the group of special units of $F$ defined in [7], so we can apply the results of [7] (which extend Thaine's results [11]) to study the ideal class group $A$.

**Theorem 14.** *If* $\mathscr{L} \not\equiv 0 \pmod{\mathfrak{p}}$ *then* $A^\rho = 0$.

*Proof.* Observe that $\rho \neq 1$ by Lemma 3, and $\boldsymbol{Z}_p[G]^\rho$ is isomorphic to the ring of integers of the unramified extension of $\boldsymbol{Q}_p$ of degree $\dim(\rho)$. Write $W = (\mathcal{O}_F^\times)^\rho$, and write $\check{\rho}$ for the contragredient of $\rho$ (given simply by $\check{\rho}(\sigma) = \rho(\sigma^{-1})$).

*Case* I: $\boldsymbol{\mu}_p \not\subset F$ or $\rho \neq \check{\rho} \otimes \omega$.

By Proposition 12 the image of $\mathscr{C}^\rho$ in $W/W^p$ is nontrivial. Therefore (since $W/W^p$ is free over the finite field $(\boldsymbol{Z}/p\boldsymbol{Z})[G]^\rho$) we can fix a map

$$\alpha\colon W \longrightarrow (\boldsymbol{Z}/p\boldsymbol{Z})[G]^\rho$$

such that $\alpha(\mathscr{C}^\rho) = (\boldsymbol{Z}/p\boldsymbol{Z})[G]^\rho$. Since $\boldsymbol{\mu}_p \not\subset F$ or $\rho \neq \check{\rho} \otimes \omega$ we can apply Theorem 3.1 of [7] with the map $\alpha$ to conclude that $A^\rho/pA^\rho = 0$, and therefore $A^\rho = 0$.

*Case* II: $\boldsymbol{\mu}_p \subset F$ and $\rho = \check{\rho} \otimes \omega$.

Since $\rho \neq 1$ we have $\rho \neq \omega$, so $\boldsymbol{\mu}_p \not\subset W$ and thus $W$ is free over $\boldsymbol{Z}_p[G]^\rho$. Therefore by Proposition 12 we can fix a map

$$\alpha\colon W \longrightarrow \boldsymbol{Z}_p[G]^\rho$$

such that $\alpha(\mathscr{C}^{\rho})=\boldsymbol{Z}_p[G]^{\rho}$. Since $\rho\neq 1$ and $\mathcal{O}_F^{\times}$ has a subgroup of finite index which is cyclic over $\boldsymbol{Z}[G]$, we can apply Corollary 3.7 of [7] with the map $\alpha$ to conclude that $A^{\rho}=0$. //

*Proof of Theorem* 1. Suppose $\mathscr{L}\not\equiv 0 \pmod{\mathfrak{p}}$. We use the notation of §2; in particular $\mathscr{S}$ is the subgroup of $\mathrm{Hom}(X, E_{\mathfrak{p}})^G$ and $A'$ the quotient of $A$ defined there. Theorem 6 shows that $S(\mathfrak{p})$ is isomorphic to a subgroup of $\mathscr{S}$, and that $\mathscr{S}$ fits into an exact sequence

$$0\longrightarrow \mathrm{Hom}(A', E_{\mathfrak{p}})^G \longrightarrow \mathscr{S} \longrightarrow B.$$

By Theorem 13, $B=0$, and $\mathrm{Hom}(A', E_{\mathfrak{p}})^G\subset \mathrm{Hom}(A^{\rho}, E_{\mathfrak{p}})$ is zero by Theorem 14. Therefore $S(\mathfrak{p})=0$. Now from the exact sequence (2)

$$0\longrightarrow E(K)/\mathfrak{p}E(K)\longrightarrow S(\mathfrak{p})\longrightarrow Ш_{\mathfrak{p}}\longrightarrow 0,$$

which is essentially the defintion of $S(\mathfrak{p})$, we conclude that $Ш_{\mathfrak{p}}=0$. //

**Remark.** Notice that in the above proof of Theorem 1 we can also conclude that if $\mathscr{L}\not\equiv 0 \pmod{\mathfrak{p}}$ then $E(K)$ is finite, so we obtain a proof of the theorem of Coates and Wiles [3]. The major difference between this proof and theirs is that by controlling $A^{\rho}$ we are able to work entirely over the field $K(E_{\mathfrak{p}})$, while they had to use the fields $K(E_{\mathfrak{p}^n})$ for all $n$.

## References


[1] Cassels, J. W. S., The rational solutions of the diophantine equation $Y^2=X^3-D$, Acta Math., **82** (1950), 243–273.

[2] Coates, J., Infinite descent on elliptic curves, In: Arithmetic and Geometry, papers dedicated to I. R. Shafarevich on the occasion of his 60th birthday, Prog. in Math., **35**, 107–136, Boston: Birkhauser (1983).

[3] Coates, J. and Wiles, A., On the conjecture of Birch and Swinnerton-Dyer, Invent. Math., **39** (1977), 223–251.

[4] Gross, B., Arithmetic on elliptic curves with complex multiplication, Lect. Notes Math., **776**, New York: Springer (1980).

[5] ——, On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication, In: Number Theory Related to Fermat's Last Theorem, Prog. in Math., **26**, 219–236. Boston: Birkhauser (1982).

[6] Lutz, E., Sur l'équation $y^2=x^3-Ax-B$ dans les corps $p$-adiques. J. reine Angew. Math., **177** (1937), 238–247.

[7] Rubin, K., Global units and ideal class groups, Invent. Math., **89** (1987), 511–526.

[8] ——, Tate-Shafarevich groups and $L$-functions of elliptic curves with complex multiplication, Invent. Math., **89** (1987), 527–560.

[9] Silverman, J., The Arithmetic of Elliptic Curves, Graduate Texts in Math., **106**, New York: Springer (1986).

[10] Stark, H., The Coates-Wiles theorem revisited, In: Number Theory Related to Fermat's Last Theorem, Prog. in Math., **26**, 349–362. Boston: Birkhauser (1982).

[11] Thaine, F., On the ideal class groups of real abelian number fields, Ann. of Math., **128** (1988), 1–18.
[12] Weil, A., Number Theory, an approach through history, Boston: Birkhauser (1984).
[13] Wiles, A. Higher explicit reciprocity laws, Ann. of Math., **107** (1978), 235–254.

*Department of Mathematics*
*The Ohio State University*
*Columbus OH 43210-1174*
*U.S.A.*