COMPOSITIO MATHEMATICA

KARL RUBIN

# Elliptic curves and $\mathbb{Z}_p$-extensions

*Compositio Mathematica*, tome 56, n° 2 (1985), p. 237-250
<http://www.numdam.org/item?id=CM_1985__56_2_237_0>

Compositio Mathematica 56 (1985) 237–250.


# ELLIPTIC CURVES AND $\mathbb{Z}_p$-EXTENSIONS

Karl Rubin *

## Introduction

Let $E$ be an elliptic curve defined over a number field $F$, with complex multiplication by the ring of integers $\mathcal{O}$ of an imaginary quadratic field $K$. For simplicity we will assume $K \subset F$. Fix a rational prime $p > 2$ such that $E$ has good reduction at all primes of $F$ above $p$, and let $\mathfrak{F} = F(E_{p^\infty})$, the extension of $F$ generated by the coordinates of all $p$-power torsion points of $E$. The theory of complex multiplication shows that the natural map

$$\mathrm{Gal}(\mathfrak{F}/F) \hookrightarrow \mathrm{Aut}(E_{p^\infty}) \cong (\mathcal{O} \otimes \mathbb{Z}_p)^\times \tag{1}$$

has finite cokernel, so $\mathfrak{F}$ is an (infinite) abelian extension of $F$ and $\mathrm{Gal}(\mathfrak{F}/F) \simeq \Delta \times \mathbb{Z}_p^2$ where $\Delta$ is a finite group. In this paper we will study arithmetic invariants of $E$, namely the Mordell-Weil group and Tate-Safarevic group of $E$ over subfields of $\mathfrak{F}$ containing $F$.

This study, which uses techniques of Iwasawa theory, divides naturally into two cases according as $p$ splits in $K$ into two distinct primes or not. The case where $p$ splits, which will not be discussed at all here, has been studied extensively since the initial work of Coates and Wiles [5] and a very satisfiactory theory has been developed. For a general reference see [4].

In the present paper we will consider only the other case, where $p$ remains prime or ramifies in $K$. The reader who is familiar with the split case will notice that although the method of attack starts off the same, the present case is more difficult and in many instances the conclusions are quite different. See §6 for some examples. The results of the first three sections are contained in the author's Ph.D. thesis [14] and more detailed proofs can be found there.

NOTATION: If $L/M$ is a Galois extension of fields $G(L/M)$ will denote the corresponding Galois group, $\overline{M}$ the algebraic closure of $M$ and $G_M = G(\overline{M}/M)$. If $A$ is an abelian group and $l$ a prime, we write $A_{l^n}$ for the subgroup of $l^n$-torsion points in $A$ and $A_{l^\infty} = \bigcup_n A_{l^n}$. If $A$ is also a $G(L/M)$ module then $A^{G(L/M)}$ will denote the submodule of elements fixed by $G(L/M)$.

* NSF postdoctoral fellow

§1. Let $E$, $F$, $\mathcal{O}$, $K$, and $p$ be as in the introduction, and we further require that $p\mathcal{O}$ be a prime ideal of $\mathcal{O}$ (the case where $p$ ramifies can be treated in exactly the same way). We begin by recalling some definitions.

Let $M$ be an algebraic extension of $F$. For any $n > 0$ we have an exact sequence

$$0 \to E_{p^n} \to E(\overline{M}) \xrightarrow{p^n} E(\overline{M}) \to 0$$

which gives rise to a $G_M$-cohomology exact sequence

$$0 \to E(M)/p^n E(M) \to H^1(G_M, E_{p^n}) \to H^1(E/M)_{p^n} \to 0$$

where we write $H^1(E/M)$ for $H^1(G_M, E(\overline{M}))$. Letting $n$ go to infinity and taking direct limits we obtain

$$0 \to E(M) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(G_M, E_{p^\infty}) \to H^1(E/M)_{p^\infty} \to 0. \tag{2}$$

Let $Ш(M)$ denote the $p$-primary part of the Tate-Safarevic group of $E$ over $M$, defined to be the kernel of the map

$$H^1(E/M)_{p^\infty} \to \bigoplus_{\mathfrak{q}} H^1(E/M_{\mathfrak{q}})$$

where the sum is taken over all primes $\mathfrak{q}$ of $M$. Also define the $p$-Selmer group $S(M)$ to be the subgroup of $H^1(G_M, E_{p^\infty})$ which makes the sequence

$$0 \to E(M) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to S(M) \to Ш(M) \to 0, \tag{3}$$

obtained by restricting (2), exact.

We similarly define a generalized Tate-Safarevic group $Ш'(M)$ to be the kernel of the map

$$H^1(E/M)_{p^\infty} \to \bigoplus_{\mathfrak{q} \nmid p} H^1(E/M_{\mathfrak{q}})$$

and the corresponding Selmer group $S'(M) \subset H^1(G_M, E_{p^\infty})$ so that

$$0 \to E(M) \otimes \mathbb{Q}_q/\mathbb{Z}_p \to S'(M) \to Ш'(M) \to 0 \tag{4}$$

is exact.

REMARK: If $M = \bigcup_{i=1}^{\infty} L_i$ with $L_1 \subset L_2 \subset \ldots$ then it is an exercise in Galois cohomology to show

$$Ш(M) = \varinjlim Ш(L_i),\ S(M) = \varinjlim S(L_i) \tag{5}$$

and similarly for $Ш'(M)$ and $S'(M)$.

In general we have $Ш(M) \subset Ш'(M)$, $S(M) \subset S'(M)$ and $Ш'(M)/Ш(M) \simeq S'(M)/S(M)$. Although we are primarily interested in $S(M)$ we deal with $S'(M)$ because it is easier to compute (see Propositions 1.1 and 1.2 below). In §§2 and 4 we study the difference between $S$ and $S'$.

Recall $\mathfrak{F} = F(E_\infty)$. Let $\mathfrak{M}$ denote the maximal abelian $p$-extension of $\mathfrak{F}$ unramified outside primes above $p$, and set $X = G(\mathfrak{M}/\mathfrak{F})$. Analogues of the following two propositions are proved in [4] (Theorems 9 and 12) for the case where $p$ splits in $K$. The proofs in our case are the same and we sketch them below.

PROPOSITION 1.1: $S'(\mathfrak{F}) \simeq \mathrm{Hom}(X, E_{p^\infty})$.

PROOF: We have

$$S'(\mathfrak{F}) \subset H^1(G_{\mathfrak{F}}, E_{p^\infty}) = \mathrm{Hom}(G_{\mathfrak{F}}, E_{p^\infty}).$$

Clearly any homomorphism from $G_{\mathfrak{F}}$ to $E_{p^\infty}$ must factor through the Galois group of the maximal abelian $p$-extension of $\mathfrak{F}$. Since $E$ has good reduction everywhere over $\mathfrak{F}$ ([5] Theorem 2) it follows from Lemma 4.1 of [3] that the elements of $S'(\mathfrak{F})$ are precisely those homomorphisms which are unramified outside primes above $p$. This proves the proposition.

PROPOSITION 1.2: *Suppose $F \subset M \subset \mathfrak{F}$. Then there is a natural map*

$$S'(M) \to \mathrm{Hom}(X, E_{p^\infty})^{G(\mathfrak{F}/M)}$$

*with finite kernel and cokernel. If $M/F$ is infinite then this map is an isomorphism.*

PROOF: The Hochschild-Serre spectral sequence [9] gives an exact sequence

$$0 \to H^1(G(\mathfrak{F}/M), E_{p^\infty}) \to H^1(G_M, E_{p^\infty}) \xrightarrow{Q} H^1(G_{\mathfrak{F}}, E_{p^\infty})^{G(\mathfrak{F}/M)}$$

$$\to H^2(G(\mathfrak{F}/M), E_{p^\infty}). \tag{6}$$

It is clear that the restriction map $Q$ maps $S'(M)$ into $S'(\mathfrak{F})$. Conversely one can show that

$$Q^{-1}(S'(\mathfrak{F})) \subset S'(M),$$

using Lemma 4.1 of [3] and the fact that only primes above $p$ can ramify in $\mathfrak{F}/M(E_p)$.

Thus (6) induces an exact sequence

$$0 \to H^1\big(G(\mathfrak{F}/M),\ E_{p^\infty}\big) \to S'(M) \to S'(\mathfrak{F})^{G(\mathfrak{F}/M)}$$
$$\to H^2\big(G(\mathfrak{F}/M),\ E_{p^\infty}\big).$$

Now to prove the proposition it is enough to show

$$H^1\big(G(\mathfrak{F}/M),\ E_{p^\infty}\big) \cong \begin{cases} 0 & \text{if } M/F \text{ is infinite} \\ E(M)_{p^\infty} & \text{otherwise.} \end{cases} \tag{7}$$

By (1), $H^1(G(\mathfrak{F}/M), E_{p^\infty}) \simeq H^1(U, K_p/\mathcal{O}_p)$ where $U \subset 1 + p\mathcal{O}_p$ and $U$ acts on $K_p/\mathcal{O}_p$ by multiplication. If $M/F$ is infinite then $U$ is cyclic and one computes easily $H^1(U, K_p/\mathcal{O}_p) = 0$. Otherwise we can write $U = V \times W$ with $V$ and $W$ cyclic, and use the inflation-restriction sequence

$$0 \to H^1\Big(V, \big(K_p/\mathcal{O}_p\big)^W\Big) \to H^1\big(U,\ K_p/\mathcal{O}_p\big) \to H^1\big(W,\ K_p/\mathcal{O}_p\big) = 0$$

to complete the proof.

§2. THEOREM 2.1: *Suppose $M_\infty$ is an infinite extension of $F$ contained in $\mathfrak{F}$. Then $Ш(M_\infty) = Ш'(M_\infty)$ and $S(M_\infty) = S'(M_\infty)$.*

The main ingredients in the proof of this theorem are Tate duality and the following lemma.

LEMMA 2.2: *Suppose $\Phi$ is a finite extension of $\mathbb{Q}_p$, and $\Phi_\infty = \bigcup_n \Phi_n$ is a ramified extension of $\Phi$ with $G(\Phi_\infty/\Phi) \simeq \mathbb{Z}_p^d$, $d \geqslant 1$. Let $\mathbb{G}$ be a formal group defined over the ring of integers of $\Phi$, of height $\geqslant 2$. Then*

$$\bigcap_n N_n\big(\mathbb{G}(\Phi_n)\big) = 0$$

*where $\mathbb{G}(\Phi_n)$ denotes the maximal ideal of $\Phi_n$ endowed with the group structure induced by $\mathbb{G}$, and $N_n$ denotes the norm map from $\mathbb{G}(\Phi_n)$ to $\mathbb{G}(\Phi)$.*

For the proof of this lemma see [14] Lemma 3.7 or [10]. If we label the fields $\Phi_n$ so $[\Phi_n : \Phi] = p^{nd}$, one can show by brute force using the logarithm map of $\mathbb{G}$ that

$$N_n\mathbb{G}(\Phi_n) \subset p^{[n(1-1/h)]-c}\mathbb{G}(\Phi)$$

where $h$ is the height of $\mathbb{G}$ and $c$ is a constant independent of $n$.

PROOF OF THEOREM 2.1: The description of $G(\mathfrak{X}/F)$ given by (1) shows that we can find a finite extension $M_0$ of $F$ contained in $M_\infty$ so that $G(M_\infty/M_0) \cong \mathbb{Z}_p^d$, $d = 1$ or 2. By choosing $M_0$ large enough we may also assume that each prime of $M_0$ above $p$ is totally ramified in $M_\infty/M_0$. Write $M_\infty = \bigcup_n M_n$.

Let $\mathcal{S}$ denote the set of primes of $M_0$ lying above $p$. Then every $\mathfrak{p} \in \mathcal{S}$ has a unique extension to each $M_n$ and we will write $M_{n,\mathfrak{p}}$ for the completion of $M_n$ at that prime.

For each $n$ we have an exact sequence

$$0 \to Ш(M_n) \to Ш'(M_n) \to \bigoplus_{\mathfrak{p} \in \mathcal{S}} H^1(E/M_{n,\mathfrak{p}})$$

so by (5) to show $Ш(M_\infty) = Ш'(M_\infty)$ it clearly will suffice to show that the $p$-part of $\varinjlim H^1(E/M_{n,\mathfrak{p}})$ is 0 for every $\mathfrak{p} \in \mathcal{S}$.

By Tate duality [17], $\varinjlim H^1(E/M_{n,\mathfrak{p}})$ is dual to $\varprojlim E(M_{n,\mathfrak{p}})$ where the inverse limit is taken with respect to the norm maps on $E(M_{n,\mathfrak{p}})$. Our assumptions on $p$ insure that $E$ has good supersingular reduction at $\mathfrak{p}$ so it follows that the $p$-part of $\varinjlim H^1(E/M_{n,\mathfrak{p}})$ is dual to $\varprojlim E_1(M_{n,\mathfrak{p}})$, where $E_1(M_{n,\mathfrak{p}})$ denotes the kernel of reduction modulo $\mathfrak{p}$ in $E(M_{n,\mathfrak{p}})$.

Write $\mathbb{E}$ for the formal group over $M_{0,\mathfrak{p}}$ giving the kernel of reduction mod $\mathfrak{p}$ on $E$. Then $\mathbb{E}(M_{n,\mathfrak{p}}) \cong E_1(M_{n,\mathfrak{p}})$ for every $n$, and $\mathbb{E}$ has height 2 since (using supersingular reduction again) $\mathbb{E}(\overline{M_{0,\mathfrak{p}}})_p \cong E_1(\overline{M_{0,\mathfrak{p}}})_p$ has $p^2$ elements. Therefore

$$\varprojlim E_1(M_{n,\mathfrak{p}}) = 0$$

by Lemma 2.2. This proves $Ш(M_\infty) = Ш'(M_\infty)$ and it follows that $S(M_\infty) = S'(M_\infty)$ as well.

REMARK: The proof above shows $Ш(M_\infty) = Ш'(M_\infty)$ by showing that *any* cocycle in $H^1(E/M_n)$ becomes locally trivial at all primes above $p$ when restricted to $H^1(E/M_\infty)$. Unfortunately this says nothing about the size of $Ш'(M_n)/Ш(M_n)$ for individual $n$. More precisely, we have "bounded" $Ш'(M_n)/Ш(M_n)$ by $\oplus_{\mathfrak{p} \in \mathcal{S}} H^1(E/M_{n,\mathfrak{p}})$. For each $n$, $\oplus_{\mathfrak{p} \in \mathcal{S}} H^1(E/M_{n,\mathfrak{p}})$ has a subgroup isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^{[M_n:\mathbb{Q}]}$, but still

$$\varinjlim \bigoplus_{\mathfrak{p} \in \mathcal{S}} H^1(E/M_{n,\mathfrak{p}}) = 0.$$

The same can happen with $Ш'(M_n)/Ш(M_n)$: it could be growing larger and larger with $n$, while still $Ш'(M_\infty) = Ш(M_\infty)$.

§3. In this section we use Iwasawa theory and the results of the previous two sections to study the size of the Selmer group. We first introduce some notation.

For any $\mathcal{O}_p$-module $A$ we define

$$\text{Dual}(A) = \text{Hom}_{\mathcal{O}_p}(A, K_p/\mathcal{O}_p).$$

If $A$ is a module over an integral domain $R$ with field of fractions $k$ define

$$\text{rank}_R A = \dim_k A \otimes_R k,$$

and if $\mathcal{O}_p \subset R$

$$\text{corank}_R A = \text{rank}_R \text{Dual}(A).$$

Let

$$G(\mathfrak{F}/F) \cong \Delta \times \mathbb{Z}_p^2$$

be the decomposition given by (1), and $F_\infty = \mathfrak{F}^\Delta$ the unique $\mathbb{Z}_p^2$-extension of $F$ inside $\mathfrak{F}$. If $M$ is any extension of $F$ inside $\mathfrak{F}$ let $\Lambda(M)$ denote the Iwasawa algebra $\mathcal{O}_p[[G(M/F)]]$, i.e.

$$\Lambda(M) = \varprojlim_L \mathcal{O}_p[G(L/F)]$$

with the inverse limit taken over finite extensions $L$ of $F$ contained in $M$. If $G(M/F) \simeq \mathbb{Z}_p^d$ then $\Lambda(M)$ is isomorphic to the ring of formal power series in $d$ variables over $\mathcal{O}_p$.

Recall $\mathfrak{M}$ is the maximal abelian $p$-extension of $\mathfrak{F}$ unramified outside primes above $p$, and $X = G(\mathfrak{M}/\mathfrak{F})$. Let

$$X(-1) = X \otimes_{\mathbb{Z}_p} \text{Hom}_{\mathcal{O}_p}(E_{p^\infty}, K_p/\mathcal{O}_p)$$

so

$$\text{Hom}(X, E_{p^\infty}) \simeq \text{Hom}_{\mathcal{O}_p}(X(-1), K_p/\mathcal{O}_p)$$

and $X(-1)$ is a $\Lambda(\mathfrak{F})$-module. The following is a slight modification of a theorem of Greenberg.

THEOREM 3.1: *$X(-1)^\Delta$ is a finitely generated $\Lambda(F_\infty)$-module and* $\text{rank}_{\Lambda(F_\infty)} X(-1)^\Delta = [F: K]$.

PROOF: [6].

COROLLARY 3.2: $\operatorname{Corank}_{\Lambda(F_\infty)} S'(F_\infty) = \operatorname{corank}_{\Lambda(F_\infty)} S(F_\infty) = \operatorname{corank}_{\Lambda(F_\infty)} E(F_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p + \operatorname{corank}_{\Lambda(F_\infty)} Ш(F_\infty) = [F: K]$.

PROOF: The first equality follows from Theorem 2.1, the second from (3). By Proposition 1.2,

$$S'(F_\infty) \cong \operatorname{Hom}_{\mathcal{O}_p}\left(X(-1),\ K_p/\mathcal{O}_p\right)^\Delta = \operatorname{Hom}_{\mathcal{O}_p}\left(X(-1)^\Delta,\ K_p/\mathcal{O}_p\right)$$

so $\operatorname{corank}_{\Lambda(F_\infty)} S'(F_\infty) = \operatorname{rank}_{\Lambda(F_\infty)} X(-1)^\Delta = [F: K]$.

COROLLARY 3.3: *If $M_\infty$ is any $\mathbb{Z}_p$-extension of $F$ in $F_\infty$ then* $\operatorname{Dual}(S(M_\infty))$ *is a finitely generated* $\Lambda(M_\infty)$*-module and* $\operatorname{corank}_{\Lambda(M_\infty)} S(M_\infty) = \operatorname{corank}_{\Lambda(M_\infty)} E(M_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p + \operatorname{corank}_{\Lambda(M_\infty)} Ш(M_\infty) \geq [F: K]$.

PROOF: Let $\gamma$ be a topological generator of $G(F_\infty/M_\infty)$. Then $\Lambda(M_\infty) = \Lambda(F_\infty)/(\gamma - 1)\Lambda(F_\infty)$. By Proposition 1.2 and Theorem 2.1,

$$S(M_\infty) = S'(M_\infty) = S(F_\infty)^{G(F_\infty/M_\infty)}$$

so

$$\begin{aligned}\operatorname{Dual}(S(M_\infty)) &= \operatorname{Dual}(S(F_\infty))/(\gamma - 1)\operatorname{Dual}(S(F_\infty)) \\ &= \operatorname{Dual}(S(F_\infty)) \otimes_{\Lambda(F_\infty)} \Lambda(M_\infty).\end{aligned}$$

Now the corollary follows from Theorem 3.1 and Corollary 3.2.

Since $\Lambda(M_\infty) \simeq \mathcal{O}_p[[T]]$ in Corollary 3.3 we conclude immediately:

COROLLARY 3.4: *If $M_\infty = \bigcup_n M_n$ is any $\mathbb{Z}_p$-extension of $F$ in $F_\infty$ then either* $\lim_{n\to\infty} \operatorname{rank}_{\mathbb{Z}} E(M_n) = \infty$ *or* $\lim_{n\to\infty} \#(Ш(M_n)) = \infty$.

In §6 we give examples of both of these phenomena.

REMARK: It is tempting to try to strengthen the conclusions of Corollary 3.4 to say something about the rate of growth of $E(M_n)$ and $Ш(M_n)$. However, it is important to rmember that our results about $S(M_\infty)$ tell us nothing quantitative about $S(M_n)$, but rather about $S'(M_n)$. For example, if $\operatorname{corank}_{\Lambda(M_\infty)} E(M_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p > 0$ then $\operatorname{corank}_{\mathcal{O}_p}(E(M_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{G(M_\infty/M_n)} \geq [M_n: F]$, but this does *not* imply that $\operatorname{rank}_{\mathcal{O}} E(M_n) \geq [M_n: F]$ because $(E(M_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{G(M_\infty/M_n)}$ can be much larger than $E(M_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ (see §§5 and 6). Similarly if $\operatorname{corank}_{\Lambda(M_\infty)} Ш(M_\infty) > 0$

then $Ш(M_\infty)^{G(M_\infty/M_n)}$ will be infinite, but $Ш(M_n)$ can be much smaller than $Ш(M_\infty)^{G(M_\infty/M_n)}$. Corollary 3.4 seems to be all one can say a priori. For some partial results in these directions see Theorem 5.2 and Corollary 5.3.

§4. For any finite abelian Galois group $G$ let

$$\hat{G} = \left\{\text{characters } \chi\colon G \to \overline{K}_p^\times\right\}$$

and let $R = \mathcal{O}_p[\mu_{\#(G)}]$ and $k = K_p(\mu_{\#(G)})$. If $A$ is any $\mathcal{O}_p[G]$-module and $\chi \in \hat{G}$ define

$$A^\chi = \left\{a \in A \otimes_{\mathcal{O}_p} R\colon a^\sigma = \chi(\sigma)a \text{ for all } \sigma \in G\right\}.$$

Then one checks that

$$\#(G)A \otimes_{\mathcal{O}_p} R \subset \bigoplus_{\chi \in \hat{G}} A^\chi \subset A \otimes_{\mathcal{O}_p} R \tag{8}$$

so in particular

$$\sum_{\chi \in \hat{G}} \operatorname{rank}_R A^\chi = \operatorname{rank}_{\mathcal{O}_p} A. \tag{9}$$

For this section and §5 we suppose that $E$ is defined over $K$, and that $L$ is a finite abelian extension of $K$. We wish to investigate the difference between $S(L)$ and $S'(L)$. Our starting point will be the following theorem of Bashmakov (see also Cassels [2]).

THOEREM 4.1: [18]. *Suppose that* $Ш(L)$ *is finite. Then*

$$\operatorname{Dual}(S'(L)/S(L)) \simeq E_1(L \otimes_K K_p)/\overline{E_1(L)}$$

*where* $E_1(L \otimes_K K_p)$ *denotes the kernel of reduction modulo* $p$ *in* $E(L \otimes_K K_p)$ *and* $\overline{E_1(L)}$ *denotes the closure of* $E(L) \cap E_1(L \otimes_K K_p)$ *inside* $E_1(L \otimes_K K_p)$.

For the rest of this section write $G = G(L/K)$. If $\chi \in \hat{G}$ write $\bar{\chi}$ for $\chi^{-1}$. We will deduce from Theorem 4.1 the following.

THEOREM 4.2: *Suppose* $Ш(L)$ *is finite. If* $\chi \in \hat{G}$ *and* $\operatorname{rank}_R \operatorname{Dual}(S'(L))^\chi \geqslant 2$, *then*

$$\operatorname{rank}_R\left(E(L) \otimes \mathbb{Z}_p\right)^\chi = \operatorname{rank}_R \operatorname{Dual}(S(L))^{\bar{\chi}} = \operatorname{rank}_R \operatorname{Dual}(S'(L))^{\bar{\chi}}$$

To prove this theorem we need two lemmas.

LEMMA 4.3: *If $A$ is a finitely-generated $\mathcal{O}_p[G]$-module and $\chi \in \hat{G}$ then* $\operatorname{rank}_R A^{\bar{\chi}} = \operatorname{rank}_R \operatorname{Dual}(A \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{\chi}$.

PROOF: Since $\operatorname{rank}_{\mathcal{O}_p} A = \operatorname{rank}_{\mathcal{O}_p} \operatorname{Dual}(A \otimes \mathbb{Q}_p/\mathbb{Z}_p)$, by (9) it will suffice to show that for all $\chi \in \hat{G}$,

$$\operatorname{rank}_R A^{\bar{\chi}} \geqslant \operatorname{rank}_R \operatorname{Dual}\left(A \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)^{\chi}. \tag{10}$$

For each $\chi \in \hat{G}$ choose a free $R$-submodule $B_\chi$ of $A^\chi$ such that $\operatorname{rank}_R B_\chi = \operatorname{rank}_R A^\chi$, and set $B = \oplus_{\chi \in \hat{G}} B_\chi \subset A \otimes_{\mathcal{O}_p} R$. By (8), $B \otimes \mathbb{Q}_p = A \otimes_{\mathcal{O}_p} k$ so we get a surjective map

$$B \otimes \mathbb{Q}_p/\mathbb{Z}_p \to A \otimes_{\mathcal{O}_p} k/R$$

and a corresponding injection

$$\operatorname{Dual}\left(A \otimes \mathbb{Q}_p/\mathbb{Z}_p\right) \otimes_{\mathcal{O}_p} R = \operatorname{Dual}\left(A \otimes_{\mathcal{O}_p} k/R\right) \hookrightarrow \operatorname{Dual}\left(B \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)$$

$$= \bigoplus_{\chi} \operatorname{Dual}\left(B_\chi \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)$$

This map sends $\operatorname{Dual}(A \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\chi$ into $\operatorname{Dual}(B_{\bar{\chi}} \otimes \mathbb{Q}_p/\mathbb{Z}_p)$ so $\operatorname{rank}_R \operatorname{Dual}(A \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\chi \leqslant \operatorname{rank}_R \operatorname{Dual}(B_{\bar{\chi}} \otimes \mathbb{Q}_p/\mathbb{Z}_p) = \operatorname{rank}_R B_{\bar{\chi}} = \operatorname{rank}_R A^{\bar{\chi}}$.

REMARK: If $G$ is infinite then Lemma 4.3 is false. In §5 we will see examples (with $L/K$ infinite) where $\operatorname{rank}_R(E(L) \otimes \mathbb{Z}_p)^{\bar{\chi}} = 0$ but $\operatorname{rank}_R \operatorname{Dual}(E(L) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\chi > 0$.

LEMMA 4.4: *Fix $\chi \in \hat{G}$. If* $\operatorname{rank}_R(E(L) \otimes \mathbb{Z}_p)^\chi > 0$ *then* $\operatorname{rank}_R \overline{E_1(L)}^\chi > 0$ (*where $\overline{E_1(L)}$ is as defined in Theorem* 4.2).

PROOF: Suppose $\operatorname{rank}_R(E(L) \otimes \mathbb{Z}_p)^\chi > 0$, or equivalently $(E(L) \otimes \mathbb{Q}_p)^\chi \neq 0$. Fix an embedding of $\bar{K}$ into $\bar{K}_p$. Since the endomorphisms of $E(L) \otimes \mathbb{Q}$ induced by elements of $G$ are simultaneously diagonalizable over $\bar{K}$, we can in fact find a nonzero $v \in E(L) \otimes_{\mathcal{O}} \bar{K}$ with $v^\sigma = \chi(\sigma)v$ for all $\sigma \in G$. It follows from a theorem of Bertand [1] that the map

$$E(L) \otimes_{\mathcal{O}} \bar{K} \to E\left(L \otimes_K K_p\right) \otimes_{\mathcal{O}_p} \bar{K}_p$$

is injective (see also [15] Corollary 7.3); thus the image of $v$ is a nonzero element of $\overline{E_1(L)}^\chi \otimes_R \bar{K}_p$ and $\operatorname{rank}_R \overline{E_1(L)}^\chi > 0$.

PROOF OF THEOREM 4.2: We have

$$\operatorname{rank}_R \operatorname{Dual}(S(L))^{\chi} = \operatorname{rank}_R \operatorname{Dual}\big(E(L)\otimes \mathbb{Q}_p/\mathbb{Z}_p\big)^{\chi}$$

$$= \operatorname{rank}_R \big(E(L)\otimes \mathbb{Z}_p\big)^{\bar{\chi}} \tag{11}$$

where the first equality comes from (3) and our assumption that $Ш(L)$ is finite, and the second from Lemma 4.3 applied to $E(L)\otimes \mathbb{Z}_p$.

By a theorem of Lutz [11] $E(L\otimes_K K_p)$ has a subgroup of finite index which is isomorphic (as a $G$-module) to $\mathcal{O}_p[G]$. In particular, for each $\chi \in \hat{G}$

$$\operatorname{rank}_R \big(E_1(L\otimes_K K_p)/\overline{E_1(L)}\big)^{\chi} = 1 - \operatorname{rank}_R \overline{E_1(L)}^{\chi}.$$

Combining this with Theorem 4.1 yields

$$\operatorname{rank}_R \operatorname{Dual}(S'(L))^{\chi} = \operatorname{rank}_R \operatorname{Dual}(S(L))^{\chi} + 1 - \operatorname{rank}_R \overline{E_1(L)}^{\chi}. \tag{12}$$

Thus if $\operatorname{rank}_R \operatorname{Dual}(S'(L))^{\chi} \geqslant 2$, then $\operatorname{rank}_R \operatorname{Dual}(S(L))^{\chi} \geqslant 1$ so by (11) and Lemma 4.4 $\operatorname{rank}_R \overline{E_1(L)}^{\bar{\chi}} \geqslant 1$. Now (11) and (12) for the character $\bar{\chi}$ prove the theorem.

REMARK: Theorem 4.2 shows some of the difficulty in obtaining information about $S(L)$ from $S'(L)$ or from the $\Lambda(F_\infty)$-module $X$ to which $S'(L)$ is related by Proposition 1.2. For example in both of the two most common cases $\operatorname{rank}_{\mathcal{O}} E(K) = 0$ or 1 we have $\operatorname{corank}_{\mathcal{O}_p} S'(K) = 1$. Thus the Mordell-Weil group does not "appear" in $X$ unless $\operatorname{rank}_{\mathcal{O}} E(K) \geqslant 2$.

§5. We still suppose that $E$ is defined over $K$. Let $M_\infty = \bigcup_n M_n$ be any $\mathbb{Z}_p$-extension of $K$ inside $K(E_{p^\infty})$, with $[M_n : K] = p^n$. Write $\Lambda = \Lambda(M_\infty)$.

LEMMA 5.1: *If $\chi$ is a character of $G(M_n/K)$ then*

$$\operatorname{rank}_R \operatorname{Dual}(S'(M_n))^{\chi}$$

$$= \operatorname{rank}_R \big(\operatorname{Dual}(S'(M_\infty)) \otimes_\Lambda \mathcal{O}_p[G(M_n/K)]\big)^{\chi}.$$

PROOF: By Proposition 1.2,

$$\operatorname{rank}_R \operatorname{Dual}(S'(M_n))^{\chi} = \operatorname{rank}_R \operatorname{Dual}\big(S'(M_\infty)^{G(M_\infty/M_n)}\big)^{\chi}.$$

But if we write $\gamma$ for a topological generator of $G(M_\infty/M_n)$,

$$\begin{aligned}\mathrm{Dual}\big(S'(M_\infty)^{G(M_\infty/M_n)}\big) &\cong \mathrm{Dual}(S'(M_\infty))/(\gamma-1)\mathrm{Dual}(S'(M_\infty)) \\ &= \mathrm{Dual}(S'(M_\infty))\otimes_\Lambda \Lambda/(\gamma-1)\Lambda\end{aligned}$$

and $\Lambda/(\gamma-1)\Lambda \cong \mathcal{O}_p[G(M_n/K)]$.

THEOREM 5.2: *Let $M_\infty = \bigcup_n M_n$ be as above, and let $r = \mathrm{corank}_\Lambda S(M_\infty)$.*

(i) *There is an integer $N$ such that if $n > N$ and $\chi$ is a character of $G(M_\infty/K)$ of conductor $p^n$ then*

$$\mathrm{rank}_R\ \mathrm{Dual}(S(M_n))^\chi \leqslant r.$$

(ii) *Suppose $r \geqslant 2$. For any $n$ and any character $\chi$ of $G(M_n/K)$, if $Ш(M_n)$ is finite then*

$$\mathrm{rank}_R\ \mathrm{Dual}(S(M_n))^\chi = \mathrm{rank}_R\big(E(M_n)\otimes \mathbb{Z}_p\big)^{\bar\chi} \geqslant r.$$

PROOF: Since $\mathrm{Dual}(S(M_\infty)) = \mathrm{Dual}(S'(M_\infty))$ is a finitely generated (Corollary 3.3) $\Lambda$-module of rank $r$ we have an exact sequence

$$0 \to \Lambda^r \to \mathrm{Dual}(S'(M_\infty)) \to W \to 0 \tag{13}$$

with a finitely generated torsion $\Lambda$-module $W$. By the structure theorem for such modules, $\mathrm{rank}_{\mathcal{O}_p} W$ is finite.

For each $n$ define

$$Z_n = \big\{\chi\colon G(M_n/K) \to \bar K_p^\times : \mathrm{rank}_R\ \mathrm{Dual}(S(M_n))^\chi > r\big\}.$$

Then $Z_1 \subset Z_2 \subset \ldots$; to prove (i) we need only show that $\#(Z_n)$ is bounded independent of $n$.

From (13) we get the exact sequence

$$\begin{aligned}\big(\mathcal{O}_p[G(M_n/K)]\big)^r \to \mathrm{Dual}(S'(M_\infty))\otimes_\Lambda \mathcal{O}_p[G(M_n/K)] \\ \to W\otimes_\Lambda \mathcal{O}_p[G(M_n/K)]\end{aligned}$$

so taking eigenspaces and applying Lemma 5.1 we see

$$\mathrm{rank}_R\ \mathrm{Dual}(S'(M_n))^\chi \leqslant r + \mathrm{rank}_R\big(W\otimes_\Lambda \mathcal{O}_p[G(M_n/K)]\big)^\chi.$$

It follows that $\mathrm{rank}_R(W\otimes_\Lambda \mathcal{O}_p[G(M_n/K)])^\chi \geqslant 1$ for all $\chi \in Z_n$, so in particular using (9) we conclude

$$\#(Z_n) \leqslant \mathrm{rank}_{\mathcal{O}_p}\big(W\otimes_\Lambda \mathcal{O}_p[G(M_n/K)]\big) \leqslant \mathrm{rank}_{\mathcal{O}_p} W.$$

This proves (i).

It follows from the classification theorem for finitely generated $\Lambda$-modules that for any $n$, $\mathrm{Dual}(S'(M_\infty)) \otimes_\Lambda \mathcal{O}_p[G(M_n/K)]$ has a submodule isomorphic to $(\mathcal{O}_p[G(M_n/K)])^r$. Therefore for any character $\chi$ of $G(M_n/K)$,

$$\mathrm{rank}_R \, \mathrm{Dual}\big(S'(M_n)\big)^\chi \geqslant r$$

by Lemma 5.1. Now if $r \geqslant 2$ and $Ш(M_n)$ is finite we can apply theorem 4.2 to prove (ii).

COROLLARY 5.3: *Suppose* $Ш(M_n)$ *is finite for all* $n$. *Then* $\mathrm{corank}_\Lambda Ш(M_\infty) \leqslant 1$. *If* $\mathrm{corank}_\Lambda(E(M_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p) > 0$ *then* $\mathrm{corank}_\Lambda Ш(M_\infty) = 0$.

PROOF: Write $r = \mathrm{corank}_\Lambda S(M_\infty)$. If either assertion is false then $r \geqslant 2$ and we can apply theorem 5.2(ii) to conclude

$$\mathrm{corank}_{\mathcal{O}_p}\big(E(M_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p\big) \geqslant rp^n$$

for all $n$. It is not hard to show that the map

$$E(M_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow E(M_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

has finite kernel, so $\mathrm{corank}_{\mathcal{O}_p}(E(M_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^{G(M_\infty/M_n)} \geqslant rp^n$ for every $n$ as well. Appealing again to the classification theorem for finitely generated $\Lambda$-modules it follows that

$$\mathrm{corank}_\Lambda\big(E(M_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p\big) \geqslant r$$

so $\mathrm{corank}_\Lambda Ш(M_\infty) = 0$. This proves the corollary.

## §6. Examples and applications

For this section we take $E$ to be an elliptic curve over $\mathbb{Q}$ with complex multiplication by the imaginary quadratic field $K$, and $p$ an odd prime of good reduction which remains prime in $K$. We will study the behavior of $E$ in two special $\mathbb{Z}_p$-extensions of $K$--the cyclotomic $\mathbb{Z}_p$-extension $K_\infty^+ \subset K(\mu_{p^\infty})$ and the anticyclotomic $\mathbb{Z}_p$-extension $K_\infty^-$, which is the unique $\mathbb{Z}_p$-extension inside $K(E_\infty)$ such that $K_\infty^-$ is Galois over $\mathbb{Q}$ and $G(K/\mathbb{Q})$ acts nontrivially on $G(K_\infty^-/K)$.

### *I. Cyclotomic $\mathbb{Z}_p$-extension*

THEOREM 6.1: *With notation as above*,

$$\mathrm{corank}_{\Lambda(K_\infty^+)} E(K_\infty^+) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0 \quad \text{and} \quad \mathrm{corank}_{\Lambda(K_\infty^+)} Ш(K_\infty^+) \geqslant 1.$$

PROOF: The first equality follows from a result proved in some cases by Wiles and the author [16] and in general by Rohrlich [13], which states that $E(K_\infty^+)$ is finitely generated over $\mathbb{Z}$. The second assertion now follows from Corollary 3.3.

REMARK: Obviously one would have a similar result for any $\mathbb{Z}_p$-extension $M_\infty$ of $K$ such that $E(M_\infty)$ is finitely generated.

*II. Anticyclotomic $\mathbb{Z}_p$-extension*

It follows from recent work of Greenberg [7], Gross-Zagier [8] and Rohrlich [12] that $\operatorname{rank}_{\mathbb{Z}} E(K_\infty^-)$ is infinite. More precisely, let $w = \pm 1$ be the sign in the functional equation of the $L$-function of $E$ over $\mathbb{Q}$.

THEOREM 6.2: *If $n$ is sufficiently large and $\chi$: $G(K_\infty^-/K) \to \overline{K}_p^\times$ is a character of conductor $p^n$ then*

$$\text{(i)}\quad \operatorname{rank}_R\big(E(K_\infty^-)\otimes \mathbb{Z}_p\big)^\chi \geqslant 1 \qquad \text{if} \quad (-1)^n \neq w$$

$$\text{(ii)}\quad \operatorname{rank}_R\big(E(K_\infty^-)\otimes \mathbb{Z}_p\big)^\chi = 0 \qquad \text{if} \quad (-1)^n = w.$$

PROOF: [7], [8], [12] for (i) and [7], [12], [15] for (ii).

$$\text{Write } \Lambda = \Lambda(K_\infty^-) \quad \text{and} \quad K_\infty^- = \bigcup_n K_n^- .$$

COROLLARY 6.3: $\operatorname{corank}_\Lambda(E(K_\infty^-)\otimes \mathbb{Q}_p/\mathbb{Z}_p) \geqslant 1$. *If $Ш(K_n^-)$ is finite for all $n$, then* $\operatorname{corank}_\Lambda(E(K_\infty^-)\otimes \mathbb{Q}_p/\mathbb{Z}_p) = 1$ *and* $\operatorname{corank}_\Lambda Ш(K_\infty^-) = 0$.

PROOF: Since $\operatorname{rank}_{\mathbb{Z}} E(K_\infty^-)$ is infinite and $\operatorname{Dual}(E(K_\infty^-)\otimes \mathbb{Q}_p/\mathbb{Z}_p)$ is a finitely generated $\Lambda$-module, we have $\operatorname{corank}_\Lambda(E(K_\infty^-)\otimes \mathbb{Q}_p/\mathbb{Z}_p) \geqslant 1$. If $Ш(K_n^-)$ is finite for every $n$ and $\operatorname{corank}_\Lambda S(K_\infty^-) \geqslant 2$, then Theorem 5.2(ii) would contradict Theorem 6.2(ii), so we must have $\operatorname{corank}_\Lambda S(K_\infty^-) = 1$, and the second assertion now follows from the definition (3) of the Selmer group.

COROLLARY 6.4: *Suppose $Ш(K_n^-)$ is finite for all $n$. Then equality holds in Theorem 6.2(i): if $n$ is sufficiently large, $(-1)^n \neq w$ and $\chi$ is a character of conductor $p^n$ then*

$$\operatorname{rank}_R\big(E(K_\infty^-)\otimes \mathbb{Z}_p\big)^\chi = 1.$$

PROOF: If $\operatorname{rank}_R(E(K_n^-)\otimes \mathbb{Z}_p)^\chi > 1$ then Lemma 4.3 shows that $\operatorname{rank}_R \operatorname{Dual}(S(K_n^-))^{\bar\chi} > 1$. By Theorem 5.2(i) and Corollary 6.3, this cannot happen if the conductor of $\chi$ is sufficiently large. Now Theorem 6.2 completes the proof.

## References

[1] D. BERTRAND: Probèmes arithmétiques liés à l'exponentielle $p$-adique sur les courbes elliptiques. C.R. Acad. Sci. Paris Sér. A *282*, (1976) 1399–1401.
[2] J.W.S. CASSELS: Arithmetic on curves of genus 1 (VII). *J. Reine Angew. Math. 216* (1964) 150–158.
[3] J.W.S. CASSELS: Arithmetic on curves of genus 1 (VIII). *J. Reine Angew. Math. 217* (1965) 180–199.
[4] J. COATES: Infinite descent on elliptic curves with complex multiplication. In: *Progress in Math*. Vol. *35*, pp. 107–138 Boston: Birkhauser (1983).
[5] J. COATES and A. WILES: On the conjecture of Birch and Swinnerton-Dyer. Invent. Math. *39* (1977) 223–251.
[6] R. GREENBERG: On the structure of certain Galois groups. *Invent. math. 47* (1978) 85–99.
[7] R. GREENBERG: On the Birch and Swinnerton-Dyer conjecture. To appear.
[8] B. GROSS and D. ZAGIER: To appear.
[9] G. HOCHSCHILD and J.-P. SERRE: Cohomology of group extensions, *Trans. Amer. Math. Soc. 74* (1953) 110–134.
[10] G. KONOVALOV: The universal $G$-norms of formal groups over a local field. *Ukranian Math. J. 28* (1976) and 3 (1977) 310–311.
[11] E. LUTZ: Sur l'equation $y^2 = x^3 - Ax - B$ dans les corps $\mathfrak{p}$-adiques. *J. Reine Angew. Math. 177* (1977) 237–247.
[12] D. ROHRLICH: On $L$-functions of elliptic curves and anticyclotomic towers. To appear.
[13] D. ROHRLICH: On $L$-functions of elliptic curves and cyclotomic towers. To appear.
[14] K. RUBIN: On the arithmetic of CM elliptic curves in $\mathbb{Z}_p$-extensions. *Thesis*, Harvard University (1980).
[15] K. RUBIN Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-dyer. *Invent. Math. 64*, (1981) 455–470.
[16] K. RUBIN and A. WILES: Mordell-Weil groups of elliptic curves over cyclotomic fields. In: *Number Theory related to Fermat's last Theorem*. Boston: Birkhauser (1982).
[17] J. TATE: Duality theorems in Galois cohomology over number fields. *Proc. Internat. Congress Math. Stockholm* 1962, pp. 288–295.
[18] M. BASHMAKOV: The cohomology of abelian varieties over a number field, *Russian Math. Surveys 27* (1972) 25–70

(Oblatum 21-XI-1983)

Institute for Advanced Study
Princeton, NJ 08540
U.S.A.

*Current address*:
Department of Mathematics
The Ohio State University
Columbus, OH 43210
U.S.A.