JOURNAL OF NUMBER THEORY **64**, 276–290 (1997)
ARTICLE NO. NT972114

The Support Problem and Its Elliptic Analogue

Capi Corrales-Rodrigáñez*

Departamento de Algebra, Facultad de Ciencias Matemáticas, Universidad Complutense de Madrid, E-28040 Madrid, Spain

and

René Schoof†

Dipartimento di Matematica, 2ª Università di Roma "Tor Vergata," I-00133 Roma, Italy

Communicated by D. J. Lewis

Received June 28, 1995

Let F be a number field, Suppose $x, y \in F^*$ have the property that for all $n \in \mathbf{Z}$ and almost all prime ideals $\mathfrak{p}$ of the ring of integers of F^* one has that $y^n \equiv 1 \pmod{\mathfrak{p}}$ whenever $x^n \equiv 1 \pmod{\mathfrak{p}}$. We show that then y is a power of x. This answers a question of Erdős. We also prove an elliptic analogue of this result.

1. INTRODUCTION

At the 1988 number theory conference in Banff, Prof. Pál Erdős asked the following question:

QUESTION. *Let x and y be positive integers with the property that for all positive integers n the set of prime numbers dividing $x^n - 1$ is equal to the set of prime numbers dividing $y^n - 1$. Is then $x = y$?*

Writing $\mathrm{Supp}(m)$ for the "support" of a positive integer m, i.e. for the set of primes dividing m, we can also say that Erdős asked whether

$$\mathrm{Supp}(x^n - 1) = \mathrm{Supp}(y^n - 1) \qquad \text{for all} \quad n \in \mathbf{Z}_{>0} \Leftrightarrow x = y$$

In this paper we give an affirmative answer to Erdős's question. In Section 2 we prove the following result.

* E-mail: capi@sunal1.mat.ucm.es.
† E-mail: schoof@fwi.uva.nl.

0022-314X/97 $25.00

THEOREM 1. *Let F be a number field and let $x, y \in F^*$. If for almost all prime ideals $\mathfrak{p}$ of the ring of integers of F and for all positive integers n one has*

$$y^n \equiv 1 \pmod{\mathfrak{p}} \qquad \text{whenever} \quad x^n \equiv 1 \pmod{\mathfrak{p}},$$

then y is a power of x.

It is easy to see that it follows from Theorem 1 that if $y^n \equiv 1 \pmod{\mathfrak{p}}$ *if and only if* $x^n \equiv 1 \pmod{\mathfrak{p}}$, then either $x = y^{\pm 1}$ or both x and y are roots of unity. Applying this with $F = \mathbf{Q}$ and x and y two positive integers, one easily obtains an answer to Erdős's question. We thank H. W. Lenstra for catching an error in an earlier version of the proof. Theorem 1 has recently been generalized by A. Schinzel [4].

In Sections 3, 4, and 5 we prove the following result. It is an elliptic analogue of Theorem 1.

THEOREM 2. *Let F be a number field and let E be an elliptic curve over F. Suppose that P and Q are two F-rational points on E. If for every integer n and almost every prime ideal $\mathfrak{p}$ of the ring of integers of F, for which E has good reduction, one has that*

$$nQ = 0 \quad \text{in } E(\mathbf{F}_{\mathfrak{p}}) \qquad \text{whenever} \quad nP = 0 \quad \text{in } E(\mathbf{F}_{\mathfrak{p}}),$$

then either $Q = fP$ for some F-rational endomorphism f of E or both P and Q are torsion points.

Here a point or an endomorphism is called F-rational if it is defined over F and $E(\mathbf{F}_{\mathfrak{p}})$ denotes the group of points on E over the residue field $\mathbf{F}_{\mathfrak{p}}$ of the prime ideal $\mathfrak{p}$. As with Theorem 1, it is easy to see that if $nQ = 0$ in $E(\mathbf{F}_{\mathfrak{p}})$ *if and only if* $nP = 0$ in $E(\mathbf{F}_{\mathfrak{p}})$, then either $Q = fP$ for some F-rational automorphism of E or both P and Q are torsion points. In the latter case P and Q have the same order, because they do so modulo infinitely many prime ideals.

A straightforward generalization of Theorems 1 and 2 to other algebraic groups is false. It is, for instance, easy to see that it is false for the additive group $\mathbf{G}_a$ and hence for the groups GL_n when $n > 1$. It would be interesting to obtain an analogue of Theorem 2 for abelian varieties.

2. THE SUPPORT PROBLEM

In this section we prove Theorem 1. First we prove a lemma. For a positive integer n we let ζ_n denote a primitive nth root of unity and μ_n the group generated by ζ_n. As usual, we write i for ζ_4.

LEMMA 2.1. *Let F be a number field and let q be a power of a prime l. If $l=2$, assume that $i\in F$. Let σ denote a generator of the cyclic group $G_q=\mathrm{Gal}(F(\zeta_q)/F)$ and let $N_q\colon F(\zeta_q)^*\to F^*$ denote the norm map. Then the following holds.*

(i) *For $\zeta\in\mu_q$ we have that $N_q(\zeta)=1$ if and only if $\zeta=\sigma(\xi)/\xi$ for some $\xi\in\mu_q$.*

(ii) *The natural map*

$$F^*/F^{*q}\to F(\zeta_q)^*/F(\zeta_q)^{*q}$$

is injective.

Proof. (i) The Galois group G_q is isomorphic to a subgroup H of $(\mathbf{Z}/q\mathbf{Z})^*=\mathrm{Aut}(\mu_q)$ and, if $l=2$, it is contained in $\{x\in(\mathbf{Z}/q\mathbf{Z})^*\colon x\equiv 1 \pmod 4\}$. Therefore H is cyclic of order d, say. Let $a\in(\mathbf{Z}/q\mathbf{Z})^*$ denote a generator, let $B=\{x\in\mathbf{Z}/q\mathbf{Z}\colon (1+a+a^2+\cdots+a^{d-1})\,x\equiv 0\}$ and $Z=\{(1-a)\,x\colon x\in\mathbf{Z}/q\mathbf{Z}\}$. Then $Z\subset B$ and the homomorphism $\psi\colon B\to\{\zeta\in\mu_q\colon N_q(\zeta)=1\}$ given by $\psi(x)=\zeta_q^x$ induces an isomorphism

$$\psi\colon B/Z\xrightarrow{\cong}\{\zeta\in\mu_q\colon N_q(\zeta)=1\}/\{\sigma(\zeta)/\zeta\colon\sigma\in G_q\}.$$

Therefore it suffices to show that $B=Z$. We leave this elementary computation to the reader.

(ii) Suppose $t\in F^*$ is equal to s^q for some $s\in F(\zeta_q)$. Then $\sigma(s)^q=s^q$ so that $\sigma(s)/s$ is a qth rooth of unity which is annihilated by the norm N_q. By part (i) this implies that $\sigma(s)/s=\sigma(\xi)/\xi$ for some $\xi\in\mu_q$. Therefore $s\xi^{-1}\in F$. Since $t=s^q=(s\xi^{-1})^q$, the lemma follows.

Alternatively, one may observe that the kernel of the map is isomorphic to the cohomology group $H^1(G_q,\mu_q)$ which is isomorphic to $\hat{H}^{-1}(G_q,\mu_q)$ because G_q is cyclic. The latter group vanishes by part (i).

In order to stress both the similarities to and the differences with the proof in the elliptic case, the proof of Theorem 1 divided into three parts. The first part involves the application of a density theorem, the second part involves Kummer theory and in the third part the proof is completed. The last part is almost trivial here, but not so in the elliptic case.

Proof of Theorem 1. Without loss of generality, we may assume that $i\in F$. Let T be a finite set of prime ideals of F containing the infinite primes, those that occur in the factorizations of x and y and those for which the conditions of the theorem do not hold.

Step 1. Let q be a power of a prime number l. Consider the number fields $F(\zeta_q,\sqrt[q]{x})$ and $F(\zeta_q,\sqrt[q]{y})$ inside a fixed algebraic closure $\bar{F}$ of F. Let $\mathfrak{p}$ be a prime ideal of F which is not T. Let p denote the number of elements

in its residue field $\mathbf{F}_\mathfrak{p}$. Suppose that $\mathfrak{p}$ is completely split in $F(\zeta_q, \sqrt[q]{x})$. This means that $p \equiv 1 \pmod q$ and that x is an qth power in $\mathbf{F}_\mathfrak{p}$. This implies that $x^{(p-1)/q} \equiv 1 \pmod \mathfrak{p}$ and therefore $y^{(p-1)/q} \equiv 1 \pmod \mathfrak{p}$. Since the multiplicative group $\mathbf{F}_\mathfrak{p}^*$ is cyclic, this, in turn, means that y is an qth power modulo $\mathfrak{p}$ and hence that $\mathfrak{p}$ is completely split in $F(\zeta_q, \sqrt[q]{y})$.

By the Frobenius Density Theorem [2, p. 136] we conclude that

$$F(\zeta_q, \sqrt[q]{y}) \subset F(\zeta_q, \sqrt[q]{x}).$$

Step 2. Let again q be a power of a prime number l and consider the well known map from Kummer theory

$$\theta: F(\zeta_q)^*/F(\zeta_q)^{*q} \to \mathrm{Hom}(\mathrm{Gal}(\bar{F}/F(\zeta_q)), \mu_q),$$

given by $\theta(t) = \varphi_t$ where $\varphi_t(\sigma) = \sigma(\sqrt[q]{t})/\sqrt[q]{t}$ for $\sigma \in \mathrm{Gal}(\bar{F}/F(\zeta_q))$. Since $F(\zeta_q, \sqrt[q]{y}) \subset F(\zeta_q, \sqrt[q]{x})$, we have that $\ker(\varphi_x) \subset \ker(\varphi_y)$. There is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker(\varphi_x) & \longrightarrow & \mathrm{Gal}(\bar{F}/F(\zeta_q)) & \xrightarrow{\varphi_x} & \mathrm{im}(\varphi_x) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \subset} & & \| & & \downarrow{\scriptstyle \psi} & & \\ 0 & \longrightarrow & \ker(\varphi_y) & \longrightarrow & \mathrm{Gal}(\bar{F}/F(\zeta_q)) & \xrightarrow{\varphi_y} & \mathrm{im}(\varphi_y) & \longrightarrow & 0 \end{array}$$

Since the group $\mathrm{im}(\varphi_x) \subset \mu_q$ is cyclic, the map ψ is simply exponentiation by an integer d and hence $\varphi_y = \varphi_x^d$. Since the map θ is injective, this implies that $y = x^d$ in the group $F(\zeta_q)^*/F(\zeta_q)^{*q}$. By Lemma 2.1 we conclude that $y = x^d$ in the group F^*/F^{*q}.

Step 3. Let O_T^* denote the multiplicative group of T-units and put $A = O_T^*/x^{\mathbf{Z}}$. We have shown that the image of y in the group A is in A^q for every prime power q. By Dirichlet's Unit Theorem, the group A is finitely generated and therefore $\bigcap_q A^q$ is trivial. We conclude that the image of y in A is trivial, i.e.

$$y = x^a$$

for some $a \in \mathbf{Z}$.

This proves Theorem 1.

3. THE ELLIPTIC ANALOGUE

The proof of Theorem 2 runs along the same lines as the proof of Theorem 1, but there are three complications, one in each step:

In step 1 the analogue of the multiplicative group $\mathbf{F}_{\mathfrak{p}}^*$ is the group $E(\mathbf{F}_{\mathfrak{p}})$ of points on the elliptic curve E modulo $\mathfrak{p}$. This group is, in general, *not* a cyclic group and we cannot simply copy the proof of Section 2. We restrict our attention to the primes $\mathfrak{p}$ for which the l-part of $E(\mathbf{E}_{\mathfrak{p}})$ is cyclic and use a group theoretical argument.

In step 2 the group $E[q]$, analogue of the group of qth roots of unity, is not cyclic either. Therefore the map "ψ" in the diagram is, a priori, not simply an integer. We show that ψ is compatible with the action of the Galois group. This severely restricts the possibilities for ψ. Since, for several reasons, we cannot work with *all* prime powers q, we cannot prove anymore in step 3 that the analogue of the intersection $\bigcap_q A^q$ is trivial, but only that it is *finite*. This step is completed by an application of Siegel's Theorem on integral points on curves of genus 1.

The details of the proofs are rather different depending on whether the elliptic curve E admits complex multiplication (CM) or not. In this section we introduce some notations and make a reduction that is useful in both cases. In Section 4 we prove Theorem 2 for elliptic curves E without complex multiplication. In Section 5 we deal with the complex multiplication case. See Silverman's book [3] for the basic properties of elliptic curves.

Let E be an elliptic curve over an algebraic number field F and let l be a prime. Let $E[l]$ denote the subgroup of points of $E(\bar{F})$ that are annihilated by l. It is a vector space of dimension 2 over $\mathbf{F}_l$ and it admits a natural action by the Galois group $\mathrm{Gal}(\bar{F}/F)$. Let F_l denote the field $F(E[l])$. This is a Galois extension of F and we put $G = \mathrm{Gal}(F_l/F)$. From the Galois cohomology sequences associated to the exact "Kummer" sequence

$$0 \longrightarrow E[l] \longrightarrow E(\bar{F}) \xrightarrow{l} E(\bar{F}) \longrightarrow 0$$

we obtain the following commutative diagram with exact rows and columns:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \ker & \longrightarrow & E(F)/lE(F) & \longrightarrow & E(F_l)/lE(E_l) \\
 & & \downarrow & & \downarrow & & \downarrow \theta \\
0 & \longrightarrow & H^1(G, E[l]) & \longrightarrow & H^1(\mathrm{Gal}(\bar{F}/F), E[l]) & \xrightarrow{\mathrm{Res}} & H^1(\mathrm{Gal}(\bar{F}/F_l), E[l])
\end{array}$$

The map θ is defined by $\theta(R) = \varphi_R$ where

$$\varphi_R(\sigma) = \sigma\left(\frac{1}{l}R\right) - \frac{1}{l}R \qquad \text{for} \quad \sigma \in \mathrm{Gal}(\bar{F}/F_l).$$

It is an injective map. The cohomology group $H^1(\mathrm{Gal}(\bar{F}/F_l), E[l])$ is canonically isomorphic to $\mathrm{Hom}(\mathrm{Gal}(\bar{F}/F_l), E[l])$. The image of

$$H^1(\mathrm{Gal}(\bar{F}/F), E[l]) \xrightarrow{\mathrm{Res}} H^1(\mathrm{Gal}(\bar{F}/F_l), E[l])$$

is G-invariant; it consists of G-homomorphisms, i.e., of homomorphims $\varphi: \mathrm{Gal}(\bar{F}/F_l) \to E[l]$ that satisfy

$$\varphi(\tau\sigma\tau^{-1}) = \tau(\varphi(\sigma)) \qquad \text{for every} \quad \tau \in \mathrm{Gal}(\bar{F}/F).$$

The following lemma is useful in the proof in both the CM and the non-CM case. It allows us to assume that the points P and Q each have infinite order.

LEMMA 3.1. *Suppose $P, Q \in E(F)$ are two points satisfying the conditions of Theorem 2 and that $Q \neq 0$. Then the point P has finite order if and only if Q has finite order. If this is the case, the order of Q divides the order of P.*

Proof. Suppose that for some integer $m \geqslant 1$, we have $mP = 0$ in the group $E(F)$. This implies that $mQ = 0$ in $E(\mathbf{F}_\mathfrak{p})$ for almost all primes $\mathfrak{p}$ and that is only possible when $mQ = 0$ as well. Therefore Q is a torsion point if P is. Moreover, the order of Q divides the order of P.

Conversely, suppose that $mQ = 0$ for some integer $m > 1$, then $Q = 0$ modulo $\mathfrak{p}$ at most for the primes $\mathfrak{p}$ of good reduction that divide m. This implies that the set

$$\{kP : k \equiv 1 \pmod{m}\}$$

contains only T-integral points for some finite set T of primes of F. By Siegel's Theorem on integral points [3, p. 247] there are only finitely many such points. This implies that P is a torsion point. This proves the lemma.

4. E HAS NO COMPLEX MULTIPLICATION

The proof of Theorem 2 is presented in three steps, each similar to the corresponding step in the proof of Theorem 1. First we prove an analogue of Lemma 2.1.

LEMMA 4.1. *Let l be a prime number for which the Galois group $G = \mathrm{Gal}(F_l/F)$ is isomorphic to $\mathrm{GL}_2(\mathbf{F}_l)$.*

(i) *Then*

$$H^q(G, E[l]) = 0 \qquad \text{for all} \quad q \geqslant 0,$$

and the natural map

$$E(F)/lE(F) \to E(F_l)/lE(F_l)$$

is injective

(ii) *If* $R \in E(F)$ *is a point not contained in* $lE(F)$, *then the map*

$$\varphi_R : \mathrm{Gal}(\bar{F}/F_l) \to E[l],$$

defined above, is surjective.

Proof. (i) Clearly $H^0(G, E[l]) = 0$. An application of Proposition 3 of [1, p. 99] with $t = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{F}_l)$ shows that $H^q(G, E[l])$ is annihilated by 2. This implies that for $l > 2$, the cohomology groups $H^q(G, E[l])$ vanish for all $q > 0$. When $l = 2$ the group $\mathrm{GL}_2(\mathbf{F}_l)$ is isomorphic to the permutation group S_3 and the result follows from a short computation. Since we do not need it, we leave this spcial case to the reader. By the diagram above, the kernel of the map $E(F)/lE(F) \to E(F_l)/lE(F_l)$ is contained in $H^1(G, E[l])$. Therefore it is trivial.

(ii) The image of φ_R is a G-submodule of $E[l]$. Since $R \notin lE(F)$, the image is not trivial. Since $E[l]$ is an irreducible G-module, it is therefore equal to $E[l]$, as required.

This proves the lemma.

Now we prove Theorem 2. Let P and Q be two points satsifying the conditions of Theorem 2. Since the theorem is trivially true when $Q = 0$, we assume that $Q \neq 0$. By Lemma 3.1 we may even assume that both points have infinite order in the group $E(F)$. The Mordell–Weil Theorem says that $E(F)$ is finitely generated. Therefore $P, Q \in lE(F)$ for only finitely many primes l. By a Theorem of Serre's [5, Thm. 2], the group $G = \mathrm{Gal}(F_l/F)$ is isomorphic to $\mathrm{GL}_2(\mathbf{F}_l)$ for all but finitely many l. Let S be a finite set of primes l containing $l = 2$, the primes for which G is not isomorphic to $\mathrm{GL}_2(\mathbf{F}_l)$ and the primes for which P or Q is contained in $lE(F)$.

Step 1. First we prove an easy group theoretical lemma.

LEMMA 4.2. *Let* l *be a prime and let* G *be a non-trivial subgroup of* $\mathrm{GL}_2(\mathbf{F}_l)$. *Let* H_1 *and* H_2 *be two 2-dimensional* $\mathbf{F}_l$*-vector spaces viewed as* G*-modules via the natural action of* G. *Let* Ω *denote the semidirect product of* G *by* $H_1 \times H_2$. *Let* $\sigma \neq 1$ *be in* G. *If for every* $h_1 \in H_1$ *the element* $(h_1, \sigma) \in H_1 \times G \subset \Omega$ *is conjugate to an element* $(h_2, \tau) \in H_2 \times G$, *then* $\sigma - 1$ *is invertible.*

Proof. Let $(h_1, \sigma) \in H_1 \times G$ and let $(h', \rho) \in \Omega$. Then

$$(h', \rho)(h_1, \sigma)(h', \rho)^{-1} = (\sigma h' + h_1, \rho\sigma)(-\rho^{-1}h', \rho^{-1}),$$
$$= (\rho^{-1}(h_1 + (\sigma - 1)\, h'), \rho\sigma\rho^{-1}).$$

The condition of the lemma implies therefore that for every $h_1 \in H_1$, there exists $h' \in H_1 \times H_2$ such that $h_1 + (\sigma - 1)\, h' \in H_2$. This implies that $H_1 \subset (\sigma - 1)(H_1 \times H_2) + H_2$ and therefore that $H_1 + H_2 \subset (\sigma - 1)\, H_1 + H_2$. We conclude that $\sigma - 1$ is surjective, as required.

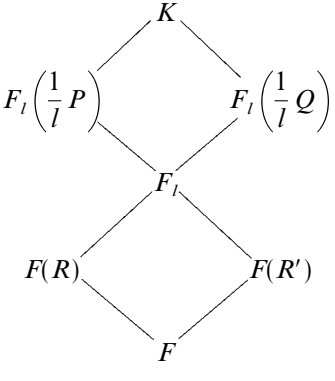
Let l be a prime not in S. Then the map φ_P is surjective and induces a G-isomorphism of $E[l]$ with $\mathrm{Gal}(F_l((1/l)\, P)/F_l)$. Here $F_l((1/l)\, P)$ denotes the extension of F_l obtained by adjoining the coordinates of one point R, or, equivalently, all points $R \in E(\bar{F})$ with $lR = P$. The Galois group of $F((1/l)\, P)$ over F is a semidirect produt of $\mathrm{Gal}(F_l((1/l)\, P)/F(R)) \cong G$ by $\mathrm{Gal}(F_l(1/l)\, P)/F_l) \cong E[l]$.

Similarly, φ_Q is surjective and induces a G-isomorphism of $\mathrm{Gal}(F_l((1/l)\, Q)/\bar{F}_l)$ with $E[l]$. The Galois group of $F((1/l)\, Q)$ over F is a semidirect product of the Galois group $\mathrm{Gal}(F_l((1/l)\, Q)/F(R')) \cong G$ by $\mathrm{Gal}(F_l((1/l)\, Q)/F_l) \cong E[l]$. Here $R' \in E(\bar{F})$ is a point satisfying $lR' = Q$.

Step 1. We claim that

$$F_l\left(\frac{1}{l}P\right) = F_l\left(\frac{1}{l}Q\right).$$

Proof. Suppose this is false. Let $K = F_l((1/l)\, P, (1/l)\, Q)$. Since $E[l]$ admits no proper G-submodules, the Galois group $V = \mathrm{Gal}(K/F_l)$ is a direct product of $H_2 = \mathrm{Gal}(K/F_l((1/l)\, Q)) \cong \mathrm{Gal}(F_l((1/l)\, P)/F_l)$ and $H_1 = \mathrm{Gal}(K/F_l((1/l)\, P)) \cong \mathrm{Gal}(F_l((1/l)\, Q)/F_l)$. The Galois group $\Omega = \mathrm{Gal}(K/F)$ is a semi-direct product of G by $H_1 \times H_2$.



We verify that the conditions of Lemma 4.2 are satisfied: Let $\sigma \neq 1$ and let (h, σ) be in the subgroup $H_1 \times G = \mathrm{Gal}(K/F(R)) \subset \Omega$. Let $\mathfrak{p}$ be a prime ideal

of degree 1 of F which satisfies the hypothesis of the theorem over which there is a prime $\mathfrak{P}$ in K whose Frobenius automorphism is equal to (h, σ). This means that $\mathfrak{p}$ splits completely in the subfield $F(R)$, but does not split in F_l. This implies that the l-part of the group of points $E(\mathbf{F}_\mathfrak{p})$ is cyclic and that one has $P = lR$ in $E(\mathbf{F}_\mathfrak{p})$. Let m denote the cardinality of $E(\mathbf{F}_\mathfrak{p})$. Then m/l kills P and therefore, by the assumptions of the theorem, m/l kills Q in $E(\mathbf{F}_\mathfrak{p})$. Since the l-part of $E(\mathbf{F}_\mathfrak{p})$ is cyclic, this implies that $Q = lR''$ for some point R'' in $E(\mathbf{F}_\mathfrak{p})$. Since G acts transitively on $E[l]$, this means that the Frobenius automorphism of $\mathfrak{P}$ is *conjugate* to an element of the form (h', τ) with $h' \in H_2$. This shows that the conditions of the lemma are satisfied.

Since G is all of $\mathrm{GL}_2(\mathbf{F}_l)$, the conclusion of the lemma that $\sigma - 1$ is invertible for all non-trivial $\sigma \in G$, is absurd and therefore $F_l((1/l)\,P) = F_l((1/l)\,Q)$, as required

Step 2. Since $F_l((1/l)\,P) = F_l((1/l)\,Q)$, the kernels of φ_P and φ_Q are equal. Therefore there is a unique homomorphism $\psi: E[l] \to E[l]$ making the following diagram commutative:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker(\varphi_P) & \longrightarrow & \mathrm{Gal}(\bar{F}/F_l) & \xrightarrow{\varphi_P} & E[l] & \longrightarrow & 0 \\ & & \| & & \| & & \downarrow{\scriptstyle \psi} & & \\ 0 & \longrightarrow & \ker(\varphi_Q) & \longrightarrow & \mathrm{Gal}(\bar{F}/F_l) & \xrightarrow{\varphi_Q} & E[l] & \longrightarrow & 0 \end{array}$$

The maps φ_P, φ_Q, and therefore ψ, are G-homomorphisms. Since $G = \mathrm{GL}_2(\mathbf{F}_l)$, this implies that ψ is simply multiplication by a scalar $d \in \mathbf{F}_l^*$.

Therefore $\varphi_Q = d \cdot \varphi_P$ and hence, by the injectivity of θ we have $Q = dP$ in the group $E(F_l)/lE(F_l)$. By Lemma 4.1(i) we also have $Q = dP$ in the group $E(F)/lE(F)$.

Step 3. We have shown that the image of Q in the group $A = E(F)/\{kP: k \in \mathbf{Z}\}$ is contained in lA for all primes $l \notin S$. By the Mordell–Weil theorem the group A is finitely generated and we see that $\bigcap_{l \notin S} lA$ is finite. This implies that

$$bQ = aP \qquad \text{for some non-zero integers } a, b \in \mathbf{Z}.$$

We claim that b divides a: let L be the extension of F obtained by adjoining $E[ab]$, the points on E that are annihilated by ab. Let $R \in E[b]$. The set of points

$$\{R - kP: k \in \mathbf{Z}\}$$

is infinite. By Siegel's Theorem [3, p. 247] on integral points on curves of genus 1, there are infinitely many prime ideals $\mathfrak{P}$ of L such that $R \equiv kP$

modulo $\mathfrak{P}$ for some $k \in \mathbf{Z}$. For such a prime $\mathfrak{P}$ we have that $bkP = 0$ in the group $E(\mathbf{F}_{\mathfrak{p}})$ where $\mathfrak{p}$ is the prime of F over which $\mathfrak{P}$ lies. Therefore

$$bkQ = akP = 0 \qquad \text{in } E(\mathbf{F}_{\mathfrak{p}}),$$

and hence R is contained in $E[a]$ modulo $\mathfrak{P}$. Since this is so for infinitely many prime ideals $\mathfrak{P}$, we have that $R \in E[a]$. Since R was an arbitrary point in $E[b]$, we have shown that $E[b] \subset E[a]$ and hence that b divides a, as required.

We have

$$bQ = bfP \qquad \text{for some} \quad f \in \mathbf{Z}.$$

This implies that $Q = fP + R$ for some $R \in E(F)$ with $bR = 0$. Let m denote the order of R. For all $k \equiv 1 \pmod{m}$ and almost all prime ideals $\mathfrak{p}$ we have

$$kP = 0 \Rightarrow kQ = 0 \Rightarrow kR = R = 0 \qquad \text{in } E(\mathbf{F}_{\mathfrak{p}}).$$

If $m \neq 1$, the points in the set

$$\{kP : k \equiv 1 \pmod{m}\}$$

are all integral outside a finite set T of primes containing the primes for which $R \equiv 0$ in $E(\mathbf{F}_{\mathfrak{p}})$. Another application of Siegel's theorem shows that P has finite order. This is not so and therefore $m = 1$ and $Q = fP$, as required.

5. E ADMITS COMPLEX MULTIPLICATION

In this section we prove Theorem 2 for elliptic curves with complex multiplication. We use the same notation as in Section 3. By Lemma 3.1 we many assume that P and Q are both of infinite order. We will also assume that all $\bar{F}$-endomorphisms of E are already defined over F. This can be accomplished by an extension of F of degree at most 2.

We can do this without loss of generality, for if $P, Q \in E(F)$ are points with $Q = fP$ for some $\bar{F}$-endomorphism f of E, then also $Q = f^{\sigma}P$ where $\sigma \in \mathrm{Gal}(\bar{F}/F)$. Subtracting these relations gives that $(f - f^{\sigma})P = 0$. Since P is not a torsion point, this implies that $f = f^{\sigma}$. This shows that f is an F-endomorphism.

Let O denote the ring of $\bar{F}$-endomorphisms of E and let k denote its quotient field. The ring O is an order in the imaginary quadratic number field k. Let $O_{\max}$ denote the ring of integers of k. The ring O is a subring of finite index in $O_{\max}$. Since all endomorphisms of E are defined over F,

the field F contains a subfield isomorphic to k. Moreover, it contains a subfield H, isomorphic to the ring class field of k of conductor $[O_{\max}: O]$. The group $E(F)$ is an O-module. See [3].

We have the following analogue of Lemma 2.1.

LEMMA 5.1. *Let l be a prime number which is split in k does not divide the index $[O_{\max}: O]$.*

(i) *The image of $G = \mathrm{Gal}(F_l/F)$ in $\mathrm{Aut}(E[l])$ is isomorphic to a subgroup of the form*

$$\left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} : \lambda, \mu \in \mathbf{F}_l^* \right\} \subset \mathrm{GL}_2(\mathbf{F}_l).$$

Moreover, if l is sufficiently large, the group G contains matrices of the form $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \mu \end{smallmatrix}\right)$ for some $\lambda, \mu \in \mathbf{F}_l^*$, $\lambda, \mu \neq 1$.

(ii) *The natural map*

$$E(F)/lE(F) \to E(F_l)/lE(F_l)$$

is injective.

(iii) *Let $R \in E(F)$. If l does not divide $\#E(F)_{\mathrm{tors}}$ and if $R \notin \mathfrak{l}E(F)$ for any prime ideal $\mathfrak{l}$ of O over l, then the map*

$$\varphi_R: \mathrm{Gal}(\bar{F}/F_l) \to E[l]$$

defined in Section 3, is surjective.

Proof. Since l is split in k and does not divide the index $[O_{\max}: O]$ we can write $l = \mathfrak{l}_1 \mathfrak{l}_2$ as a product of distinct prime ideals $\mathfrak{l}_1, \mathfrak{l}_2$ of O.

(i) We have that $E[l] = E[\mathfrak{l}_1] \times E[\mathfrak{l}_2]$ as Galois modules, so that the field F_l is generated by the fields $F_{\mathfrak{l}_1} = F(E[\mathfrak{l}_1])$ and $F_{\mathfrak{l}_2} = F(E[\mathfrak{l}_2])$. Since the endomorphisms of E are defined over F, both $F_{\mathfrak{l}_1}$ and $F_{\mathfrak{l}_2}$ are Galois extensions of F. Therefore, with a suitable choice of basis, the image of the canonical map

$$\mathrm{Gal}(F_l/F) \to \mathrm{GL}(E[l])$$

is contained in the subgroup $\left\{ \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right) : \lambda, \mu \in \mathbf{F}_l^* \right\}$.

To prove the second statement, it suffices to show that for sufficiently large l the fields $F_{\mathfrak{l}_1}$ and $F_{\mathfrak{l}_2}$ are not contained in one another. Suppose therefore that $F_{\mathfrak{l}_1} \subset F_{\mathfrak{l}_2}$. Then $\zeta_l \in F_l = F_{\mathfrak{l}_2}$. If l is such that all primes of F over l are primes of good reduction, then $F_{\mathfrak{l}_2}$ is unramified at the primes

over $\mathfrak{l}_1$. However, if l is large enough, then $\zeta_l \notin F$ and the extension $F_{\mathfrak{l}_2}$ is ramified at all primes over l, including those over $\mathfrak{l}_1$. This proves (i).

(ii) The group G has order prime to l. Therefore $H^1(G, E[l]) = 0$ and the map

$$E(F)/lE(F) \to E(F_l)/lE(F_l)$$

is injective.

(iii) Suppose φ_R is not surjective. Since the image of φ_R in $E[l]$ is a G-submodule, it is contained in a proper submodule. The proper submodules of $E[l]$ are $E[\mathfrak{l}_1]$ and $E[\mathfrak{l}_2]$. Suppose, for instance, that the image of φ_R is contained in $E[\mathfrak{l}_1]$. This implies that $\mathfrak{l}_1 P \subset lE(F)$ and, since l does not divide $\# E(F)_{\text{tors}}$, that $R \in \mathfrak{l}_2 E(F)$.

This proves the lemma.

Since the group $E(F)$ is finitely generated and since P and Q have infinite order, there are only finitely many primes l such that $P, Q \in \mathfrak{l}E(F)$ for some prime ideal $\mathfrak{l}$ of O over l. Moreover, there are only finitely many prime numbers l that divide the index $[O_{\max}: O]$ or $\# E(F)_{\text{tors}}$ and almost all primes are sufficiently large in the sense of (i). In other words, there are only finitely many prime numbers l for which the conditions (i) and (iii) of Lemma 5.1 are not satisfied.

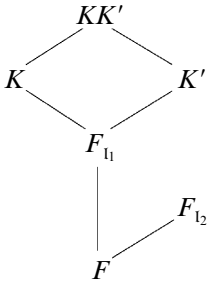
Let S be a finite set containing these exceptional prime numbers. Let $l \notin S$ be a prime which is completely split in F. Since $k \subset H \subset F$, it is also split in k and in the ring class field H of conductor $[O_{\max}: O]$. Therefore l splits in O as a product of two distinct principal prime ideals $\mathfrak{l}_1 = (\pi_1)$ and $\mathfrak{l}_2 = (\pi_2)$.

Step 1. We claim that

$$F_l\left(\frac{1}{l} P\right) = F_l\left(\frac{1}{l} Q\right).$$

By Lemma 5.1(i) we have that $F_{\mathfrak{l}_1} = F(E[\mathfrak{l}_1])$ and $F_{\mathfrak{l}_2} = F(E[\mathfrak{l}_2])$ are non-trivial extensions of F, satisfying $F_{\mathfrak{l}_2} \not\subset F_{\mathfrak{l}_1}$. The field $F_l((1/l) P)$ is generated by the Galois extensions $F_{\mathfrak{l}_1}((1/\pi_1) P)$ and $F_{\mathfrak{l}_2}((1/\pi_2) P)$ and, similarly, $F_l((1/l) Q)$ is generated by $F_{\mathfrak{l}_1}((1/\pi_1) Q)$ and $F_{\mathfrak{l}_2}((1/\pi_2) Q)$. Therefore it suffices to show that $F_{\mathfrak{l}_1}((1/\pi_1) P) = F_{\mathfrak{l}_1}((1/\pi_1) Q)$ and $F_{\mathfrak{l}_2}((1/\pi_2) P) = F_{\mathfrak{l}_2}((1/\pi_2) Q)$.

Let $K = F_{\mathfrak{l}_1}((1/\pi_1) P)$ and $K' = F_{\mathfrak{l}_1}((1/\pi_1) Q)$ and suppose that $K \neq K'$. By Lemma 5.1(iii), the groups $H = \text{Gal}(KK'/K') \cong \text{Gal}(K/F_{\mathfrak{l}_1})$ and $H' = \text{Gal}(KK'/K) \cong \text{Gal}(K'/F_{\mathfrak{l}_1})$ are cyclic of order l. By the assumptions on l, the intersection $H \cap H'$ is trivial.



Let $h \in H'$ be a non-trivial element. Let $\mathfrak{p}$ be a prime of F satisfying the hypothesis of the theorem and which is of degree 1, does not divide $[O_{\max}: O]$, does not split completely in F_{l_2} and such that the Frobenius automorphism of some prime $\mathfrak{P}$ of KK' over $\mathfrak{p}$ is equal to h. We can find such a prime ideal $\mathfrak{p}$ by Cebotarev's Density Theorem, because $F_{l_2} \not\subset F_{l_1}$ and the F_{l_1}-automorphisms of KK' commute with those of $F_{l_2}F_{l_1}$.

Since the prime $\mathfrak{p}$ is completely split in K, we have that $P = \pi_1 R$ for some point R in the group $E(\mathbf{F}_\mathfrak{p})$. Since $\mathfrak{p}$ is *not* split in F_{l_2}, it is not split in F_l and the l-part of the group $E(\mathbf{F}_\mathfrak{p})$ is equal to the group $E(\overline{\mathbf{F}_p})[\pi_1^a]$ for some $a > 0$. This group is cyclic. Let $m = \#E(\mathbf{F}_\mathfrak{p})$. We have that $(m/l)P = 0$ and therefore, by assumption, $(m/l)Q = 0$ which in turn implies that $Q = \pi_1 R'$ for some point $R' \in E(\mathbf{F}_\mathfrak{p})$. Therefore the Frobenius automorphism of $\mathfrak{P}$ is contained in H. This implies that $h \in H$, contradicting the fact that $H \cap H'$ is trivial.

Therefore $K = K'$ and this completes the proof of our claim.

Step 2. As in the proof of the case without complex multiplication, we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Ker}(\varphi_P) & \longrightarrow & \mathrm{Gal}(\bar{F}/F_l) & \xrightarrow{\varphi_P} & E[l] & \longrightarrow & 0 \\ & & & & & & \downarrow \psi & & \\ 0 & \longrightarrow & \ker(\varphi_Q) & \longrightarrow & \mathrm{Gal}(\bar{F}/F_l) & \xrightarrow{\varphi_Q} & E[l] & \longrightarrow & 0 \end{array}$$

Again, all maps are G-homomorphisms. In contrast to the non-CM case, this time G is not all of $\mathrm{GL}_2(\mathbf{F}_l)$. By Lemma 5.1(i), the group $E[l]$ is the product of the two non-isomorphic G-modules $E[\mathfrak{l}_1]$ and $E[\mathfrak{l}_2]$, so that

$$\psi = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$$

for some $\lambda, \mu \in \mathbf{F}_l^*$. Therefore $\varphi_Q = f \cdot \varphi_P$ for some endomorphism $f \in O$ which is congruent to $\lambda \pmod{\mathfrak{l}_1}$ and congruent to $\mu \pmod{\mathfrak{l}_2}$. Since

all endomorphisms in Q are defined over F, the map θ is an injective O-morphism and we conclude that in the group $E(F_l)/lE(F_l)$ we have that $Q = fP$ for some $f \in O$. By Lemma 5.1(ii) the equality $Q = fP$ holds in the group $E(F)/lE(F)$ as well.

Step 3. We have shown that the image of Q in the O-module $A = E(F)/\{fP : f \in O\}$ is contained in lA for all primes l not in S, that are split in F. There are infinitely many such primes. By the Mordell–Weil theorem the group A is finitely generated and we conclude that

$$\bigcap_{\substack{l \text{ split in } F \\ l \notin S}} lA$$

is finite. Therefore $bQ = gP$ for some integer $b \neq 0$ and some non-zero endomorphism $g \in O$.

Let L be the extension of F obtained by adjoining the points in $E[bg]$ and let $R \in E[b]$. The set of points

$$\{R - kP : k \in \mathbf{Z}\}$$

is infinite. By Siegel's Theorem on integral points on curves of genus 1, there are infinitely many prime ideals $\mathfrak{P}$ of L such that $R \equiv kP$ modulo $\mathfrak{P}$ for some $k \in \mathbf{Z}$. For such a prime $\mathfrak{P}$ we have that $kbP = 0$ in the group $E(\mathbf{F}_\mathfrak{p})$, where $\mathfrak{p}$ is the prime of F over which $\mathfrak{P}$ lies. Therefore

$$kbQ = kgP = gR = 0 \qquad \text{in } E(\mathbf{F}_\mathfrak{p}),$$

and hence R is contained in $E[g]$ modulo $\mathfrak{P}$. Since this is so for infinitely many prime ideals $\mathfrak{P}$, we have that $R \in E[g]$. Since R was an arbitrary point in $E[b]$, we have shown that $E[b] \subset E[g]$. This implies that b divides g in the ring O and hence

$$bQ = bfP \qquad \text{for some endomorphism} \qquad f \in O.$$

Consequently $Q = fP + R$ for some torsion point R in $E(F)$. As in the proof in the case where E does not admit any complex multiplications, one deduces, using Siegel's Theorem once more, that $Q = fP$. This completes the proof of Theorem 2.

REFERENCES

1. J. W. S. Cassels and A. Fröhlich, Eds., "Algebraic Number Theory," Academic Press, London/New York, 1967.
2. G. Janusz, "Algebraic Number Theory," Academic Press, New York/London, 1973.

3. J. Silverman, "The Arithmetic of Elliptic Curves," Graduate Texts in Mathematics, Vol. 106, Springer-Verlag, Heidelberg/New York, 1986.
4. A. Schinzel, On exponential congruences, *Mat. Zametki*, to appear.
5. J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331. (Œuvres, III, Springer-Verlag, Berlin/Heidelberg/New York/Tokyo, 1986, 1–73.)