C. R. Math. Rep. Acad. Sci. Canada Vol. **38** (2) 2016, pp. 75–84

On Dependence of Rational Points on Elliptic Curves

Mohammad Sadek

Presented by Pierre Milman, FRSC

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$. Let Γ be a subgroup of $E(\mathbb{Q})$ and $P \in E(\mathbb{Q})$. In [1], it was proved that if E has no nontrivial rational torsion points, then $P \in \Gamma$ if and only if $P \in \Gamma \bmod p$ for finitely many primes p. In this note, assuming the General Riemann Hypothesis, we provide an explicit upper bound on these primes when E does not have complex multiplication and either E is a semistable curve or E has no exceptional prime.

Résumé. Soit E une courbe elliptique définie sur $\mathbb{Q}$. Soit Γ un sous-groupe de $E(\mathbb{Q})$ et $P \in E(\mathbb{Q})$. Dans [1], il on a prouvé que si E n'a pas de points de torsion rationels non trivials, alors $P \in \Gamma$ si et seulement si $P \in \Gamma \bmod p$ pour un nombre fini de nombres premiers p. Dans cette note, supposant l'hypothèse général de Riemann, nous fournissons une borne-supérieure explicite sur ces nombres premiers quand E n'a pas de multiplication complexe et soit E est une courbe semi-stable soit E n'a aucun nombre premier exceptionnel.

1. **Introduction** For a given set of rational points on an elliptic curve E defined over $\mathbb{Q}$, there are several methods to check if these points are linearly dependent. These methods include heights on elliptic curves, and the two descent algorithm. In [1], the authors showed that linear dependence of rational points on certain abelian varieties over a given number field K satisfies a local to global principle. Namely, a set of rational points on such an abelian variety satisfies a dependence relation over K if and only if it satisfies a dependence relation when reduced modulo all but finitely many primes of K. In fact, they even proved a stronger version of the latter result. More precisely, a dependence relation of rational points holds on these abelian varieties if and only if these points satisfy dependence relations modulo finitely many primes. The reader interested in detecting dependence of rational points on abelian varieties via reduction maps may consult [3, 4] and the references there.

In this note, we analyse the aforementioned results. Given an elliptic curve $E/\mathbb{Q}$ and a basis $P_1, \ldots, P_r$ for $E(\mathbb{Q})$, a point $P \in E(\mathbb{Q})$ lies in a subgroup

Received by the editors on April 15, 2015; revised August 18, 2015.

I would like to thank the referee for many comments, corrections, suggestions, and a great deal of patience that helped the author improve the manuscript significantly.

AMS Subject Classification: Primary: 11G05; secondary: 14G05.

Keywords: Elliptic curves, rational points, linear dependence.

$\Gamma \subset E(\mathbb{Q})$ if and only if the reduction of P lies in Γ modulo finitely many primes. The choice of these primes depends on E, the points $P, P_1, \ldots, P_r$, and the subgroup Γ. Assuming that E has no nontrivial rational torsion points, we introduce an explicit upper bound on these primes when E has no complex multiplication and either E is semistable or E has no exceptional prime where certain values are not attained by the j-invariant of E. The key idea in order to provide such a bound is to use an effective version of Chebotarev's theorem which assumes the Generalized Riemann hypothesis, GRH.

2. **Linear Dependence of Rational Points** In this section we will review the main results of [1] for an elliptic curve defined over $\mathbb{Q}$. Let E be an elliptic curve defined over $\mathbb{Q}$. We assume moreover that E has no nontrivial torsion over $\mathbb{Q}$. Let $P_1, \ldots, P_r$ be a basis for $E(\mathbb{Q})$.

For each $j, 1 \leq j \leq r$, a lattice $\widetilde{\Gamma}_j \subset E(\mathbb{Q})$ is defined, see p. 334 for the precise definition of $\widetilde{\Gamma}_j$. Given $P \in E(\mathbb{Q})$ there exist $n_1, \ldots, n_r \in \mathbb{Z}$ such that $P = n_1 P_1 + \ldots + n_r P_r$. For each $1 \leq j \leq r$ and for each prime $l \mid n_j$, the field $L_{j,l}$ is defined as follows:

$$L_{j,l} := \mathbb{Q}\left(E[l^{k_{j,l}+1}], \frac{1}{l^{k_{j,l}}}\widetilde{\Gamma}_j\right),$$

where $k_{j,l}$ is chosen such that the image of the residual representation

$$\overline{\rho}_{l^{k_{j,l}+1}} : \mathrm{Gal}\left(\mathbb{Q}(E[l^{k_{j,l}}])/\mathbb{Q}\right) \to \mathrm{GL}_2\left(\mathbb{Z}/l^{k_{j,l}+1}\mathbb{Z}\right)$$

contains a nontrivial homothety and such that $E[l^{k_{j,l}}]$ contains at least r points, see Theorem 6.3 of [1]. In particular since $E[l^{k_{j,l}}] \cong \mathbb{Z}/l^{k_{j,l}}\mathbb{Z} \times \mathbb{Z}/l^{k_{j,l}}\mathbb{Z}$, it follows that $l^{k_{j,l}} \geq \sqrt{r}$. Moreover one must have $k_{j,l} \geq \mathrm{ord}_l(n_j)$, see Theorem 6.4 in [1]. Therefore one may choose $k_{j,l} \geq \max\left\{\dfrac{\log r}{2\log l}, \dfrac{\log |n_j|}{\log l}\right\}$ such that the image of the representation $\overline{\rho}_{l^{k_{j,l}+1}}$ contains a nontrivial homothety.

One observes that

$$L_{j,l} \subset F_{j,l} := \mathbb{Q}\left(E[l^{k_{j,l}+1}], \frac{1}{l^{k_{j,l}}}E(\mathbb{Q})\right)$$

since $\widetilde{\Gamma}_j \subset E(\mathbb{Q})$.

The authors in [1] defined a finite set $S_{j,l}$ which contains all primes q such that every $\sigma \in \mathrm{Gal}(L_{j,l}/\mathbb{Q})$ is a Frobenius element at some $q \in S_{j,l}$. An effective version of Chebotarev's theorem was used to construct the set $S_{j,l}$.

Given a number field L, an effective version of Chebotarev's theorem by Lagarias and Odlyzko states that there are effectively computable constants $b_{1,L}$ and $b_{2,L}$ such that every element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ is equal to the Frobenius element $\mathrm{Frob}_q \in \mathrm{Gal}(L/\mathbb{Q})$ for an integer prime q such that $q \leq b_{1,L}\Delta_L^{b_{2,L}}$ where Δ_L is the discriminant of L.

For each j such that $n_j \neq 0$, the following sets were defined in [1]

$$\begin{aligned} S_{j,l} &:= \{q : q \leq b_{1,L_{j,l}} \Delta_{L_{j,l}}^{b_{2,L_{j,l}}} \text{ and } q \text{ is a good prime for } E\}, \\ S_j &:= \bigcup_{l|n_j} S_{j,l}. \end{aligned}$$

The set S is defined by

$$S := \bigcup_{1 \leq j \leq r, n_j \neq 0} S_j.$$

A local to global property for dependence of rational points on an abelian variety of certain type defined over a number field can be found in [1] and the references there. In fact, an elliptic curve defined over $\mathbb{Q}$ is an abelian variety which satisfies the hypotheses of [1, Theorem 6.4], see [1, Corollary 4.3]. Throughout this note, if $P \in \mathbb{P}^2(\mathbb{Q})$, we write P_p for the reduction of P in $\mathbb{P}^2(\mathbb{F}_p)$.

Theorem 2.1 (Theorem 6.4, [1]). *Let E be an elliptic curve defined over $\mathbb{Q}$. Let $P \in E(\mathbb{Q})$ and let Γ be a subgroup of $E(\mathbb{Q})$. Let S be the finite set defined above. If $P_p \in \Gamma$ mod p for all $p \in S$ then $P \in \Gamma + E(\mathbb{Q})_{\text{tor}}$. Hence if $E(\mathbb{Q})_{\text{tor}} \subset \Gamma$, then the following conditions are equivalent:*

(1) $P \in \Gamma$.
(2) $P_p \in (\Gamma \text{ mod } p)$ for all $p \in S$.

Remark 2.2. In Theorem 2.1, the equivalence holds because $S_{j,l}$ contains the primes q for which every $\sigma \in \text{Gal}(L_{j,l}/\mathbb{Q})$ is equal to the Frobenius element Frob_q at q. An effective version of Chebotarev's theorem by Lagarias and Odlyzko is used to provide an upper bound for these primes q, see the proofs of Theorem 6.2 and Theorem 6.4 of [1]. Thus one can replace $S_{j,l}$ with any finite set containing the primes q in the definition of S in Theorem 2.1. In fact, we will use a different effective version of Chebotarev's theorem to introduce an alternative finite set.

In the following lemma, we collect different effective versions of Chebotarev's Density Theorem. One can use these versions to redefine the sets $S_{j,l}, S_j$ and S, see Remark 2.2. The following can be found as Theorem 2.2 and Proposition 2.3 in [5].

Lemma 2.3. *Let $L/\mathbb{Q}$ be a finite Galois extension. We denote the absolute value of the discriminant and the degree of $L/\mathbb{Q}$ by Δ_L and d_L respectively. Let C be a conjugacy class of $\text{Gal}(L/\mathbb{Q})$. There is an integer prime p such that the Frobenius at p is in C, and such that p satisfies the following bounds.*

(a) *There is an absolute effectively computable constant A such that $p \leq 2\Delta_L^A$.*

Now we assume the GRH.

(b) *There is an absolute effectively computable constant b such that $p \leq b(\log \Delta_L)^2$. In fact, one may take $b = 70$.*
(c) *If S is a set of prime numbers such that $L/\mathbb{Q}$ is unramified outside of S, for the conjugacy class C in $\mathrm{Gal}(L/\mathbb{Q})$, there exists a prime number $p \notin S$ such that the Frobenius at p is in C, and such that*

$$p \leq 280 d_L^2 \left(\log d_L + \sum_{q \in S} \log q \right)^2 .$$

For each $1 \leq j \leq r$ and each prime $l \mid n_j$, we recall that $L_{j,l} \subset F_{j,l} := \mathbb{Q}\left(E[l^{k_{j,l}+1}], \frac{1}{l^{k_{j,l}}} E(\mathbb{Q})\right)$. Now we define sets $S'_{j,l}, S'_j$ and S' under the assumption of the GRH. Assuming the GRH, one can use Lemma 2.3 (c) in order to define a set $S'_{j,l}$ which contains all the primes q such that every $\sigma \in \mathrm{Gal}(F_{j,l}/\mathbb{Q})$ is the Frobenius element at some $q \in S'_{j,l}$. We set

$$\begin{aligned}
S'_{j,l} &:= \left\{ q : q \leq 280 d_{F_{j,l}}^2 \left(\log d_{F_{j,l}} + \sum_{q \in B} \log q \right)^2 \text{ and } q \text{ is a good prime for } E \right\}, \\
S'_j &:= \bigcup_{l \mid n_j} S'_{j,l}, \\
S' &:= \bigcup_{1 \leq j \leq r, n_j \neq 0} S'_j,
\end{aligned}$$

where $d_{F_{j,l}}$ is the degree of the extension $F_{j,l}/\mathbb{Q}$, and B is the set of primes outside which the field $F_{j,l}$ is unramified. In fact, the field $F_{j,l}$ is unramified outside the set of bad primes of E and the prime l, see [8, Theorem 1].

Theorem 2.1 and Remark 2.2 yield the following consequence.

COROLLARY 2.4. *Assume that E is an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\mathrm{tor}} = \{O_E\}$. Let $P \in E(\mathbb{Q})$ and Γ a subgroup of $E(\mathbb{Q})$. Let S' be defined as above. The following conditions are equivalent:*

(1) $P \in \Gamma$.
(2) $P_p \in (\Gamma \ mod\ p)$ *for all* $p \in S'$.

3. Bounds In this section we find explicit bounds for the coefficients of a linear dependence relation in $E(\mathbb{Q})$.

3.1. A bound on the coefficients of a linear dependence relation Let E be an elliptic curve defined over $\mathbb{Q}$ with rank r such that $E(\mathbb{Q})_{\mathrm{tor}} = \{O_E\}$. Let $P_1, \ldots, P_r$ be a basis for $E(\mathbb{Q})$. Recall that the height pairing on E is

$$\begin{aligned}
\langle\ ,\ \rangle &: E \times E \to \mathbb{R} \\
\langle P, Q \rangle &= \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)
\end{aligned}$$

where $\hat{h} : E \to \mathbb{R}$ is the canonical height on E, see (§9, VIII, [9]). The regulator matrix R_E of E is given by $(\langle P_i, P_j \rangle)_{1 \leq i,j \leq r}$. The eigen values of Reg_E are $\lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_r$.

Lemma 3.1. *Let $P \in E(\mathbb{Q})$ be such that*

$$P = \sum_{i=1}^{r} n_i P_i,\ n_i \in \mathbb{Z}.$$

For each j, $1 \leq j \leq r$, one has

$$|n_j| \leq \left| \frac{\langle P, P \rangle}{\lambda_1} \right|^{1/2}$$

where $N^T = \begin{pmatrix} n_1 & n_2 & \ldots & n_r \end{pmatrix}$.

Proof. Using the fact that the height pairing $\langle\ ,\ \rangle$ is bilinear and positive definite, one obtains the following equality

$$\langle P, P \rangle = \sum_{i,j} n_i n_j \langle P_i, P_j \rangle = N^T \,\mathrm{Reg}_E\, N \geq 0.$$

In addition, one has

$$\min_i \lambda_i \leq \frac{N^T \,\mathrm{Reg}_E\, N}{N^T N} \leq \max_i \lambda_i.$$

One observes that $N^T N = \sum_i n_i^2$, therefore for any j, $1 \leq j \leq r$, one has

$$\langle P, P \rangle = N^T \,\mathrm{Reg}_E\, N \geq \lambda_1 N^T N \geq \lambda_1 n_j^2.$$

□

3.2. Bounding the degree of a Kummer extension In the following lemma we estimate the degree of the Kummer extension $F_{j,l} = \mathbb{Q}\left(E[l^{k_{j,l}+1}], \frac{1}{l^{k_{j,l}}} E(\mathbb{Q})\right)$.

Lemma 3.2. *Let $E/\mathbb{Q}$ be an elliptic curve of rank r. Let l be an integer prime and m a positive integer. Let L denote the field $\mathbb{Q}\left(E[l^m], \frac{1}{l^{m-1}} E(\mathbb{Q})\right)$. Then*

$$[L : \mathbb{Q}] \leq (l^2 - 1)(l^2 - l) l^{2mr + 4(m-1)}.$$

Proof. The Galois group of the field extension

$$\mathbb{Q}\left(E[l^m], \frac{1}{l^{m-1}} E(\mathbb{Q})\right) / \mathbb{Q}(E[l^m])$$

can be viewed as a subgroup of the product $(E[l^m])^r$. Therefore, the degree of the extension is at most l^{2mr}. Now it is known that $\mathrm{Gal}\,(\mathbb{Q}(E[l^m])/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/l^m\mathbb{Z})$, where the latter group is of order $(l^2 - 1)(l^2 - l) l^{4(m-1)}$, hence follows the upper bound for $[L : \mathbb{Q}]$. □

4. **Main Results** We assume that E is an elliptic curve defined over $\mathbb{Q}$ with $E(\mathbb{Q})_{\text{tor}} = \{O_E\}$ and the rank of $E(\mathbb{Q})$ is $r > 0$. Therefore, all rational points in $E(\mathbb{Q})$ are of infinite order. Let $P_1, \ldots, P_r$ be a basis for $E(\mathbb{Q})$.

Let $\Gamma = d_1\mathbb{Z}P_1 + d_2\mathbb{Z}P_2 + \ldots + d_s\mathbb{Z}P_s + \ldots + d_r\mathbb{Z}P_r$ where $d_i \in \mathbb{Z} \setminus \{0\}$ if $1 \leq i \leq s$ and $d_i = 0$ otherwise. Assume that $P = n_1P_1 + \ldots + n_rP_r$ for some $n_i \in \mathbb{Z}$. In view of Corollary 2.4, $P \in \Gamma$ if and only if $P \in \Gamma \bmod p$ for every prime p lying in the finite set S'.

LEMMA 4.1. *Assume the GRH. For any prime $q \in S'_{j,l}$, one has*

$$q \leq 280M_{j,l}^2 \left[\log(M_{j,l}\, Q_{j,l})\right]^2$$

where $M_{j,l} = (l^2-1)(l^2-l)l^{2(k_{j,l}+1)r+4k_{j,l}}$, and $Q_{j,l}$ is the product of the prime divisors of the discriminant of the field extension $F_{j,l}/\mathbb{Q}$.

PROOF. Recall that

$$S'_{j,l} := \left\{ q : q \leq 280 d_{F_{j,l}}^2 \left(\log d_{F_{j,l}} + \sum_{p \in B_{j,l}} \log p \right)^2 \text{and } q \text{ is a good prime for } E \right\}$$

where $B_{j,l}$ is the set of primes outside which $F_{j,l}$ is unramified. Those primes are exactly the prime divisors of the discriminant of the field extension $F_{j,l}/\mathbb{Q}$. In particular, the set $B_{j,l}$ contains the bad primes of E together with l. We set $d_{F_{j,l}}$ to be the degree of the extension $F_{j,l}/\mathbb{Q}$. Therefore for every $q \in S'_{j,l}$, one has $q \leq 280 d_{F_{j,l}}^2 \left(\log d_{F_{j,l}} + \sum_{l'} \log l' \right)^2$ where l' is a prime in $B_{j,l}$. Now the statement of the lemma follows once one observes that $M_{j,l}$ is the upper bound of $d_{F_{j,l}}$ obtained in Lemma 3.2. □

We recall that a prime integer l is said to be an *exceptional prime* for an elliptic curve E defined over $\mathbb{Q}$ if the mod l Galois representation

$$\rho_{E,l} : \text{Gal}\left(\mathbb{Q}(E[l])/\mathbb{Q}\right) \to \text{GL}_2(\mathbb{Z}/l\mathbb{Z})$$

is not surjective. If E has complex multiplication then every prime is exceptional except possibly for the prime 2. If E has no complex multiplication then it was proved by Serre that the number of exceptional primes is finite, see [7]. In fact Serre conjectured that any exceptional prime for E is less than or equal to 37. Mazur proved that if E is semistable with no complex multiplication, then no prime ≥ 11 can be exceptional for E, see [6]. In [2], in terms of heights, almost all elliptic curves are proved to have no exceptional primes.

We will use the following two lemmas to produce an explicit bound on the primes in the finite set S' defined in §2 if E defined over $\mathbb{Q}$ has no complex multiplication, and either E has no exceptional primes or E is semistable.

Lemma 4.2. *Let E be an elliptic curve defined over $\mathbb{Q}$ with no complex multiplication. Let j be the j-invariant of E. Let $\rho_{l^n} : \mathrm{Gal}\left(\mathbb{Q}(E[l^n])/\mathbb{Q}\right) \to \mathrm{GL}_2(\mathbb{Z}/l^n\mathbb{Z})$ be the Galois representation associated to the l^n-torsion points of E. The following statements hold.*

i. *ρ_2 is not surjective if and only if $j = 256(t+1)^3/t$ or $j = t^2+1728$ for some $t \in \mathbb{Q}$.*
ii. *ρ_3 is not surjective if and only if $j = 27(t+1)(t+9)^3/t^3$ or $j = t^3$ for some $t \in \mathbb{Q}$.*
iii. *ρ_5 is not surjective if and only if*

$$\begin{aligned} j &= \frac{5^3(t+1)(2t+1)^3(2t^2-3t+3)^3}{(t^2+t-1)^5}, \\ j &= \frac{5^2(t^2+10t+5)^3}{t^5}, \quad \textit{or} \\ j &= t^3(t^2+5t+40) \end{aligned}$$

iv. *ρ_7 is not surjective if and only if*

$$\begin{aligned} j &= \frac{t(t+1)^3(t^2-5t+1)^3(t^2-5t+8)^3(t^4-5t^3+8t^2-7t+7)^3}{(t^3-4t^2+3t+1)^7}, \\ j &= \frac{64t^3(t^2+7)^3(t^2-7t+14)^3(5t^2-14t-7)^3}{(t^3-7t^2+7t+7)^7}, \ \textit{or} \\ j &= \frac{(t^2+245t+2401)^3(t^2+13t+49)}{t^7} \end{aligned}$$

for some $t \in \mathbb{Q}$.

Proof. This is Proposition 6.1 in [10]. □

Lemma 4.3. *Let E be an elliptic curve defined over $\mathbb{Q}$ with no complex multiplication. Let j be the j-invariant of E. Let $\rho_{l^\infty} : \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \to \mathrm{GL}_2(\mathbb{Z}_l)$ be the Galois representation describing the Galois action on the Tate module of E. The following statements hold.*

i. *The representation ρ_{2^∞} is not surjective if and only if ρ_2 is not surjective, or j is of the form*

$$-4t^3(t+8),\ -t^2+1728,\ 2t^2+1728,\ \textit{or}\ -2t^2+1728$$

for some $t \in \mathbb{Q}$.
ii. *The representation ρ_{3^∞} is not surjective if and only if ρ_3 is not surjective, or*

$$j = -\frac{3^7(t^2-1)^3(t^6+3t^5+6t^4+t^3-3t^2+12t+16)^3(2t^3+3t^2-3t-5)}{(t^3-3t-1)^9}$$

for some $t \in \mathbb{Q}$.

iii. *If $l \geq 5$ then ρ_{l^∞} is not surjective if and only if ρ_l is not surjective.*

PROOF. This is Lemma 6.6 in [10]. □

One remarks that if ρ_{l^∞} is surjective then ρ_{l^n} is surjective for any positive integer n.

THEOREM 4.4. *We assume the GRH. Let $E/\mathbb{Q}$ be an elliptic curve with no complex multiplication and no exceptional primes. Assume that $E(\mathbb{Q}) \cong \mathbb{Z}^r, r > 0$. Let $P_1, \ldots, P_r$ be a basis for $E(\mathbb{Q})$, and λ the minimum eigen value of the regulator matrix $(\langle P_i, P_j \rangle)_{1 \leq i,j \leq r}$. We assume that the j-invariant j of E is not written as*

$$\frac{256(t+1)^3}{t},\ t^2+1728,\ -4t^3(t+8),\ -t^2+1728,\ 2t^2+1728,\ or\ -2t^2+1728$$

for any $t \in \mathbb{Q}$. Let $P \in E(\mathbb{Q})$ and Γ a subgroup of $E(\mathbb{Q})$. The following conditions are equivalent.

(1) *$P \in \Gamma$ where $P = n_1 P_1 + \ldots + n_r P_r$, $n_i \in \mathbb{Z}$.*
(2) *$P_p \in \Gamma$ mod p, for every prime $p \leq 280 M^2 \left[\log(M\,Q)\right]^2$ where*

$$\begin{aligned} M &= (C-1)\left(C-\sqrt{C}\right) C^{K(r+2)+r}, \\ C &= \left|\frac{\langle P, P\rangle}{\lambda}\right|^{1/2}, \\ K &= \max\left\{2, \frac{\log r}{2\log 2}, \frac{\log C}{\log 2}\right\},\ and \\ Q &= \max_{\substack{1\leq j\leq r \\ l \mid n_j}} Q_{j,l} \end{aligned}$$

where $Q_{j,l}$ is the product of the prime divisors of the discriminant of $F_{j,l}/\mathbb{Q}$.

PROOF. Theorem 2.1 implies that $P \in \Gamma$ if and only if $P_p \in \Gamma \bmod p$ for every $p \in S'$ where

$$S' := \bigcup_{1\leq j\leq r,\, n_j \neq 0} \left(\bigcup_{l \mid n_j} S'_{j,l} \right).$$

Lemma 4.1 implies that if $q \in S'_{j,l}$, then $q \leq 280 M_{j,l}^2 \left[\log(M_{j,l}\, Q_{j,l})\right]^2$ where $M_{j,l} = (l^2-1)(l^2-l) l^{2(k_{j,l}+1)r+4k_{j,l}}$, and we choose $k_{j,l} \geq \max\left\{\frac{\log r}{2\log l}, \frac{\log |n_j|}{\log l}\right\}$ such that the image of the residual representation

$$\overline{\rho}_{l^{k_{j,l}+1}} : \mathrm{Gal}\left(\mathbb{Q}(E[l^{k_{j,l}}])/\mathbb{Q}\right) \to \mathrm{GL}_2\left(\mathbb{Z}/l^{k_{j,l}}\mathbb{Z}\right)$$

contains a nontrivial homothety, see §2. Since E has no exceptional primes it follows that $\overline{\rho}_{l^2}$ is surjective for every prime l, hence the image of $\overline{\rho}_{l^2}$ contains a nontrivial homothety for every prime $l \neq 2$. It follows that one can set $k_{j,l} = \max\left\{1, \dfrac{\log r}{2\log l}, \dfrac{\log|n_j|}{\log l}\right\}$ when $l \neq 2$. In view of Lemma 4.2 and Lemma 4.3 our assumption on the values taken by the j-invariant of E forces ρ_{2^∞} to be surjective, and hence the representation ρ_{2^n} is surjective for any positive integer n. In particular the residual representation $\overline{\rho}_8$ is surjective. In other words the image of $\overline{\rho}_8$ contains a nontrivial homothety. Therefore one may set $k_{j,2} = \max\left\{2, \dfrac{\log r}{2\log 2}, \dfrac{\log|n_j|}{\log 2}\right\}$.

For every j, $1 \leq j \leq r$, one has $|n_j| \leq C$, see Lemma 3.1. If l is a prime dividing n_j, then $2 \leq l \leq \sqrt{C}$. Therefore $k_{j,l} \leq K = \max\left\{2, \dfrac{\log r}{2\log 2}, \dfrac{\log C}{\log 2}\right\}$ for every j, l. Thus one obtained an upper bound $M = (C-1)\left(C - \sqrt{C}\right) C^{(K+1)r+2K}$ for $M_{j,l}$ in Lemma 4.1 for any l, j. Therefore if $p \in S'$, then $p \leq 280M^2\left[\log(M\,Q)\right]^2$. □

Theorem 4.5. *We assume the GRH. Let $E/\mathbb{Q}$ be a semistable elliptic curve with no complex multiplication such that $E(\mathbb{Q}) \cong \mathbb{Z}^r, r > 0$. Let $P_1, \ldots, P_r$ be a basis for $E(\mathbb{Q})$, and λ the minimum eigen value of the regulator matrix $(\langle P_i, P_j\rangle)_{1\leq i,j\leq r}$. We assume that the j-invariant j of E is not written as*

$$\frac{256(t+1)^3}{t},\ t^2+1728,\ -4t^3(t+8),\ -t^2+1728,\ 2t^2+1728,\ -2t^2+1728,$$

$$\frac{27(t+1)(t+9)^3}{t^3},\ t^3,$$

$$-\frac{3^7(t^2-1)^3(t^6+3t^5+6t^4+t^3-3t^2+12t+16)^3(2t^3+3t^2-3t-5)}{(t^3-3t-1)^9},$$

$$\frac{5^3(t+1)(2t+1)^3(2t^2-3t+3)^3}{(t^2+t-1)^5}, \frac{5^2(t^2+10t+5)^3}{t^5},\ t^3(t^2+5t+40),$$

$$\frac{t(t+1)^3(t^2-5t+1)^3(t^2-5t+8)^3(t^4-5t^3+8t^2-7t+7)^3}{(t^3-4t^2+3t+1)^7},$$

$$\frac{64t^3(t^2+7)^3(t^2-7t+14)^3(5t^2-14t-7)^3}{(t^3-7t^2+7t+7)^7},\ \text{or}\ \frac{(t^2+245t+2401)^3(t^2+13t+49)}{t^7}$$

for any $t \in \mathbb{Q}$. Let $P \in E(\mathbb{Q})$ and Γ a subgroup of $E(\mathbb{Q})$. The following conditions are equivalent.

(1) *$P \in \Gamma$ where $P = n_1P_1 + \ldots + n_rP_r$, $n_i \in \mathbb{Z}$.*
(2) *$P_p \in \Gamma$ mod p, for every prime $p \leq 280M^2\left[\log(M\,Q)\right]^2$ where $M = (C-1)\left(C - \sqrt{C}\right)C^{K(r+2)+r}$, $C = \left|\dfrac{\langle P, P\rangle}{\lambda}\right|^{1/2}$,*

$K = \max\left\{2, \dfrac{\log r}{2\log 2}, \dfrac{\log C}{\log 2}\right\}$, *and* $Q = \max\limits_{\substack{1\le j\le r\\ l\mid n_j}} Q_{j,l}$ *where* $Q_{j,l}$ *is the product of the prime divisors of the discriminant of* $F_{j,l}/\mathbb{Q}$.

PROOF. The proof is similar to that of Theorem 4.4. Since E is semistable with no complex multiplication, it follows that the residual representation

$$\overline{\rho}_{l^2} : \mathrm{Gal}\left(\mathbb{Q}(E[l])/\mathbb{Q}\right) \to \mathrm{GL}_2\left(\mathbb{Z}/l\mathbb{Z}\right)$$

is surjective for any $l \geq 11$, see [7]. That the j-invariant is not one of the ones above implies that $\overline{\rho}_{l^2}$ is surjective for any prime $l < 11$, see Lemma 4.2 and Lemma 4.3. It follows that the image of $\overline{\rho}_{l^2}$ contains a nontrivial homothety for any $l \neq 2$. Again our assumption on the j-invariant implies that ρ_{2^∞} is surjective which yields that the residual representation $\overline{\rho}_8$ contains a nontrivial homothety. The latter argument together with the fact that $2 \leq l \leq \sqrt{C}$ yield the upper bound K for $k_{j,l}$, hence the upper bound M for $M_{j,l}$ for every j, l, see Lemma 4.1. □

REFERENCES

1. G. Banaszak and P. Krasoń. On arithmetic in Mordell-Weil groups. *Acta Arithmetica*, 150(4):315–337, 2011.
2. W. Duke. Elliptic curves with no exceptional primes. *C. R. Acad. Sci. Paris*, 325(8):813–818, 1997.
3. W. Gajda and K. Górnisiewicz. Linear dependence in mordell-weil groups. *Journal für die reine und angew. Mathematik*, 630:219–233, 2009.
4. P. Jossen. Detecting linear dependence on a simple abelian variety via reduction maps. *Commentarii Math. Helv.*, 88(2):323–352, 2013.
5. S. Lichtenstein. The effective Chebotarev density theorem and modular forms mod $\mathfrak{m}$. *Proc. Amer. Math Soc.*, 136(10):3419–3428, 2008.
6. B. Mazur. Rational isogenies of prime degree. *Invent. Math.*, 44:129–162, 1978.
7. J. P. Serre. Propriésés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15:123–201, 1972.
8. J. P. Serre and J. Tate. Good reduction of abelian varieties. *Annals of Mathematics*, 88(3):492–517, 1968.
9. J. Silverman. *The Arithmetic of Elliptic Curves*. GTM 106. Springer-Verlag, New York, 1986.
10. D. Zywina. On the surjectivity of mod ℓ representations associated to elliptic curves. *submitted*.

Department of Mathematics and Actuarial Science, American University in Cairo, Cairo, Egypt
e-mail: mmsadek@aucegypt.edu