Invent. math. 101, 225–235 (1990)

*Inventiones mathematicae*


# Cyclicity and generation of points mod $p$ on elliptic curves

Rajiv Gupta[1,*] and M. Ram Murty[2,*]

[1] Department of Mathematics, University of British Columbia, Vancouver V6T 1Y4, Canada
[2] Department of Mathematics, McGill University, Montreal H3A 2K6, Canada

## 1. Introduction

In this paper we study the group of points modulo $p$ of elliptic curves defined over $\mathbb{Q}$. In particular, we are interested in the frequency with which this group is cyclic and with which it is generated by a fixed set of global rational points. Let $E$ be an elliptic curve over $\mathbb{Q}$ and for each prime $p$ where $E$ has good reduction, let $\bar{E}(\mathbb{F}_p)$ be the group of rational points on the reduction of $E$ modulo $p$. In [14], Serre raised the question of how often this group is cyclic, and following Hooley's work [6] on Artin's primitive root conjecture, showed that the number of such $p \leqq x$ is $\sim cx/\log x$ for some constant $c$, assuming the Generalized Riemann Hypothesis (GRH). The second author removed this hypothesis for curves with complex multiplication (CM) in [9], and also demonstrated unconditionally the existence of infinitely many primes for which $\bar{E}(\mathbb{F}_p)$ is cyclic in [10], for certain non-CM elliptic curves. Though the method of [9] establishes an asymptotic formula, the method of [10] does not give a good lower bound for the number of such primes. We will prove unconditionally:

**Theorem 1.** *The group $\bar{E}(\mathbb{F}_p)$ is cyclic for infinitely many $p$ if and only if $E$ has a non-rational 2-division point, and moreover, in this case, the number of primes $p \leqq x$ for which $\bar{E}(\mathbb{F}_p)$ is cyclic is $\gg x/\log^2 x$.*

The proof of this result is given in section 2; the key is a result from the theory of sieves.

In [3] we discussed the following question, raised by Lang and Trotter [8]: Given a rational point $X$ of infinite order in the Mordell-Weil group $E(\mathbb{Q})$, how often does the reduction of $X$ mod $p$ equal the full group $\bar{E}(\mathbb{F}_p)$? This question is analogous to the classical question of how often a given integer is a primitive root mod $p$, but the situation cannot be handled by Hooley's method, owing to the large

* Research partially supported by grants from NSERC

size of the conjugacy classes. However, if $E$ has CM by the ring of integers of the imaginary quadratic field $k$, the authors were able to prove in [3] that the set of primes $p$ such that $\bar{E}(\mathbb{F}_p) = \langle \bar{X} \rangle$ and $p$ splits in $k$ has a density. This method does not apply to primes which are inert in $k$, and we must consider the following somewhat weaker question, also raised in [8].

Let $\Gamma$ be a free subgroup of $E(\mathbb{Q})$ of rank $r(\Gamma)$ and define

$$S(\Gamma) = \{p \text{ prime} | \bar{E}(\mathbb{F}_p) = \Gamma_p\} ,$$

where $\Gamma_p$ is the reduction of $\Gamma$ mod $p$. Also, if $E$ has CM by $k$, let

$$S'(\Gamma) = \{p \text{ prime} | \bar{E}(\mathbb{F}_p) = \Gamma_p \text{ and } p \text{ is inert in } k\} .$$

One expects the sets $S(\Gamma)$ and $S'(\Gamma)$ to have certain densities $\delta(\Gamma)$ and $\delta'(\Gamma)$ (see sections 4 and 5). Provided $r(\Gamma)$ is sufficiently large, one can verify these expectations under the assumption of the GRH (see [3]). The ranks for which our results apply can be lowered substantially by not insisting on producing the full densities above but rather positive multiples of them. Such results were previously known (see [3]) only for CM curves with $r(\Gamma) \geqq 10$ and non-CM curves with $r(\Gamma) \geqq 18$.

**Theorem 2.** *If $E$ has CM and $r(\Gamma) \geqq 2$, then, under the GRH, $S'(\Gamma)$ contains a set of density $\geqq (1 - \log 2 - \varepsilon)\delta'(\Gamma)$ for any $\varepsilon > 0$*

**Theorem 3.** *If $E$ has CM and $r(\Gamma) \geqq 6$, then, under the GRH, $S(\Gamma)$ has density $\delta(\Gamma)$.*

**Theorem 4.** *If $E$ does not have CM and $r(\Gamma) \geqq 7$, then, under the GRH, for every $\varepsilon > 0$, $S(\Gamma)$ contains a set of density*

$$(1 - \log(20/9) - \varepsilon)\delta(\Gamma) ,$$

*and if we assume Artin's holomorphy conjecture, then $S(\Gamma)$ contains a set of density*

$$(1 - \log(4/3) - \varepsilon)\delta(\Gamma) .$$

The holomorphy conjecture referred to above is the statement that all Artin L-series of the extensions $L_n/\mathbb{Q}$ are analytic at $s \neq 1$, where the fields $L_n$ are as defined in section 3. Theorems 2 and 3 rely on the improved error estimate in the Chebotarev density theorem of [12], and this improvement is conditional on Artin's holomorphy conjecture. Section 3 is devoted to showing that this holds for curves with CM. In section 4 we give the proofs of Theorems 2 and 3, and in section 5 we prove theorem 4.

## 2. Cyclicity of $\bar{E}(\mathbb{F}_p)$

We let $E$ be a fixed elliptic curve over $\mathbb{Q}$, and let $K_n = \mathbb{Q}(E[n])$ for each positive integer $n$, where $E[n]$ is the set of $n$-division points of $E$. If $p$ is a prime of good reduction, it is easy to see that for any prime $q$, $(\mathbb{Z}/q\mathbb{Z})^2 \subset \bar{E}(\mathbb{F}_p)$ if and only if $p$ splits completely in $K_q$. This gives:

**Lemma 1.** *If $p$ is a prime of good reduction, $\bar{E}(\mathbb{F}_p)$ is cyclic if and only if $p$ does not split completely in $K_q$ for any prime $q$.*

On the GRH, primes which do not split completely in any $K_q$ can be successfully enumerated, and an inclusion-exclusion argument leads to the following result due to Serre [14] (see also [9]).

**Theorem.** *Assuming GRH, the primes p for which $\bar{E}(\mathbb{F}_p)$ is cyclic have density*

$$\delta = \sum_{n \geqq 1} \mu(n)/[K_n : \mathbb{Q}] ,$$

*where $\mu(n)$ denotes the Möbius function.*

We recall that Serre [13] has shown that for $E$ without CM,

$$[K_n : \mathbb{Q}] \asymp |GL_2(\mathbb{Z}/n\mathbb{Z})| ,$$

and if $E$ has CM by $\mathcal{O}_k$, then

$$[K_n : \mathbb{Q}] \asymp |(\mathcal{O}_k/n\mathcal{O}_k)^x| ,$$

so that the infinite sum above converges absolutely.

If any of the fields $K_q$ for $q$ prime is trivial, then clearly $\delta = 0$, and by the following well-known fact, this can only happen for $q = 2$.

**Lemma 2.** *The cyclotomic field $\mathbb{Q}(\zeta_n)$ is contained in $K_n$ for any n.*

*Proof.* This follows from properties of the Weil pairing $e_n$, a non-degenerate bilinear pairing $e_n : E[n] \times E[n] \to \mu_n$, where $\mu_n$ is the group of $n$-th roots of unity. The non-degeneracy of $e_n$ gives its surjectivity, and its Galois invariance means that its image is contained in $K_n$. See [16, Cor 8.1.1 p. 98] for details.

One can show that $\delta$ vanishes exactly when $K_2 = \mathbb{Q}$, and this gives in particular the infinitude of the set of primes $p$ for which $\bar{E}(\mathbb{F}_p)$ is cyclic if $K_2 \neq \mathbb{Q}$, on GRH. The key to eliminating GRH in Theorem 1 is the following lemma from sieve theory.

**Lemma 3.** *Let $S_\varepsilon(x)$ be the set of primes $p \leqq x$ such that all odd prime divisors of $p - 1$ are distinct and $\geqq x^{1/4+\varepsilon}$, p does not split completely in the field $K_2$, and E has good reduction at p. Then if $K_2 \neq \mathbb{Q}$ there is an $\varepsilon > 0$ such that $|S_\varepsilon(x)| \gg x/\log^2 x$.*

*Proof.* Since $K_2$ contains a non-trivial abelian extension of $\mathbb{Q}$ if it is non-trivial (it is the splitting field of a cubic polynomial), the restriction that $p$ not split completely in $K_2$ can be insured by imposing a congruence condition on $p$. This condition can be added to the lower bound sieve of, for example, Fouvry and Iwaniec [1] (see [2], [5]) to give the desired lower bound.

*Proof of Theorem 1.* Fix an $\varepsilon$ satisfying Lemma 3 and define

$$S(a, x) = \{p \in S_\varepsilon(x) | a_p = a\}$$

for each integer $a$ with $|a| \leqq 2x^{1/2}$, where $a_p$ denotes the trace of the Frobenius of $E$ at $p$. By Weil's Theorem, $S_\varepsilon(x)$ is the (disjoint) union of these $S(a, x)$. Now for each $S(a, x)$, we enumerate those $p \in S(a, x)$ for which $\bar{E}(\mathbb{F}_p)$ is not cyclic. Indeed, if $\bar{E}(\mathbb{F}_p)$ is not cyclic, then $(\mathbb{Z}/q\mathbb{Z})^2 \subset \bar{E}(\mathbb{F}_p)$ for some prime $q$, and by Lemma 1 and the

definition of $S_\varepsilon(x)$, $q$ is odd and $p$ splits completely in $K_q$. By Lemma 2, $p$ also splits completely in $\mathbb{Q}(\zeta_q)$, so we have $p \equiv 1 \bmod q$, i.e.

$$q | p - 1 . \tag{1}$$

Moreover, $|\bar{E}(\mathbb{F}_p)| = p + 1 - a$, so $q^2 | p + 1 - a$ and thus $q | a - 2$. Notice that $a$ cannot equal 2 since then $q^2$ would divide $p - 1$. Now by (1), $q \geqq x^{1/4+\varepsilon}$ and since $|a - 2| \ll x^{1/2}$, $q$ is determined by $a$, for $x$ sufficiently large. Any $p \in S(a, x)$ for which $\bar{E}(\mathbb{F}_p)$ is not cyclic satisfies

$$p \equiv a - 1 \bmod q^2$$

and the number of such $p$ is

$$< x/q^2 + O(1) \ll x^{1/2-2\varepsilon} .$$

The total number of $p \in S_\varepsilon(x)$ for which $\bar{E}(\mathbb{F}_p)$ is not cyclic is therefore

$$\ll x^{1/2-2\varepsilon} x^{1/2} = o(x/\log^2 x) ,$$

and this completes the proof.

## 3. Some group-theoretic preliminaries

Throughout this section we assume that $E$ has CM by the ring of integers of $k$ and let $\Gamma$ be a free subgroup of $E(\mathbb{Q})$ of rank $r(\Gamma)$. For each positive integer $n \geqq 3$, let $L_n = \mathbb{Q}(E[n], \frac{1}{n}\Gamma)$, a Galois extension of $\mathbb{Q}$ with Galois group over $\mathbb{Q}$ equal to a semidirect product of a subgroup of $GL_2(\mathbb{Z}/n\mathbb{Z})$ and a subgroup of $E[n]^{r(\Gamma)}$. Also, set $L_2 = k\mathbb{Q}(E[2], \frac{1}{2}\Gamma)$ and $G_2 = \mathrm{Gal}(L_2/\mathbb{Q})$; note that by Lemma 6 of [9], $k \subset L_n$ for all $n$. In this section we will prove the following key fact for the proof of Theorems 2 and 3.

**Proposition 1.** *Artin's holomorphy conjecture holds for the extensions $L_n/\mathbb{Q}$.*

Before proving this, we need some preliminary facts about characters of semidirect products. Let $A$ and $H$ be two subgroups of a finite group $G$ and suppose that $A$ is normal and $G = AH$ with $A \cap H = 1$. That is, $G$ is a semidirect product of $H$ by $A$. Suppose in addition that $A$ is abelian. In such a situation, it is classical knowledge that all the irreducible representations of $G$ can be constructed from those of $H$ (see e.g. Serre [15]).

Indeed, if $\chi$ is a character of $A$ and $h \in H$, define $\chi^h$ by

$$\chi^h(a) = \chi(h^{-1}ah) .$$

Then $\chi^h$ is a character of $A$ and this gives an action of $H$ on the character group of $A$ (which is isomorphic to $A$ since $A$ is abelian). Let $H_\chi$ be the stabilizer of $\chi$ and extend $\chi$ to $G_\chi = AH_\chi$ by defining $\tilde{\chi}(ah) = \chi(a)$. Then $\tilde{\chi}$ is still a one-dimensional character of $G_\chi$. Now let $\rho$ be any irreducible representation of $H_\chi$; we can view $\rho$ as a representation of $G_\chi$ by factoring through $A$. Set

$$\psi_{\chi,\rho} = \mathrm{Ind}_{G_\chi}^{G}(\tilde{\chi} \otimes \rho) .$$

An easy computation shows that $(\psi_{\chi,\rho}, \psi_{\chi,\rho}) = 1$ and therefore $\psi_{\chi,\rho}$ is irreducible. Moreover, all irreducible representations of $G$ arise as one of these.

*Proof of Proposition 1.* We suppose that $n \geqq 3$, but the same argument as below, with minor modifications, works for $L_2$ as well. Let $K_n = \mathbb{Q}(E[n])$ and denote by $M$ the Galois group of $K_n/\mathbb{Q}$. Let $H$ be the Galois group of $L_n/K_n$ and write $G$ for the Galois group of $L_n/\mathbb{Q}$. Every irreducible character of $G$ is obtained as follows. Take $\chi \in \hat{H}$, the character group of $H$, which we know is abelian. Then if $G_\chi = HM_\chi$, every irreducible representation is of the form

$$\psi_{\chi,\rho} = \mathrm{Ind}_{G_\chi}^{G}(\tilde{\chi} \otimes \rho) .$$

Suppose that $M_\chi$ is not abelian (for otherwise, the $L$-series attached to $\psi_{\chi,\rho}$ is entire). Let $M_0 = \mathrm{Gal}(K/k)$ where $k$ is the CM field of $E$; we know that $M_0$ is abelian. Then we have an exact sequence

$$1 \to M_0 \to M \to \{\pm 1\} \to 1$$

and as $M_\chi \subset M$ and $M_\chi$ is not abelian, there is an element $\sigma_\chi \in M_\chi$ such that $\sigma_\chi \mapsto -1$. We can view elements of $M$ as ordered pairs $(\tau, \sigma)$ where $\tau = \pm 1$ and $\sigma \in M_0$. With this notation, write $\sigma_\chi = (-1, \varepsilon)$. Then

$$\sigma_\chi^2 = (-1, \varepsilon)(-1, \varepsilon) = (1, -\varepsilon + \varepsilon) = (1, 0) .$$

If $g \in M_\chi \subset M$, then $g = (\tau, m_0)$. If $\tau = 1$, then $g \in M_0$. If $\tau = -1$,

$$g\sigma_\chi = (-1, m_0)(-1, \varepsilon) = (1, -\varepsilon + m_0) \in M_\chi \cap M_0 .$$

Hence every element of $M_\chi$ can be written as $(M_\chi \cap M_0)\tau^j, j = 0$ or 1. We have an exact sequence

$$1 \to M_\chi \cap M_0 \to M_\chi \to \{\pm 1\} \to 1 .$$

Thus, $\rho$ can be written as

$$\rho = \mathrm{Ind}_{M'_\chi}^{M_\chi} \omega$$

for some abelian character $\omega$ of a subgroup $M'_\chi \subset M_\chi$. Since

$$\mathrm{Ind}_{M'_\chi}^{M_\chi} \omega = \mathrm{Ind}_{HM'_\chi}^{HM_\chi} \omega ,$$

we have

$$\tilde{\chi} \otimes \mathrm{Ind}_{HM'_\chi}^{HM_\chi} \omega = \mathrm{Ind}_{HM'_\chi}^{HM_\chi} (\omega \otimes \tilde{\chi}|_{HM'_\chi})$$

by Frobenius reciprocity. Therefore, every irreducible representation of $G$ is of the form

$$\mathrm{Ind}_{G_\chi}^{G}(\tilde{\chi} \otimes \rho) = \mathrm{Ind}_{G_\chi}^{G}(\mathrm{Ind}_{G'_\chi}^{G_\chi}(\omega \otimes \tilde{\chi})) = \mathrm{Ind}_{G'_\chi}^{G}(\omega \otimes \tilde{\chi})$$

where $G'_\chi = HM'_\chi$. Thus every character of $G$ is monomial and Artin's conjecture holds.

## 4. Generation of $\bar{E}(\mathbb{F}_p)$ in the CM case

We keep the notation and assumptions of section 3 and set $G_n = \mathrm{Gal}(L_n/\mathbb{Q})$. We were able to show in [3] that if $\Gamma$ has rank 1, the reduction of $\Gamma$ generates the group

$\bar{E}(\mathbb{F}_p)$ for a density $\alpha$ of primes $p$ which split in $k$, on the GRH. The argument follows Hooley's [6] once one notes that the condition "$q$ divides the index of $\Gamma$ in $\bar{E}(\mathbb{F}_p)$" can be expressed in terms of the splitting completely of a prime $\pi$ in $k$ above $p$ in certain extensions of $k$. The number of these primes can be sufficiently well estimated using the result of Lagarias and Odlyzko [7] to prove that they have a density. This method falls through if $p$ is inert in $k$ since the divisibility condition can no longer be expressed in terms of a "splitting completely" criterion, and the enumeration of primes for which it holds becomes worse. We are no longer able to deal with the case where the subgroup $\Gamma$ of $\bar{E}(\mathbb{F}_p)$ has rank one, but can handle the case $r(\Gamma) \geqq 2$.

If $q$ is a prime and $p \nmid \Delta q$, where $\Delta$ is the discriminant of $E$, then one can show that if $\Gamma_p$ denotes the reduction of $\Gamma$ mod $p$, $q|[\bar{E}(\mathbb{F}_p):\Gamma_p]$ if and only if $\sigma_q(p) \subset C_q$, where $\sigma_q(p)$ denotes the Frobenius symbol of $p$ in the extension $L_q/\mathbb{Q}$ (a conjugacy class of $G_q$), and $C_q$ is a certain subset of $G_q$ which is closed under conjugation (see [3], p. 35). If $p$ is a prime of good reduction which is inert in $k$, so that $|\bar{E}(\mathbb{F}_p)| = p + 1$, then $q|[\bar{E}(\mathbb{F}_p):\Gamma_p]$ if and only if $\sigma_q(p) \subset C'_q$, where $C'_q = \{\sigma \in C_q | \sigma|_k = -1\}$. For our purposes, the important fact about these objects is:

**Lemma 4.** *The size of $G_q$ is $\asymp q^{2r(\Gamma)+2}$ and the sizes of $C_q$ and $C'_q$ are $\asymp q^{r(\Gamma)+1}$.*

*Proof.* This is proved in [3], p. 35 for $G_q$ and $C_q$, and the same argument applies to $C'_q$.

For any $n$, let $C_n$ (respectively $C'_n$) be the set of elements of $G_n$ whose restriction to $L_q$ lies in $C_q$ (respectively $C'_q$) for all $q|n$; $C_n$ and $C'_n$ are also closed under conjugation. Then an inclusion-exclusion makes it reasonable to expect that the primes for which $\bar{E}(\mathbb{F}_p) = \Gamma_p$ have density

$$\delta(\Gamma) = \sum_{n \geqq 1} \mu(n) \frac{|C_n|}{|G_n|},$$

and indeed, such a result was proved in [3] under the assumption of the GRH, provided $r(\Gamma) \geqq 10$. Also, we expect $S'(\Gamma)$ to have density

$$\delta'(\Gamma) = \sum_{n \geqq 1} \mu(n) \frac{|C'_n|}{|G_n|}.$$

In order to enumerate the sets $S(\Gamma)$ and $S'(\Gamma)$, we will need the following estimates for the error term in the Chebotarev density theorem.

**Proposition 2.** *Let $L/K$ be a Galois extension with Galois group $G$, and $C \subset G$ be closed under conjugation, and assume the GRH. Define*

$$\pi_C(x) = |\{\mathfrak{p} \text{ a prime of } K \text{ unramified in } L | \mathrm{Norm}_{K/\mathbb{Q}}\mathfrak{p} \leqq x \text{ and } \mathrm{Frob}_{L/K}(\mathfrak{p}) \subset C\}|.$$

*Let $d_K$ (resp. $d_L$) be the absolute value of the discriminant of $K$ (resp. $L$), $n_K = [K:\mathbb{Q}]$, $n_L = [L:\mathbb{Q}]$, $n = [L:K]$, and $P(L/K)$ be the set of rational primes lying under the primes of $K$ which ramify in $L$. Then*

$$\pi_C(x) = \frac{|C|}{|G|} li\, x + O\left(\frac{|C|}{|G|} x^{1/2}(\log d_L + n_L \log x)\right),$$

*and if Artin's holomorphy conjecture holds for $L/K$, then*

$$\pi_C(x) = \frac{|C|}{|G|}\, li\, x + O\left(|C|^{1/2} x^{1/2} \log\left(n d_K^{1/n_K} \left(\prod_{p \in P(L/K)} p\right) x\right)\right).$$

*Proof.* The first assertion is due to Lagarias and Odlyzko [7], and the second is due to Murty, Murty, and Saradha [12].

A key ingredient in the proof of Theorems 2 and 3 is the following lemma.

**Lemma 5.** *Let*

$$\pi_n(x) = |\{p \leqq x | \sigma_p(p) \in C_n'\}|\,.$$

*Then, under GRH, we have*

$$\pi_n(x) = \frac{|C_n'|}{|G_n|}\, li\, x + O(|C_n'|^{1/2} x^{1/2} \log nx)\,.$$

*Proof.* Artin's holomorphy conjecture holds for the extension $L_n/\mathbb{Q}$ by Proposition 1. Therefore, by Proposition 2,

$$\pi_n(x) = \frac{|C_n'|}{|G_n|}\, li\, x + O\left(|C_n'|^{1/2} x^{1/2} \log\left([L_n:\mathbb{Q}] \left(\prod_{p \in P(L_n/\mathbb{Q})} p\right) x\right)\right),$$

and this gives the desired result since $[L_n:\mathbb{Q}] \ll n^{2r(\Gamma)+2}$ and only the primes of bad reduction and those dividing $n$ can ramify in $L_n$.

*Proof of Theorem 2.* Let

$$N(x) = |\{p \leqq x | p \in S'(\Gamma)\}|;$$

we want to show $N(x) \geqq (1 - \log 2 - \varepsilon)\delta'(\Gamma)$. Following [3], we introduce the notation: $N(x, y) = |S(x, y)|$, where

$$S(x, y) = \{p \leqq x | p \text{ is inert in } k \text{ and } \sigma_q(p) \neq C_q \text{ for any } q \leqq y\}\,,$$

and $M(x, y, z) = |T(x, y, z)|$, where

$$T(x, y, z) = \{p \leqq x | p \text{ is inert in } k \text{ and } \sigma_q(p) \subset C_q \text{ for some } y < q < z\}\,.$$

Then, as in [3], we have

$$N(x, y) - M(x, y, 2x) \leqq N(x) \leqq N(x, y)$$

and by inclusion-exclusion,

$$N(x, y) = \sum \mu(m) \pi_m(x)\,,$$

where the summation is over all square-free integers all of whose prime factors are $\leqq y$. If

$$\delta'(y) = \sum \mu(m) \frac{|C_m'|}{|G_m|}\,,$$

with the range of summation as above, then using Lemma 5, we get

$$N(x, y) = \delta'(y) \frac{x}{\log x} + o(x/\log x)\,,$$

where $y$ is sufficiently small and $y = y(x) \to \infty$ as $x \to \infty$ (e.g. $y = (1/6)\log x$), and $\delta(y) \to \delta'(\Gamma)$ as $y \to \infty$. If some prime in the range $x^{1/2}\log x < q < 2x$ divides $[\bar{E}(\mathbb{F}_p):\Gamma_p]$, then $|\Gamma_p| < 2x^{1/2}\log x$, so by Lemma 14 of [3], we have

$$M(x, x^{1/2}\log x, 2x) = O(x/\log^2 x)\,.$$

Let $\tilde{\Gamma}$ be a rank 1 subgroup of $\Gamma$, so that

$$M(x, y, z) \leqq \tilde{M}(x, y, z)\,,$$

where $\tilde{M}(x, y, z)$ represents the same quantity as above but with $\Gamma$ replaced by $\tilde{\Gamma}$. By Lemmas 4 and 5,

$$\tilde{M}(x, y, x^{1/4}/\log x) \leqq \sum_{y < q < x^{1/4}/\log x} ((1/q^2)\,li\,x + O(qx^{1/2}\log qx)) = o(x/\log x)$$

since $y \to \infty$ as $x \to \infty$, so we need only deal with $M(x, x^{1/4}/\log x, x^{1/2}\log x)$. In fact, it suffices to estimate

$$M'(x, x^{1/4}/\log x, x^{1/2}\log x) = |S(x, y) \cap T(x, x^{1/4}/\log x, x^{1/2}\log x)|\,.$$

It is convenient to introduce

$$M'(x, y; q) = |\{p \in S(x, y) | \sigma_q(p) \subset C_q'\}|\,.$$

If $\sigma_q(p) \subset C_q'$, then $q|[\bar{E}(\mathbb{F}_p):\Gamma_p]$, so $p \equiv -1 \bmod q$. We can utilize this to obtain an upper bound for $M'(x, y; q)$. In the enumeration of $S(x, y)$ above, one has to replace the fields $L_m$, where all prime divisors of $m$ are $\leqq y$, with the compositum of these fields with $\mathbb{Q}(\zeta_q)$, and the size of the conjugacy set *does not increase.* Moreover, for $q$ sufficiently large, the field $L_q$, and hence $\mathbb{Q}(\zeta_q)$, is disjoint from all these $L_m$. This leads to

$$M'(x, y; q) \leqq \frac{\delta'(y)}{q-1}\,li\,x + O(x^{1/2}\log qx)\,,$$

for $q$ sufficiently large, and using the fact that

$$\sum_{x^{1/4}/\log x < q < x^{1/2}/\log^2 x} \frac{1}{q-1} \sim \log\log(x^{1/2}/\log^2 x) - \log\log(x^{1/4}/\log x) \sim \log 2\,,$$

we obtain the estimate

$$M(x, x^{1/4}/\log x, x^{1/2}/\log^2 x) \leqq (1 - \log 2 - \varepsilon)\delta'(\Gamma)\,li\,x$$

for $x$ sufficiently large. To handle the remaining interval $M(x, x^{1/2}/\log^2 x, x^{1/2}\log x)$, we use the Brun-Titchmarsh theorem (see [4]). Since if $q|[\bar{E}(\mathbb{F}_p):\Gamma_p]$ then $p \equiv 1 \bmod q$, we have

$$M(x, x^{1/2}/\log^2 x, x^{1/2}\log x) \ll \sum_{x^{1/2}/\log^2 x < q < x^{1/2}\log x} \frac{x}{q\log(x/q)}\,,$$

which is easily seen to be $o(x/\log x)$. This completes the proof of Theorem 2.

*Proof of Theorem 3.* The proof is very similar to that given above, so we give only a sketch. One does an initial sieve as before and obtains a bound

$$M(x, y, x^{1/4}/\log x) = o(x/\log x)\,,$$

and since $r(\Gamma) \geqq 6$, Lemma 14 of [3] yields

$$M(x, x^{1/4} \log x) = o(x/\log x) .$$

The remaining interval is handled as above using the Brun-Titchmarsh theorem for inert primes and a generalization of it to number fields for primes which split in $k$, as in [3].

## 5. Generation of $\bar{E}(\mathbb{F}_p)$ in the non-CM case

We now suppose that $E$ does not have CM, and ask how often $\bar{E}(\mathbb{F}_p) = \Gamma_p$. If $p \nmid q\Delta$, then we have as before that $q|[\bar{E}(\mathbb{F}_p):\Gamma_p]$ if and only if $\sigma_q(p) \subset C_q$, where $C_q$ is a conjugacy subset of $G_q = \mathrm{Gal}(L_q/\mathbb{Q})$, and $L_q = \mathbb{Q}(E[q], \frac{1}{q}\Gamma)$, but in this case, the sizes of $G_q$ and $C_q$ are bigger; we have:

**Lemma 6.** *We have* $|G_q| \asymp q^{2r(\Gamma)+4}$ *and* $|C_q| \asymp q^{r(\Gamma)+3}$.

*Proof.* See [3], p. 35. The difference from Lemma 4 arises from the fact that the Galois group of $\mathbb{Q}(E[q])/\mathbb{Q}$ is almost always $GL_2(\mathbb{Z}/q\mathbb{Z})$.

We expect $S(\Gamma)$ to have density $\delta(\Gamma)$, where $\delta(\Gamma)$ is as in section 4. Because of the large size of the conjugacy sets involved and the resulting worsening of the error terms in the Chebotarev density theorem, one can only prove this in case $r(\Gamma) \geqq 18$, under the GRH (see [3]). Using the improved error term of [12], one can improve this to $r(\Gamma) \geqq 11$, under the assumption of Artin's holomorphy conjecture.

We are able to bring the rank down even further by not insisting on producing a set of density $\delta(\Gamma)$ but rather a positive multiple of it, as we did in section 3.

*Proof of Theorem 4.* We will use the same notation as in the proof of Theorem 2. For $r(\Gamma) \geqq 7$, we are able to handle $M(x, x^{2/9+\varepsilon}, 2x)$ using Lemma 14 of [3], and after doing an initial sieve as before, are left with having to estimate $M(x, y, x^{2/9+\varepsilon})$, where $y \to \infty$ as $x \to \infty$. We instead estimate $\tilde{M}(x, y, x^{1/4+\varepsilon})$, corresponding to a rank-one subgroup $\tilde{\Gamma}$ of $\Gamma$. Using Proposition 2, one can show under the GRH that

$$\tilde{M}(x, y, x^{1/10-\varepsilon}) = o(x/\log x) ,$$

since the size of the conjugacy class involved is $\asymp q^4$ by Lemma 6, and hence the error terms are essentially $O(q^4 x^{1/2})$. One must use the fact, which is proved as in [3, Lemma 7], that $d_{\tilde{L}_n} \ll [\tilde{L}_n:\mathbb{Q}]\log n$. Under the additional assumption of Artin's holomorphy conjecture, one can show using Proposition 2 that

$$\tilde{M}(x, y, x^{1/6-\varepsilon}) = o(x/\log x) .$$

To estimate the remaining portion of the tail, we impose the condition $q|[\bar{E}(\mathbb{F}_p):\tilde{\Gamma}_p]$ into the initial sieve. Letting $m$ be a square-free integer all of whose prime factors are $\leqq y$, we proceed to estimate the number of primes $p$ for which $\sigma_m(p) \subset C_m$ and $q|[\bar{E}(\mathbb{F}_p):\tilde{\Gamma}_p]$. Let $F_q$ be the (non-Galois) extension of $\mathbb{Q}$ of degree $q^2$ obtained by adjoining to $\mathbb{Q}$ some value of $\frac{1}{q}X$, where $X$ is a generator of $\tilde{\Gamma}$. From [3], $p$ has $q$ first degree primes above it in $F_q$ or splits completely in $\mathbb{Q}(E[q])$. The latter condition has the effect of introducing essentially $q^4$ (the degree of $\mathbb{Q}(E[q])$

over $\mathbb{Q}$) into the denominator of the main term and only a factor of $\log q$ into the error term. Also, applying Proposition 2 to the Galois extension $F_qL_m/F_q$, with the conjugacy set $C_m^*$ which is the extension of $C_m$, we get the following estimate for the number of first-degree primes of $F_q$ with norm $\leqq x$ and whose Frobenius symbol lies in $C_m^*$:

$$\frac{|C_m|}{|G_m|} li\, x + O(|C_m| q^2 x^{1/2} \log mqx) .$$

Here we have used the estimates

$$d_{L_m} \ll [L_m:\mathbb{Q}]\log m,\ d_{F_q} \ll [F_q:\mathbb{Q}]\log q ,$$

which can be easily proved as in [3] because of the limited ramification in these fields. Using the same notation as before, we conclude that

$$M(x, x^\alpha, x^{2/9+\varepsilon}) \leqq \delta(\Gamma) \sum_{x^\alpha < q < x^{2/9+\varepsilon}} \left(\frac{1}{q} + \frac{1}{q^4}\right) li\, x + O(|C_m| q x^{1/2} \log mqx) .$$

Choosing $y$ sufficiently small but still tending to $\infty$ (e.g. $y = c \log\log x$), and using

$$\sum_{x^\alpha < q < x^{2/9+\varepsilon}} \frac{1}{q} \sim \log \frac{2/9 + \varepsilon}{\alpha} ,$$

with $\alpha = 1/10 - \varepsilon$ or $1/6 - \varepsilon$, we obtain the desired result.

## 6. Concluding remarks

If $E$ is an elliptic curve over a number field $K$, then one can still ask the question of how often $E(F_v)$ is cyclic where $v$ is a prime ideal of $K$. The method of proof of Theorem 1 requires a corresponding sieve result. More precisely, we need to know that primes that split completely in $K$ are well-distributed in arithmetic progressions. If $K$ is an abelian extension of $\mathbb{Q}$, this amounts to putting additional congruence conditions on the primes so that the theorem of Fouvry and Iwaniec of sieve theory can be employed without alteration. Hence, if $K$ is abelian over $\mathbb{Q}$, then there are at least $\gg x/\log^2 x$ prime ideals $v$ of $K$ such that $\mathrm{Norm}(v) \leqq x$ and $E(F_v)$ is cyclic, provided $E[q] \not\subset E(K)$ for any prime $q$. However, if $K$ is not abelian over $\mathbb{Q}$, one would have to introduce non-abelian conditions into the sieve theorem of Fouvry and Iwaniec. This has been done for the classical theorem of Bombieri and Vinogradov (see [11]). But this would only produce primes $p$ of the desired type such that all the odd prime factors of $p - 1$ are $\gg p^{1/4-\varepsilon}$. This is not sufficient for our needs since the fact that the exponent is $> 1/4$ was crucial to our argument.

## References

1. Fouvry, E., Iwaniec, H.: Primes in arithmetic progression. Acta Arith. **42**, 197–218 (1983)
2. Gupta, R., Murty, M.R.: A remark on Artin's conjecture. Invent. Math. **78**, 127–130 (1984)
3. Gupta, R., Murty, M.R.: Primitive points on elliptic curves. Compos. Math. **58**, 13–44 (1986)

4. Halberstam, H., Richert, H.E.: Sieve Methods. London Mathematical Society Monographs No. 4. New York: Academic Press 1975
5. Heath-Brown, D.R.: Artin's conjecture for primitive roots. Q. J. Math., Oxf. II. Ser. **37**, 27–38 (1986)
6. Hooley, C.: On Artin's conjecture. J. Reine Angew. Math. **225**, 209–220 (1967)
7. Lagarias, J., Odlyzko, A.: Effective versions of the Chebotarev density theorem. In: Algebraic Number Fields Fröhlich, A. (ed.). New York: Academic Press 1977, pp. 409–464
8. Lang, S., Trotter, H.: Primitive points on elliptic curves. Bull. Am. Math. Soc. **83**, 289–292 (1977)
9. Murty, M.R.: On Artin's conjecture. J. Number Theory **16**, 147–168 (1983)
10. Murty, M.R.: On the supersingular reduction of elliptic curves. Proc. Indian Acad. Sci., Math. Sci. **97**, 247–250 (1987)
11. Murty, M.R., Murty, V.K.: A variant of the Bombieri-Vinogradov theorem. In: Conference Proceedings of the CMS Vol. 7 (1987), AMS publication
12. Murty, M.R., Murty, V.K., Saradha, N.: Modular forms and the Chebotarev density theorem. Am. J. Math. **110**, 253–281 (1988)
13. Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15**, 259–331 (1972)
14. Serre, J.-P.: Resumé de cours (1977). See: Oeuvres. Berlin-Heidelberg-New York: Springer 1986
15. Serre, J.-P.: Linear Representations of Finite Groups. Berlin-Heidelberg-New York: Springer 1977
16. Silverman, J.: The Arithmetic of Elliptic Curves. Berlin-Heidelberg-New York: Springer 1986

Oblatum 14-VII-1989 & 7-XI-1989