ACTA ARITHMETICA
117.4 (2005)

On the number of prime divisors of the order of elliptic curves modulo p

by

Jörn Steuding (Madrid) and Annegret Weng (Mainz)

1. Introduction and statement of results. Let E be an elliptic curve defined over $\mathbb{Q}$. Throughout this paper p denotes a prime number and $\mathbb{F}_p$ is the finite prime field with p elements. Let N_p count the number of points on the curve $\overline{E}(\mathbb{F}_p)$, i.e. the curve $\overline{E} := E$ modulo p. Koblitz [6] conjectured that

$$\#\{p \le N : N_p \text{ is prime}\} \sim C_E \frac{N}{(\log N)^2},$$

where C_E is a positive computable constant depending on E. The motivation for this question comes from applications of elliptic curves in cryptography; see [5], [9]. In cryptosystems based on the discrete logarithm problem we are interested in elliptic curves having a group order which is as prime as possible.

By Selberg's parity phenomenon (see [1]) we know that sieve methods alone cannot detect primes, but almost prime numbers, i.e. numbers with *few* prime divisors only. Let $\Omega(n)$ and $\nu(n)$ count the number of prime divisors of an integer n with and without multiplicities, respectively. Assuming the Generalized Riemann Hypothesis (GRH), i.e. the non-vanishing of all Dedekind zeta-functions $\zeta_K(s)$ of number fields K for $\operatorname{Re} s > 1/2$, V. K. Murty and Miri [10] proved that *if E does not have complex multiplication (CM) and has a trivial torsion group over $\mathbb{Q}$, then*

$$\Omega(N_p) \le 16 \text{ for more than } \gg \frac{N}{(\log N)^2} \text{ primes } p \le N;$$

their method relies on Selberg's sieve identity (see [1]). We shall use the linear sieve with logarithmic weights. Introducing weights into the sifting process increases the power of sieve methods in various results. However, the use of weight functions leads without knowledge on the distribution of squarefull numbers in the sifted sequence only to results about the number

2000 *Mathematics Subject Classification*: 11N36, 14H52.
Key words and phrases: linear sieve with weights, group order of elliptic curves.

of prime divisors without multiplicities. In almost all examples of interesting sequences in sieve theory the set of squarefull numbers is sufficiently thin such that the squarefull numbers give no significant contribution. Unfortunately, for the sequence of the N_p nothing is known in that direction.

Moreover, we use refinements of the explicit version of Chebotarev's theorem due to Serre and to M. R. Murty, V. K. Murty and Saradha to prove

THEOREM 1. *Let E be an elliptic curve over $\mathbb{Q}$ such that the finitely many elliptic curves E', $\mathbb{Q}$-isogenous to E, have trivial $\mathbb{Q}$-torsion group. Assume GRH. Then*:

(i) *If E does not have CM, then*

$$\#\{p \le N : \nu(N_p) \le 5\} \ge C_1 \frac{N}{(\log N)^2}, \tag{1}$$

where C_1 is a positive computable constant depending on E; the inequality for $\nu(N_p)$ can be replaced by $\Omega(N_p) \le 8$.

(ii) *If E has CM by an order $\mathcal{O}$ in an imaginary quadratic field and χ is the corresponding quadratic character, then*

$$\#\{p \le N : \chi(p) = 1,\ \Omega(N_p) \le 3\} \ge C_2 \frac{N}{(\log N)^2}, \tag{2}$$

where C_2 is a positive computable constant depending on E.

As far as we know, Theorem 1 gives the best theoretical result. In practice there seem to be enough curves with the property that N_p is prime sufficiently often [6].

Note that M. R. Murty and V. K. Murty [11] proved under assumption of the truth of GRH the Turán–Kubilius type inequality

$$\sum_{p \le x} (\nu(N_p) - \log\log p)^2 \ll \pi(x) \log\log x,$$

which implies that the mean-value of the number of prime divisors of N_p is $\log\log p$.

2. The explicit version of Chebotarev's density theorem. The proof of the theorem relies beneath the sieve-theoretical part mainly on the distribution of prime numbers and the distribution of the orders N_p, which is ruled by Chebotarev's density theorem. Assuming GRH, we have the prime number theorem

$$\pi(x) = \operatorname{Li} x + O(x^{1/2} \log x), \quad \text{where} \quad \operatorname{Li} x := \int_2^x \frac{du}{\log u},$$

and $\pi(x)$ counts the number of primes $p \le x$. Furthermore, let K be a number field of degree n_K over $\mathbb{Q}$ and L be a finite Galois extension of K

with discriminant d_L. For each prime ideal $\mathfrak{P}$ in L write $D_{\mathfrak{P}}$ and $I_{\mathfrak{P}}$ for the decomposition and inertia group at $\mathfrak{P}$, respectively. Let $\sigma_{\mathfrak{P}} \in D_{\mathfrak{P}}/I_{\mathfrak{P}}$ be the Frobenius element at $\mathfrak{P}$. If $\mathfrak{P}$ above $\mathfrak{p}$ is unramified in L/K, then $I_{\mathfrak{P}}$ is trivial and the conjugacy class of $\sigma_{\mathfrak{P}}$ is given by the Artin symbol $\sigma_{\mathfrak{p}} := \left[\frac{L/K}{\mathfrak{p}}\right]$. Now let G be the Galois group of L over K and let C be a subset of G, closed under conjugation, and write $\pi_C(x)$ for the number of prime ideals $\mathfrak{p}$ of K, unramified in L, for which $\left[\frac{L/K}{\mathfrak{p}}\right] \subseteq C$ and $N_{K/\mathbb{Q}}\mathfrak{p} \le x$. Then, assuming GRH, Chebotarev's density theorem, in the effective form proved by Lagarias and Odlyzko [7], states

$$\pi_C(x) = \frac{\#C}{\#G}\,\pi_K(x) + O\Big(\frac{\#C}{\#G}\,x^{1/2}(\log d_L + n_L \log x)\Big), \tag{3}$$

where $\pi_K(x)$ counts the number of prime ideals in K of norm $\le x$, d_L is the absolute value of the discriminant of L, and $n_L = [L:\mathbb{Q}]$; note that the implied constant is absolute.

The explicit version of Chebotarev's density theorem can be further improved in particular cases as pointed out by Serre in [14]. Let φ be a class function on G and set

$$\pi_\varphi(x) = \sum_{\substack{N\mathfrak{p}\le x\\ \mathfrak{p}\text{ unramified in } L/K}} \varphi(\sigma_{\mathfrak{p}}).$$

If φ is equal to the characteristic function δ_C of a conjugacy class C, we have $\pi_\varphi(x) = \pi_C(x)$. We further define

$$\widetilde{\pi}_\varphi(x) = \sum_{N\mathfrak{p}^m \le x} \frac{1}{m}\,\varphi(\sigma_{\mathfrak{p}}^m),$$

where we have to explain the meaning of $\varphi(\sigma_{\mathfrak{p}}^m)$ for the ramified primes. For a prime ideal $\mathfrak{p}$ which ramifies in L/K, define

$$\varphi(\sigma_{\mathfrak{p}}^m) = \frac{1}{\#I_{\mathfrak{P}}} \sum \varphi(g)$$

where $I_{\mathfrak{P}}$ is the inertia group at a prime $\mathfrak{P} \in L$, $\mathfrak{P} \mid \mathfrak{p}$, and the sum is taken over all $g \in D_{\mathfrak{P}}$ whose image in $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ maps to $\sigma_{\mathfrak{p}}^m$.

The functions $\pi_\varphi(x)$ and $\widetilde{\pi}_\varphi(x)$ are closely related:

$$\pi_\varphi(x) = \widetilde{\pi}_\varphi(x) + O\Big(\sup_{g\in G}|\varphi(g)|\Big(\frac{1}{\#G}\log d_L + n_K x^{1/2}\Big)\Big), \tag{4}$$

where the O-constant is absolute. Suppose that φ_H is a class function on a subgroup $H \subseteq G$ and φ is a class function on G with $\varphi = \mathrm{Ind}_H^G \varphi_H$. Then $\widetilde{\pi}_\varphi(x) = \widetilde{\pi}_{\varphi_H}(x)$.

Now given a conjugacy class C and a subgroup H of G with $C \cap H \neq \emptyset$, let C_H be the conjugacy class of $C \cap H$ in H. We set

$$m_{C_H} = \frac{\#C}{\#C_H} \cdot \frac{\#H}{\#G} \qquad \text{and} \qquad \varphi_{H,C}(x) = \begin{cases} m_{C_H} & \text{for } x \in C, \\ 0 & \text{otherwise.} \end{cases}$$

We then have

$$\varphi_C = \operatorname{Ind}_H^G \varphi_{H,C}.$$

On the other hand, φ_H is the m_{C_H}th multiple of the indicator function of C_H on H. Hence,

$$\widetilde{\pi}_{\varphi_C}(x) = \widetilde{\pi}_{\varphi_{H,C}}(x) = m_{C_H} \widetilde{\pi}_{\varphi_{C_H}}(x).$$

If the error term in (4) is negligible we may replace π_C by $m_{C_H} \pi_{C_H}$.

Moreover, we shall use the following theorem due to M. R. Murty, V. K. Murty and N. Saradha [13]. Define

$$M(L/K) = [L : K] d_K^{1/n_K} \prod_{p \in P(L/K)} p,$$

where $P(L/K)$ is the set of primes in K which ramify in L. Then

LEMMA 2. *Assume GRH. Let D be a non-empty union of conjugacy classes in G.*

(i) *If Artin's conjecture is true for the irreducible characters of G, then*

$$\pi_D(x) = \frac{\#D}{\#G} \operatorname{Li} x + O((\#D)^{1/2} x^{1/2} n_K \log(xM(L/K))).$$

(ii) *Let H be a normal subgroup of G such that Artin's conjecture is true for the irreducible characters of G/H, and $HD \subseteq D$. Then*

$$\pi_D(x) = \frac{\#D}{\#G} \operatorname{Li} x + O\left(\left(\frac{\#D}{\#H} \right)^{1/2} x^{1/2} n_K \log(xM(L/K)) \right).$$

3. Applying Chebotarev's theorem to elliptic curves. Let E be a fixed elliptic curve over $\mathbb{Q}$ with conductor N_E and ℓ be a prime number. The Galois group G_ℓ of the Galois extension $\mathbb{Q}(E[\ell])/\mathbb{Q}$ obtained by adjoining all ℓ-torsion points $E[\ell]$ defined over the algebraic closure $\overline{\mathbb{Q}}$ acts on the 2-dimensional $\mathbb{F}_\ell$-vector space $E[\ell]$. Let $p \neq \ell$ be a prime for which E has good reduction. Then p is unramified in the extension $\mathbb{Q}(E[\ell])/\mathbb{Q}$. The group order of the elliptic curve modulo p is divisible by ℓ if and only if the Frobenius $\sigma_{\mathfrak{P}}$ of every $\mathfrak{P} \,|\, p$ corresponds to an element $\sigma \in G_\ell$ fixing at least a subspace of dimension one of $E[\ell]$.

Serre [15] proved that if E does not have CM, then $G_\ell \simeq \mathrm{Gl}(2, \mathbb{F}_\ell)$ and $G_{\ell^2} \simeq \mathrm{Gl}(2, \mathbb{Z}/\ell^2\mathbb{Z})$ for all but finitely many ℓ. Let L' be the finite set of exceptional primes with $G_\ell \not\simeq \mathrm{Gl}(2, \mathbb{F}_\ell)$.

Suppose $G_\ell = \mathrm{Gl}(2, \mathbb{F}_\ell)$. Then we have

$$\begin{aligned}\pi_E(x,\ell) &= \#\{p \le x : p \nmid \ell \cdot N_E, N_p \equiv 0 \bmod \ell\} \\ &= \#\{p \le x : p \nmid \ell \cdot N_E, \sigma_{\mathfrak{P}} \text{ has eigenvalue one for all } \mathfrak{P} \mid p\} = \pi_D(x),\end{aligned}$$

where D is the set of conjugacy classes of matrices in G with at least one eigenvalue equal to one. We now want to apply the explicit Chebotarev theorem to compute $\pi_D(x)$. For that we use an argument similar to the one used in [13, Section 4]. Firstly, we consider the Borel subgroup B of upper triangular matrices in G_ℓ. Let M be the field fixed by B with

$$d_M = [M : \mathbb{Q}] = [G : B] = \ell + O(1).$$

Denote by D_B the set of conjugacy classes of matrices in B with at least one eigenvalue equal to one.

The subgroup U of unipotent matrices in B is normal and B/U is abelian. Hence, Artin's conjecture holds. Since $UD_B \subseteq D_B$ we may apply the second assertion of Lemma 2. This leads to

$$\pi_{D_B}(x) = \frac{\#D_B}{\#B} \operatorname{Li} x + O(\ell^{3/2} x^{1/2} \log(\ell N_E x)).$$

For a single conjugacy class C in D the intersection $C \cap B$ is non-empty and we have

$$\widetilde{\pi}_\varphi(x) - \pi_\varphi(x) \ll \ell x^{1/2} + \ell \log(\ell N_E x)$$

for both $\varphi = \varphi_{B,D}$ and $\varphi = \delta_D$ (with the notation introduced in Section 2). Using the explicit version of Chebotarev's theorem as explained in Section 2, we may replace π_D by $m_{D_H}\pi_{D_H}$ to get

$$\begin{aligned}\pi_D(x) &= m_{D_H}\pi_{D_H}(x) + O(\ell x^{1/2} + \ell \log(\ell N_E)) \\ &= \frac{1}{\delta(\ell)} \operatorname{Li} x + O(\ell^{3/2} x^{1/2} \log(\ell N_E x)),\end{aligned}$$

where

$$\delta(\ell) := \frac{\#G}{\#D}.$$

Note that for $\ell \notin L'$ we have

$$\delta(\ell) = \frac{(\ell-1)(\ell^2-1)}{\ell^2-2}.$$

The function δ is multiplicative. Hence

$$\begin{aligned}\pi_E(x,d) &= \#\{p \le x : p \nmid d \cdot N_E,\ N_p \equiv 0 \bmod d\} \\ &= \frac{1}{\delta(d)} \operatorname{Li} x + O(d^{3/2} x^{1/2} \log(d N_E x))\end{aligned} \tag{5}$$

for squarefree d.

Later we will also be interested in the number of squarefull N_p, i.e. in the number $\pi_E(x, \ell^2)$. In this case we need to consider the group $\mathrm{Gl}(2, \mathbb{Z}/\ell^2\mathbb{Z})$.

Following the same reasoning as above we get

$$\pi_E(x,\ell^2) = \#\{p \le x : p \nmid \ell \cdot N_E,\ N_p \equiv 0 \bmod \ell^2\} = \frac{\#D'}{\#\operatorname{Gl}(2,\mathbb{Z}/\ell^2\mathbb{Z})} \operatorname{Li} x + O(\ell^3 x^{1/2} \log(\ell N_E x)) \tag{6}$$

where D' is the set of conjugacy classes of those matrices in $\operatorname{Gl}(2,\mathbb{Z}/\ell^2\mathbb{Z})$ which either have an eigenvalue one or are the identity on $E[\ell]$. By a simple counting argument,

$$\frac{\#D'}{\#\operatorname{Gl}(2,\mathbb{Z}/\ell^2\mathbb{Z})} = \frac{1}{\ell^2} + O\left(\frac{1}{\ell^3}\right).$$

If E has CM by an order $\mathcal{O}$ in some imaginary quadratic field, we distinguish two classes of primes: supersingular primes (which are inert or ramified in $\mathcal{O}$, i.e., $\chi(p) = 0, -1$) and ordinary primes (which split in $\mathcal{O}$, $\chi(p) = 1$); see [8]. Note that we automatically have class number one: $h(\mathcal{O}) = 1$, since E is defined over $\mathbb{Q}$.

For the supersingular primes, N_p is given by a linear polynomial in p, namely $p+1$. Such problems have already been considered in the literature and it can be shown that $\nu(p+1) \le 4$ for infinitely many p (see [2]).

We concentrate on the more interesting case where p splits. Let $\pi(x,1)$ be the number of primes $p \le x$ with $\chi(p) = 1$ and let

$$\pi_E(x,1,d) = \#\{p \le x : \chi(p) = 1,\ N_p \equiv 0 \bmod d\}.$$

For a curve with CM we have $G_\ell \simeq (\mathcal{O}/\ell\mathcal{O})^*$ for all but finitely many ℓ; see [17]. As above, the set L' contains the exceptional primes. For these primes, G_ℓ is a subgroup of $(\mathcal{O}/\ell\mathcal{O})^*$. The fact that the Galois group G_ℓ is smaller in the CM case leads to better error terms and hence to slightly better results. Setting

$$\delta(\ell) = \begin{cases} \ell^2 - 1 & \text{if } \ell \text{ is inert,} \\ \dfrac{(\ell-1)^2}{2\ell - 3} & \text{if } \ell \text{ splits,} \\ \ell - 1 & \text{if } \ell \text{ is ramified,} \end{cases} \tag{7}$$

and applying the first assertion of Lemma 2 under assumption of GRH, we get

$$\pi_E(x,1,d) = \frac{1}{2\delta(d)} \operatorname{Li} x + O(d^{1/2} x^{1/2} \log(dx)) \tag{8}$$

for squarefree d (since Artin's conjecture is known to be true for abelian G).

Next we consider the numbers N_p that are divisible by a square of a prime ℓ. For all but finitely many primes ℓ that split in $\mathcal{O}$ we have

$$\operatorname{Gal}(\mathbb{Q}(E[\ell^2])/\mathbb{Q}) \simeq (\mathcal{O}/\ell^2\mathcal{O})^* \simeq (\mathbb{Z}/\ell^2\mathbb{Z})^* \times (\mathbb{Z}/\ell^2\mathbb{Z})^*.$$

Let P_1, P_2 be a $\mathbb{Z}/\ell^2\mathbb{Z}$-basis for the ℓ^2-division points on $E(\overline{\mathbb{Q}})$. In this special case the field extensions $\mathbb{Q}(P_i)/\mathbb{Q}$ are Galois with Galois group G_{P_i} isomorphic to $(\mathbb{Z}/\ell^2\mathbb{Z})^*$. Now an elliptic curve over $\mathbb{F}_p$ with $\chi(p) = 1$ has group order divisible by ℓ^2 if one of the following three cases occurs: the Frobenius of p in G_{P_1} is the identity, the Frobenius of p in G_{P_2} is the identity or is the Frobenius of p in G_ℓ. In all three cases we obtain under assumption of GRH

$$\pi_E(x, \ell^2) = \frac{\#D'}{\#G_{\ell^2}} \operatorname{Li} x + O(x^{1/2} \log(\ell x)) \tag{9}$$

where D' is the set of conjugacy classes of elements in G_{ℓ^2} which either acts trivially on the ℓ-torsion points or fixes an ℓ^2-torsion point. Again, by a simple counting argument, we have

$$\frac{\#D'}{\#G_{\ell^2}} = \frac{1}{\ell^2} + O\bigg(\frac{1}{\ell^3}\bigg).$$

4. Sifting the group orders. Below, let ℓ_j denote prime numbers. We follow the notation of [2].

First, assume that E does not have CM. We have $\delta(\ell) = \ell + O(1)$ for all but finitely many primes ℓ. Since $E'_{\mathrm{tors}}(\mathbb{Q})$ is trivial for all $\mathbb{Q}$-isogenous curves, the set of primes p with $N_p \not\equiv 0 \bmod \ell$ has positive density for all ℓ (see [4]). Hence, there exists a constant $\mu > 1$ such that $\delta(\ell) \geq \mu$ for all ℓ. Setting $\omega(\ell) = \ell/\delta(\ell)$, we see that

$$0 \leq \frac{\omega(\ell)}{\ell} \leq \frac{1}{\mu} < 1.$$

This shows that axiom Ω_1 of [2] holds. Furthermore,

$$\sum_{w \leq \ell < z} \frac{\omega(\ell) \log \ell}{\ell} = \sum_{w \leq \ell < z} \frac{\log \ell}{\ell} + O(1) = \log \frac{z}{w} + O(1)$$

by Mertens' theorem (see [3]), and hence, axiom $\Omega_2(1, L)$ of [2] is satisfied. Now let $X = \pi(N)$. In view of (5), under assumption of GRH,

$$R_d := \pi_E(N, d) - \frac{1}{\delta(d)} \operatorname{Li} N \ll d^{3/2} N^{1/2} \log(dN).$$

Note that

$$3^{\nu(d)} = 2^{\nu(d) \log 3/\log 2} \leq \tau(d)^{\log 3/\log 2},$$

where $\tau(d)$ is the divisor function (i.e., the number of positive divisors of d). Since $\tau(d) \ll d^\varepsilon$ (see [3]), we obtain

$$\sum_{d < X^\alpha} \mu(d)^2 3^{\nu(d)} |R_d| \ll N^{1/2+\varepsilon} \sum_{d < X^\alpha} d^{3/2+\varepsilon} \ll N^{1/2+5\alpha/2+\varepsilon},$$

which is $o(X/\log X)$ for $\alpha < 1/5$. Thus, for each of these values axiom $R(1, \alpha)$ of [2] is satisfied.

Later we shall prove the inequality

$$\#\{p \le N : \nu(N_p) \le r\} \ge \mathcal{W}(u,v,\lambda) \tag{10}$$

with the sifting function

$$\mathcal{W}(u,v,\lambda) := \sum_{\substack{p\le N\\ (N_p,P(X^{1/v}))=1}} \left\{1-\lambda \sum_{\substack{X^{1/v}\le \ell_1<X^{1/u}\\ \ell_1\mid N_p}} \left(1-u\,\frac{\log \ell_1}{\log X}\right)\right\}, \tag{11}$$

where $P(z) := \prod_{\ell<z}\ell$ and u, v, λ are certain positive constants, depending on r and α, which will be specified soon. We are interested in the minimal value for r such that the sifting function can be bounded below by a quantity as in (1).

Define

$$W(z) = \prod_{\ell<z}\left(1-\frac{\omega(\ell)}{\ell}\right) = \prod_{\ell<z}\left(1-\frac{1}{\delta(\ell)}\right).$$

Then, by Theorem 9.1 and Lemma 9.1 of [2],

$$\mathcal{W}(u,v,\lambda) \ge XW(X^{1/v})\{f(u,v,\lambda,\alpha) + O((\log X)^{-1/14})\}$$

for

$$\frac{1}{\alpha} < u < v, \quad \frac{2}{\alpha} \le v \le \frac{4}{\alpha}, \quad 0 < \lambda \ll 1, \tag{12}$$

where

$$f(u,v,\lambda,\alpha) := \frac{2e^{\gamma}}{\alpha v}\left(\log(\alpha v-1) - \lambda\alpha u \log\frac{v}{u} + \lambda(\alpha u-1)\log\frac{\alpha v-1}{\alpha u-1}\right),$$

and where $\gamma = 0.577\ldots$ is the Euler–Mascheroni constant. A simple computation shows

$$W(z) = \prod_{\ell\in L',\,\ell<z} c_\ell \prod_{\ell\notin L',\,\ell<z}\left(1-\frac{1}{\ell}\right)\left(1-\frac{\ell^2-\ell-1}{(\ell-1)^3(\ell+1)}\right),$$

where

$$c_\ell = \frac{\delta(\ell)-1}{\delta(\ell)}\cdot\frac{(\ell-1)^2(\ell+1)}{\ell^3-2\ell^2-\ell+3}.$$

Note that Mertens' theorem gives

$$\prod_{\ell<z}\left(1-\frac{1}{\ell}\right) = \frac{e^{-\gamma}}{\log z} + O(1).$$

This leads to the main term of the theorem up to a factor depending on u, v and λ if $f(u,v,\lambda,\alpha) > 0$. It remains to prove inequality (10) and to determine r with some positive $f(u,v,\lambda,\alpha)$.

In (10), p is counted with weight 1 if and only if N_p has no prime divisors $< X^{1/u}$, i.e.

$$\Omega(N_p) \le [u], \tag{13}$$

where $[u]$ denotes the largest integer $\le u$. Now suppose that p gives a positive contribution

$$1-\lambda \sum_{\substack{X^{1/v}\le \ell_1<X^{1/u}\\ \ell_1\mid N_p}} \left(1-u\,\frac{\log \ell_1}{\log X}\right)$$

in (11), but less than 1. Clearly, N_p may have prime divisors $\ell_2 \ge X^{1/u}$, but for each of these

$$1-u\,\frac{\log \ell_2}{\log X} \le 1-u\,\frac{\log X^{1/u}}{\log X}=0.$$

Hence, N_p is counted with weight at most

$$1-\lambda\left(\nu(N_p)-u\,\frac{\log N_p}{\log X}\right).$$

Now assume that $\nu(N_p)=r+1$ for which

$$1-\lambda\left(r+1-u\,\frac{\log N_p}{\log X}\right)\le 0,$$

that is,

$$r \ge u\,\frac{\log N_p}{\log X}+\frac{1}{\lambda}-1.$$

In view of the Hasse bound (see [16])

$$|N_p-p-1|\le 2\sqrt{p},$$

for $p \gg N$ we obtain

$$r \ge u+\frac{1}{\lambda}-1.$$

Then putting

$$r=\max\{[u-1+1/\lambda],[u]\} \tag{14}$$

covers condition (13). It remains to find suitable parameters u, v, λ for which condition (11) is satisfied and which give a positive value for $f(u,v,\lambda,\alpha)$. We are not interested in the best possible constants in (1) and (2). For instance,

$$f(5.1, 20, 0.53, 1/5.05)=0.34522\ldots,$$

which yields $r=[5.98679\ldots]=5$. This proves (1).

If we want to replace $\nu(N_p)$ by $\Omega(N_p)$, we have to set aside those primes p counted in (11) for which N_p is divisible by a square of a prime ℓ_1 satisfying $X^{1/v}\le \ell_1 < X^{1/u}$. Using (6) we get

$$\begin{aligned}\#\{p \le N : \ell_1^2 \,|\, N_p \text{ with } X^{1/v} \le \ell_1 < X^{1/u}\} \\ = \sum_{X^{1/v} \le \ell_1 < X^{1/u}} \#\{p \le N : \ell_1^2 \,|\, N_p\} \\ \ll \frac{N}{\log N} \sum_{X^{1/v} \le \ell_1 < X^{1/u}} \frac{1}{\ell_1^2} + X^{1/2+\varepsilon} \sum_{X^{1/v} \le \ell_1 < X^{1/u}} \ell_1^3 = o\bigg(\frac{N}{(\log N)^2}\bigg)\end{aligned}$$

provided that $8 < u$. Since $f(8.1, 32, 0.53, 1/8.05) = 0.33867\ldots$ we get here $r = [8.98679\ldots] = 8$ in (14), which proves the Ω-result in the non-CM case under assumption of GRH.

Now assume that E has CM. The proof runs analogously to the non-CM case. We only point out the differences. If the discriminant of the imaginary quadratic order is $\not\equiv 5 \bmod 8$, it can easily be checked that the curve always has non-trivial 2-torsion points. Since $E'_{\mathrm{tors}}(\mathbb{Q})$ is trivial for all $\mathbb{Q}$-isogenous curves, the discriminant of the endomorphism ring has to be $\equiv 5 \bmod 8$, and by (7) we have

$$0 \le \frac{\omega(\ell)}{\ell} \le \frac{1}{\mu} < 1$$

for all primes. This shows that axiom Ω_1 of [2] holds; the verification of the axiom $\Omega_2(1, L)$ of [2] follows as in the non-CM case. Put $X = \frac{1}{2}\operatorname{Li} N$. By (3) we have

$$\#\{p \le N : \chi(p) = 1\} - X \ll N^{1/2} \log N.$$

Using (8) we get for d squarefree

$$R_d = \pi_E(N, 1, d) - \frac{1}{2\delta(d)} \operatorname{Li} N \ll d^{1/2} N^{1/2} \log(dN),$$

and therefore

$$\sum_{d < X^\alpha} \mu(d)^2 3^{\nu(d)} |R_d| = o\bigg(\frac{X}{\log X}\bigg)$$

for $\alpha < 1/3$. For the correction term we get

$$\prod_{\ell \in L',\, \ell < X^{1/v}} c_\ell \prod_{\substack{\ell < X^{1/v} \\ \chi(\ell) = 0}} \bigg(1 - \frac{1}{(\ell-1)^2}\bigg) \prod_{\substack{\ell < X^{1/v} \\ \chi(\ell) \ne 0}} \bigg(1 - \chi(\ell)\,\frac{\ell^2 - \ell - 1}{(\ell - \chi(\ell))(\ell-1)^2}\bigg).$$

For the numbers N_p that are divisible by a square of a prime ℓ_1, satisfying $X^{1/v} \le \ell_1 < X^{1/u}$, in view of (9) we get

$$\begin{aligned}\#\{p \le N : \ell_1^2 \,|\, N_p \text{ with } X^{1/v} \le \ell_1 < X^{1/u}\} \\ \ll \frac{N}{\log N} \sum_{X^{1/v} \le \ell_1 < X^{1/u}} \frac{1}{\ell_1^2} + X^{1/2+\varepsilon} \sum_{X^{1/v} \le \ell_1 < X^{1/u}} 1,\end{aligned}$$

which is $o(X/\log X)$ provided that $2 < u$. Hence, there is no influence of squarefull N_p on our result. A short computation shows that $f(3.1, 12, 0.53, 1/3.05) = 0.35532\ldots$, which yields $r = [3.98679\ldots] = 3$ in (14). This proves (2).

Note that in Koblitz's conjecture, $C_E = \prod(1-1/\delta(\ell))(1-1/\ell)^{-1}$, which is, in the notation of our proof, equal to $\lim_{z\to\infty} W(z)\prod(1-1/\ell)^{-1}$.

5. Concluding remarks. It seems out of reach to replace the assumption of GRH in the use of Chebotarev's density theorem by a suitable Bombieri–Vinogradov theorem as it was done in Chen's celebrated approach towards the Goldbach conjecture (see [2]). The known results in that direction due to M. R. Murty and V. K. Murty [12] are not uniform in a sufficiently large range.

The ideas in this paper can be generalized in several directions. First, one can also consider elliptic curves with complex multiplication by an order $\mathcal{O}$ with class number $h(\mathcal{O}) > 1$. Here, the elliptic curve can be defined over the ring class field of the order. Next we can consider principally polarized abelian varieties of dimension $d > 1$. If the principally polarized abelian variety A has endomorphism ring equal to $\mathbb{Z}$ and dimension d where $d = 2$, 6 or odd, the Galois group $\mathrm{Gal}(\mathbb{Q}(A[\ell])/\mathbb{Q})$ is isomorphic to the general symplectic group $\mathrm{GSp}(2d, \ell)$ for all but finitely many ℓ.

For the following three non-CM curves we know that $\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \simeq \mathrm{Gl}(2, \mathbb{Z}/\ell\mathbb{Z})$ for all ℓ (cf. [15], [6]):

$$y^2 + y = x^3 - x, \quad y^2 + y = x^3 + x^2, \quad y^2 + xy + y = x^3 - x^2.$$

The smallest primes p with $\Omega(N_p) > 8$ are equal to 487, resp. 523, resp. 1289. The smallest primes with $\nu(N_p) > 5$ are given by 53377, resp. 43721, resp. 92357.

Acknowledgements. The authors are grateful to Prof. V. K. Murty for suggesting several improvements of an earlier version of the present paper. We thank the anonymous referee for valuable comments and remarks.

References

[1] E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, Astérisque 18 (1987), 2nd ed.

[2] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.

[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Univ. Press, 1938.

[4] N. M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. 62 (1981), 481–502.

[5] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp. 48 (1987), 203–209.

[6] N. Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. 131 (1988), 157–165.
[7] J. Lagarias and A. Odlyzko, *Effective versions of the Chebotarev density theorem*, in: Algebraic Number Fields, A. Fröhlich (ed.), Academic Press, New York, 1977, 409–464.
[8] S. Lang, *Elliptic Functions*, Addison-Wesley, Reading, MA, 1973.
[9] V. Miller, *Use of elliptic curves in cryptography*, in: Advances in Cryptology—Crypto '85, Lecture Notes in Comput. Sci. 218, Springer, Berlin, 1986, 417–426.
[10] S. A. Miri and V. K. Murty, *An application of sieve methods to elliptic curves*, in: Progress in Cryptology—Indocrypt 2001, Lecture Notes in Comput. Sci. 2247, Springer, Berlin, 2001, 91–98.
[11] M. R. Murty and V. K. Murty, *Prime divisors of Fourier coefficients of modular forms*, Duke Math. J. 51 (1984), 57–76.
[12] —, —, *A variant of the Bombieri–Vinogradov theorem*, in: Number Theory, CMS Conf. Proc. 7, Amer. Math. Soc., Providence, RI, 1987, 243–272.
[13] M. R. Murty, V. K. Murty and N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. Math. 110 (1988), 253–281.
[14] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. 54 (1981), 123–201.
[15] —, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), 259–331.
[16] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.
[17] —, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, New York, 1994.

Departamento de Matemáticas
Universidad Autónoma de Madrid
C. Universitaria de Cantoblanco
28049 Madrid, Spain
E-mail: jorn.steuding@uam.es

Fachbereich Mathematik
Johannes Gutenberg Universität Mainz
Staudinger Weg 9
D-55129 Mainz, Germany
E-mail: weng@mathematik.uni-mainz.de

Received on 19.9.2002
and in revised form on 26.7.2004 (4379)