ACTA ARITHMETICA
110.2 (2003)

On the order of unimodular matrices modulo integers

by

PÄR KURLBERG (Gothenburg)

1. Introduction. Given an integer b and a prime p such that $p \nmid b$, let $\mathrm{ord}_p(b)$ be the multiplicative order of b modulo p. In other words, $\mathrm{ord}_p(b)$ is the smallest nonnegative integer k such that $b^k \equiv 1 \bmod p$. Clearly $\mathrm{ord}_p(b) \le p-1$, and if the order is maximal, b is said to be a primitive root modulo p. Artin conjectured (see the preface in [1]) that if $b \in \mathbb{Z}$ is not a square, then b is a primitive root for a positive proportion (¹) of the primes.

What about the "typical" behaviour of $\mathrm{ord}_p(b)$? For instance, are there good lower bounds on $\mathrm{ord}_p(b)$ that hold for a full density subset of the primes? In [3], Erdős and Murty proved that if $b \neq 0, \pm 1$, then there exists a $\delta > 0$ so that $\mathrm{ord}_p(b)$ is at least $p^{1/2} \exp((\log p)^{\delta})$ for a full density subset of the primes (²). However, we expect the typical order to be much larger. In [6] Hooley proved that the Generalized Riemann Hypothesis (GRH) implies Artin's conjecture. Moreover, if $f : \mathbb{R}^+ \to \mathbb{R}^+$ is an increasing function tending to infinity, Erdős and Murty [3] showed that GRH implies that the order of b modulo p is greater than $p/f(p)$ for a full density subset of the primes.

It is also interesting to consider lower bounds for $\mathrm{ord}_N(b)$ where N is an integer. It is easy to see that $\mathrm{ord}_N(b)$ can be as small as $\log N$ infinitely often (take $N = b^k - 1$), but we expect the typical order to be quite large. Assuming GRH, we can prove that the lower bound $\mathrm{ord}_N(b) \gg N^{1-\varepsilon}$ holds for most integers.

THEOREM 1. *Let $b \neq 0, \pm 1$ be an integer. Assuming GRH, the number of $N \le x$ such that* $\mathrm{ord}_N(b) \ll N^{1-\varepsilon}$ *is $o(x)$. That is, the set of integers N such that* $\mathrm{ord}_N(b) \gg N^{1-\varepsilon}$ *has density one.*

However, the main focus of this paper is to investigate a related question, namely lower bounds on the order of unimodular matrices modulo $N \in \mathbb{Z}$.

2000 *Mathematics Subject Classification*: Primary 11N37; Secondary 11A07.
Author supported in part by the National Science Foundation (DMS 0071503).

(¹) The constant is given by an Euler product that depends on b.

(²) Pappalardi has shown [9] that δ can be taken to be approximately 0.15.

That is, if $A \in \mathrm{SL}_2(\mathbb{Z})$, what can be said about lower bounds for $\mathrm{ord}_N(A)$, the order of A modulo N, that hold for most N? It is a natural generalization of the previous questions, but our main motivation comes from mathematical physics (quantum chaos): In [7] Rudnick and I proved that if A is hyperbolic ([3]), then a strong form of quantum ergodicity for toral automorphisms follows from $\mathrm{ord}_N(A)$ being slightly larger than $N^{1/2}$, and we then showed that this condition holds for a full density subset of the integers ([4]). Again, we expect that the typical order is much larger. In order to give lower bounds on $\mathrm{ord}_N(A)$, it is essential to have good lower bounds on $\mathrm{ord}_p(A)$ for p prime:

THEOREM 2. *Let* $A \in \mathrm{SL}_2(\mathbb{Z})$ *be hyperbolic, and let* $f : \mathbb{R}^+ \to \mathbb{R}^+$ *be an increasing function tending to infinity more slowly than* $\log x$. *Assuming GRH, there are at most* $O\big(\frac{x}{f(x)^{1-\varepsilon}\log x}\big)$ *primes* $p \le x$ *such that* $\mathrm{ord}_p(A) < p/f(p)$. *In particular, the set of primes* p *such that* $\mathrm{ord}_p(A) \ge p/f(p)$ *has density one.*

Using this we obtain an improved lower bound on $\mathrm{ord}_N(A)$ that is valid for most integers.

THEOREM 3. *Let* $A \in \mathrm{SL}_2(\mathbb{Z})$ *be hyperbolic. Assuming GRH, the number of* $N \le x$ *such that* $\mathrm{ord}_N(A) \ll N^{1-\varepsilon}$ *is* $o(x)$. *That is, the set of integers* N *such that* $\mathrm{ord}_N(A) \gg N^{1-\varepsilon}$ *has density one.*

REMARKS. If A is elliptic ($|\mathrm{tr}(A)| < 2$) then A has finite order (in fact, at most 6). If A is parabolic ($|\mathrm{tr}(A)| = 2$), then $\mathrm{ord}_p(A) = p$ unless A is congruent to the identity matrix modulo p, and hence there exists a constant $c_A > 0$ so that $\mathrm{ord}_N(A) > c_A N$. Apart from the application in mind, it is thus natural to only treat the hyperbolic case.

As far as unconditional results for primes go, we note that the proof in [3] relies entirely on analyzing the divisor structure of $p-1$, and we expect that their method should give a similar lower bound on the order of A modulo p. An unconditional lower bound of the form

$$\mathrm{ord}_p(b) \gg p^{\eta} \tag{1}$$

for a full proportion of the primes and $\eta > 1/2$ would be quite interesting. In this direction, Goldfeld [5] proved that if $\eta < 3/5$, then (1) holds for a positive, but not full, proportion of the primes.

Clearly $\mathrm{ord}_p(A)$ is related to $\mathrm{ord}_p(\varepsilon)$, where ε is one of the eigenvalues of A. Since A is assumed to be hyperbolic, ε is a power of a fundamental unit in a real quadratic field. The question of densities of primes p such

(3) A is hyperbolic if $|\mathrm{tr}(A)| > 2$.

(4) More precisely: there exists $\delta > 0$ so that $\mathrm{ord}_N(A) \gg N^{1/2}\exp((\log N)^{\delta})$ for a full density subset of the integers.

that $\mathrm{ord}_p(\lambda)$ is maximal, for λ a fundamental unit in a real quadratic field, does not seem to have received much attention until quite recently; in [10] Roskam proved that GRH implies that the set of primes p for which $\mathrm{ord}_p(\lambda)$ is maximal has positive density. (The work of Weinberger [12], Cooke and Weinberger [2] and Lenstra [8] does treat the case $\mathrm{ord}_p(\lambda) = p-1$, but not the case $\mathrm{ord}_p(\lambda) = p+1$.)

2. Preliminaries

2.1. *Notation.* If $\mathfrak{O}_F$ is the ring of integers in a number field F, we let $\zeta_F(s) = \sum_{\mathfrak{a}\subset\mathfrak{O}_F} N(\mathfrak{a})^{-s}$ denote the zeta function of F. By GRH we mean that all nontrivial zeros of $\zeta_F(s)$ lie on the line $\mathrm{Re}(s) = 1/2$ for all number fields F.

Let ε be an eigenvalue of A, satisfying the equation

$$\varepsilon^2 - \mathrm{tr}(A)\varepsilon + \det(A) = 0. \tag{2}$$

Since A is hyperbolic, $K = \mathbb{Q}(\varepsilon)$ is a real quadratic field. Let $\mathfrak{O}_K$ be the integers in K, and let D_K be the discriminant of K. Since A has determinant one, ε is a unit in $\mathfrak{O}_K$. For $n \in \mathbb{Z}^+$ we let $\zeta_n = e^{2\pi i/n}$ be a primitive nth root of unity, and $\alpha_n = \varepsilon^{1/n}$ be an nth root of ε. Further, with $Z_n = K(\zeta_n)$, $K_n = K(\zeta_n, \alpha_n)$, and $L_n = K(\alpha_n)$, we let σ_p denote the Frobenius element in $\mathrm{Gal}(K_n/\mathbb{Q})$ associated with p. We let F_{p^k} denote the finite field with p^k elements, and we let $F_{p^2}^1 \subset F_{p^2}^\times$ be the norm one elements in F_{p^2}, i.e., the kernel of the norm map from $F_{p^2}^\times$ to $F_p^\times$. Let $\langle A\rangle_p$ be the group generated by A in $\mathrm{SL}_2(F_p)$. Then $\langle A\rangle_p$ is contained in a maximal torus (of order $p-1$ or $p+1$), and we let i_p be the index of $\langle A\rangle_p$ in this torus. Finally, let $\pi(x) = |\{p \le x : p \text{ is prime}\}|$ be the number of primes up to x.

2.2. *Kummer extensions and Frobenius elements.* We want to characterize primes p such that $n \mid i_p$, and we can relate this to primes splitting in certain Galois extensions as follows:

Reduce equation (2) modulo p and let $\overline{\varepsilon}$ denote a solution to equation (2) in F_p or F_{p^2}. (Note that if p does not ramify in K then the order of A modulo p equals the order of ε modulo p.) If p splits in K then $\overline{\varepsilon} \in F_p$, and if p is inert, then $\overline{\varepsilon} \in F_{p^2} \setminus F_p$. In the latter case, $\overline{\varepsilon} \in F_{p^2}^1$ since the norm one property is preserved when reducing modulo p. Now, $F_p^\times$ and $F_{p^2}^1$ are cyclic groups of order $p-1$ and $p+1$ respectively. Thus, if p splits in K then $\mathrm{ord}_p(\varepsilon) \mid p-1$, whereas if p is inert in K then $\mathrm{ord}_p(\varepsilon) \mid p+1$.

LEMMA 4. *Let p be unramified in K_n, and let $C_n = \{1, \gamma\} \subset \mathrm{Gal}(K_n/\mathbb{Q})$, where γ is given by $\gamma(\zeta_n) = \zeta_n^{-1}$ and $\gamma(\alpha_n) = \alpha_n^{-1}$. Then the condition that $n \mid i_p$ is equivalent to $\sigma_p \in C_n$. Moreover, C_n is invariant under conjugation.*

Proof. The split case: Since $n \mid i_p$ and $i_p \mid p-1$ we have $\zeta_n \in F_p$, i.e. F_p contains all nth roots of unity. Moreover, $\overline{\varepsilon}$ is an nth power of some element in F_p, and thus the polynomial $x^n - \varepsilon$ splits completely in F_p. In other words, p splits completely in K_n and σ_p is trivial.

The inert case: Since n divides i_p, $\overline{\varepsilon}$ is an nth power of some element in $F^1_{p^2}$ and hence $\alpha_n \in F_{p^2}$. Moreover, $n \mid p^2-1$ implies that $\zeta_n \in F_{p^2}$. Now, $N^{F_{p^2}}_{F_p}(\alpha_n) = 1$ and $N^{F_{p^2}}_{F_p}(\zeta_n) = \zeta_n^{p+1} = 1$ implies that

$$\sigma_p(\zeta_n) \equiv \zeta_n^{-1} \bmod p, \qquad \sigma_p(\alpha_n) \equiv \alpha_n^{-1} \bmod p.$$

For p that does not ramify in K_n we thus have

$$\sigma_p(\zeta_n) = \zeta_n^{-1}, \qquad \sigma_p(\alpha_n) = \alpha_n^{-1}. \tag{3}$$

Now, an element $\tau \in \mathrm{Gal}(K_n/\mathbb{Q})$ is of the form

$$\tau : \quad \begin{cases} \zeta_n \mapsto \zeta_n^t, & t \in \mathbb{Z}, \\ \alpha_n \mapsto \alpha_n^u \zeta_n^s, & s \in \mathbb{Z}, \quad u \in \{1,-1\}. \end{cases}$$

Composing γ and τ then gives

$$\tau \circ \gamma : \quad \begin{cases} \zeta_n \mapsto \zeta_n^{-1} \mapsto \zeta_n^{-t}, \\ \alpha_n \mapsto \alpha_n^{-1} \mapsto \alpha_n^{-u}\zeta_n^{-s}, \end{cases}$$

and

$$\gamma \circ \tau : \quad \begin{cases} \zeta_n \mapsto \zeta_n^{t} \mapsto \zeta_n^{-t}, \\ \alpha_n \mapsto \alpha_n^{u}\zeta_n^{s} \mapsto \alpha_n^{-u}\zeta_n^{-s}, \end{cases}$$

which shows that γ is invariant under conjugation. ∎

2.3. *The Chebotarev Density Theorem.* In [11] Serre proved that the Generalized Riemann Hypothesis (GRH) implies the following version of the Chebotarev Density Theorem:

THEOREM 5. *Let $E/\mathbb{Q}$ be a finite Galois extension of degree $[E:\mathbb{Q}]$ and discriminant D_E. For p a prime let $\sigma_p \in G = \mathrm{Gal}(E/\mathbb{Q})$ denote the Frobenius conjugacy class, and let $C \subset G$ be a union of conjugacy classes. If the nontrivial zeros of $\zeta_E(s)$ lie on the line* $\mathrm{Re}(s) = 1/2$, *then for $x \geq 2$,*

$$|\{p \leq x : \sigma_p \in C\}| = \frac{|C|}{|G|}\,\pi(x) + O\biggl(\frac{|C|}{|G|}\,x^{1/2}(\log D_E + [E:\mathbb{Q}]\log x)\biggr).$$

Now, primes that ramify in K_n divide nD_K (see Lemma 10), so as far as densities are concerned, ramified primes can be ignored. The bounds on the size of D_{K_n} (see Lemma 10) and Lemma 4 then give the following:

COROLLARY 6. *If GRH is true then*

$$|\{p \leq x : n \mid i_p\}| = \frac{2}{[K_n:\mathbb{Q}]}\,\pi(x) + O(x^{1/2}(\log(xn))). \tag{4}$$

Remark. For Theorems 2 and 3 to be true, it is enough to assume that the Riemann hypothesis holds for all ζ_{K_n}, $n > 1$.

2.3.1. *Bounds on degrees.* In order to apply the Chebotarev Density Theorem we need bounds on the degree $[K_n : \mathbb{Q}]$. We will first assume that ε is a fundamental unit.

Lemma 7. *If ε is a fundamental unit in K and if $n = 4$ or $n = q$ for q an odd prime, then* $\mathrm{Gal}(K_n/K)$ *is nonabelian.*

Proof. We start by showing that $[K_n : Z_n] = n$. Consider first the case $n = q$. If $\alpha_q \in Z_q$ then $\beta = N_K^{Z_q}(\alpha_q) = \alpha_q^{[Z_q:K]}\zeta_q^t \in K \subset \mathbb{R}$ for some integer t. Since q is odd we may assume that $\alpha_q \in \mathbb{R}$, and this forces $\zeta_q^t = 1$, which in turn implies that $\alpha_q^{[Z_q:K]} \in K$. Because ε is a fundamental unit this means that $q \mid [Z_q : K]$. On the other hand, $[Z_q : K] \mid \phi(q)$, a contradiction. Thus $\alpha_q \notin Z_q$, and hence K_q/Z_q is a Kummer extension of degree q.

For $n = 4$ we note that $i \in Z_4 = K(i)$. Thus $\alpha_2 = \sqrt{\varepsilon} \in Z_4$ implies that $\sqrt{-\varepsilon} \in Z_4$. However, either $\sqrt{\varepsilon}$ or $\sqrt{-\varepsilon}$ is real and generates a *real* degree two extension of K, whereas $K(i)$ is a nonreal quadratic extension of K, and hence $\alpha_2 \notin Z_4$. Now, if $\alpha_4 \in Z_4(\alpha_2)$ then $N_{Z_4}^{Z_4(\alpha_2)}(\alpha_4) = \alpha_4^2 i^t \in Z_4$ for some $t \in \mathbb{Z}$, and thus $\alpha_4^2 = \alpha_2 \in Z_4$, which contradicts $\alpha_2 \notin Z_4$. Therefore,

$$[Z_4(\alpha_4) : Z_4] = [Z_4(\alpha_4) : Z_4(\alpha_2)][Z_4(\alpha_2) : Z_4] = 4.$$

Finally, we note that the commutator of any nontrivial element $\sigma_1 \in \mathrm{Gal}(K_n/Z_n)$ with any nontrivial element $\sigma_2 \in \mathrm{Gal}(K_n/L_n)$ is nontrivial (we may regard $\mathrm{Gal}(K_n/Z_n)$ and $\mathrm{Gal}(K_n/L_n)$ as subgroups of $\mathrm{Gal}(K_n/K)$). Hence $\mathrm{Gal}(K_n/K)$ is nonabelian. ∎

Lemma 8. *If ε is a fundamental unit then*

$$[K_n : Z_n] \geq n/2.$$

Proof. Clearly $Z_n(\alpha_{q^k}) \subset K_n$, and since field extensions of relative prime degrees are disjoint, it is enough to show that if $q^k \parallel n$ is a prime power then $q^k \mid [Z_n(\alpha_{q^k}) : Z_n]$ if q is odd, and $q^{k-1} \mid [Z_n(\alpha_{q^k}) : Z_n]$ if $q = 2$.

If q is odd then Lemma 7 implies that $\alpha_q \notin Z_n$ since $\mathrm{Gal}(Z_n/K)$ is abelian. Hence, if $m \in \mathbb{Z}$ and $\alpha_{q^k}^m \in Z_n$, we must have $q^k \mid m$. Now, if $\sigma \in \mathrm{Gal}(Z_n(\alpha_{q^k})/Z_n)$ then $\sigma(\alpha_{q^k}) = \alpha_{q^k}\zeta_{q^k}^{t_\sigma}$ for some integer t_σ. Thus there exists an integer t such that

$$\beta = N_{Z_n}^{Z_n(\alpha_{q^k})}(\alpha_{q^k}) = \alpha_{q^k}^{[Z_n(\alpha_{q^k}):Z_n]}\zeta_q^t \in Z_n.$$

Multiplying β by $\zeta_q^{-t} \in Z_n$ we find that $\alpha_{q^k}^{[Z_n(\alpha_{q^k}):Z_n]} \in Z_n$, and hence $q^k \mid [Z_n(\alpha_{q^k}) : Z_n]$.

For $q = 2$ the proof is similar, except that a factor of two is lost if $\alpha_2 \in Z_n$. ∎

Remark. $K_2/\mathbb{Q}$ is a Galois extension of degree four, hence abelian and therefore contained in some cyclotomic extension by the Kronecker–Weber Theorem, and it is thus possible that $\alpha_2 \in Z_n$ for some values of n.

Lemma 9. *We have*

$$n\phi(n) \ll_K [K_n : \mathbb{Q}] \leq 2n\phi(n).$$

Proof. We first observe that $[Z_n : K]$ equals $\phi(n)$ or $\phi(n)/2$ depending on whether $K \subset \mathbb{Q}(\zeta_n)$ or not. We also have the trivial upper bound $[K_n : Z_n] \leq n$.

For a lower bound of $[K_n : Z_n]$ we argue as follows: Let $\gamma \in K$ be a fundamental unit. Since the norm of ε is one we may write $\varepsilon = \gamma^k$ for some $k \in \mathbb{Z}$. (Note that k does not depend on n.) As $[Z_n(\gamma^{1/n}) : Z_n(\varepsilon^{1/n})] \leq k$, Lemma 8 gives $[Z_n(\varepsilon^{1/n}) : Z_n] \geq n/k$. The upper and lower bounds now follow from

$$[K_n : \mathbb{Q}] = [K_n : Z_n][Z_n : K][K : \mathbb{Q}]. \ ∎$$

2.3.2. *Bounds on discriminants*

Lemma 10. *If p ramifies in K_n then $p \mid nD_K$. Moreover,*

$$\log(\mathrm{disc}(K_n/\mathbb{Q})) \ll_K [K_n : K] \log n.$$

Proof. First note that

$$\mathrm{disc}(K_n/\mathbb{Q}) = N_{\mathbb{Q}}^{K}(\mathrm{disc}(K_n/K)) \cdot \mathrm{disc}(K/\mathbb{Q})^{[K_n:K]}.$$

From the multiplicativity of the different we get

$$\mathrm{disc}(K_n/K) = \mathrm{disc}(Z_n/K)^{[K_n:Z_n]} \cdot N_K^{Z_n}(\mathrm{disc}(K_n/Z_n)).$$

Since ε is a unit, so is $\varepsilon^{1/n}$. Thus, if we let $f(x) = x^n - \varepsilon$ then $f'(x) = nx^{n-1}$, and therefore the principal ideal $f'(\varepsilon^{1/n})\mathfrak{O}_{K_n}$ equals $n\mathfrak{O}_{K_n}$. In terms of discriminants this means that

$$\mathrm{disc}(K_n/Z_n) \mid N_{Z_n}^{K_n}(n\mathfrak{O}_{K_n})$$

and similarly it can be shown that

$$\mathrm{disc}(Z_n/K) \mid N_K^{Z_n}(n\mathfrak{O}_{Z_n}).$$

Thus $\mathrm{disc}(K_n/\mathbb{Q})$ divides

$$N_{\mathbb{Q}}^{K}(N_K^{K_n}(n\mathfrak{O}_{K_n}) \cdot N_K^{Z_n}(n\mathfrak{O}_{Z_n})^{[K_n:Z_n]}) \cdot \mathrm{disc}(K/\mathbb{Q})^{[K_n:K]} = n^{4[K_n:K]} \cdot \mathrm{disc}(K/\mathbb{Q})^{[K_n:K]},$$

which proves the two assertions. ∎

3. Proof of Theorem 2. In order to bound the number of primes $p < x$ for which $i_p > x^{1/2}$ we will need the following lemma:

LEMMA 11. *The number of primes p such that* $\operatorname{ord}_p(A) \le y$ *is* $O(y^2)$.

Proof. Given A there exists a constant C_A such that $\det(A^n - I) = O(C_A^n)$. Now, if the order of A modulo p is n, then certainly p divides $\det(A^n - I) \ne 0$. Putting $M = \prod_{n=1}^{y} \det(A^n - I)$ we see that any prime p for which A has order $n \le y$ must divide M. Finally, the number of prime divisors of M is bounded by

$$\log M \ll \sum_{n=1}^{y} n \log C_A \ll y^2. \ \blacksquare$$

First step: We consider primes p such that $i_p \in (x^{1/2}\log x, x)$. By Lemma 11 the number of such primes is

$$O\biggl(\Bigl(\frac{x}{x^{1/2}\log x}\Bigr)^2\biggr) = O\Bigl(\frac{x}{\log^2 x}\Bigr). \tag{5}$$

Second step: Consider p such that $q \mid i_p$ for some prime $q \in \bigl(\frac{x^{1/2}}{\log^3 x}, x^{1/2}\log x\bigr)$. We may bound this by considering primes $p \le x$ such that $p \equiv \pm 1 \bmod q$ for $q \in \bigl(\frac{x^{1/2}}{\log^3 x}, x^{1/2}\log x\bigr)$. Since $q \le x^{1/2}\log x$, Brun's sieve gives (up to an absolute constant) the bound $x/(\phi(q)\log x)$, and the total contribution from these primes is at most

$$\sum_{q \in (\frac{x^{1/2}}{\log^3 x}, x^{1/2}\log x)} \frac{x}{\phi(q)\log(x/q)} \ll \frac{x}{\log x} \sum_{q \in (\frac{x^{1/2}}{\log^3 x}, x^{1/2}\log x)} \frac{1}{q}. \tag{6}$$

Now, summing reciprocals of primes in a dyadic interval, we get

$$\sum_{q \in [M,2M]} \frac{1}{q} \ll \frac{\pi(2M)}{M} \le \frac{1}{\log M}.$$

Hence

$$\sum_{q \in (\frac{x^{1/2}}{\log^3 x}, x^{1/2}\log x)} \frac{1}{q} \ll \frac{1}{\log x} \log_2\left(\frac{x^{1/2}\log x}{x^{1/2}/\log^3 x}\right) \ll \frac{\log\log x}{\log x}$$

and the right hand side of (6) is $O\bigl(\frac{x\log\log x}{\log^2 x}\bigr)$.

Third step: Now consider p such that $q \mid i_p$ for some prime $q \in \bigl(f(x)^2, \frac{x^{1/2}}{\log^3 x}\bigr)$. We are now in the range where GRH is applicable; by Corollary 6 and Lemma 9 we have

$$|\{p \le x : q \mid i_p\}| \ll \frac{x}{q\phi(q)\log x} + O(x^{1/2}\log(xq^2)).$$

Summing over $q \in \big(f(x)^2, \frac{x^{1/2}}{\log^3 x}\big)$ we find that the number of such $p \le x$ is bounded by

$$\sum_{q \in (f(x)^2, \frac{x^{1/2}}{\log^3 x})} \left(\frac{x}{q^2 \log x} + O(x^{1/2} \log(xq^2)) \right). \tag{7}$$

Now,

$$\sum_{q \in (f(x)^2, \frac{x^{1/2}}{\log^3 x})} \frac{1}{q^2} \ll \frac{1}{f(x)}$$

and thus (7) is

$$\ll \frac{x}{f(x) \log x} + \frac{x}{\log^2 x}.$$

Fourth step: For the remaining primes p, any prime divisor $q \mid i_p$ is smaller than $f(x)^2$. Hence i_p must be divisible by some integer $d \in (f(x), f(x)^3)$. Again Lemmas 6 and 9 give

$$|\{p \le x : d \mid i_p\}| \ll \frac{x}{d\phi(d) \log x} + O(x^{1/2} \log(xd^2)).$$

Noting that $\phi(d) \gg d^{1-\varepsilon}$ and summing over $d \in (f(x), f(x)^3)$ we find that the number of such $p \le x$ is bounded by

$$\sum_{d \in (f(x), f(x)^3)} \left(\frac{x}{d^{2-\varepsilon} \log x} + O(x^{1/2} \log(xd^2)) \right). \tag{8}$$

Now,

$$\sum_{d \in (f(x), f(x)^3)} \frac{1}{d^{2-\varepsilon}} \ll \frac{1}{f(x)^{1-\varepsilon}}$$

and

$$\sum_{d \in (f(x), f(x)^3)} x^{1/2} \log(xd^2) \ll f(x)^3 x^{1/2} \log(x^2),$$

therefore (8) is

$$\ll \frac{x}{f(x)^{1-\varepsilon} \log x}.$$

4. Proof of Theorems 1 and 3. Given a composite integer $N = \prod_{p|N} p^{a_p}$ we wish to use the lower bounds on $\mathrm{ord}_p(b)$ (or $\mathrm{ord}_p(A)$) to obtain a lower bound on $\mathrm{ord}_N(b)$. The main obstacle is that $\mathrm{ord}_N(b)$ can be much smaller than $\prod_{p|N} \mathrm{ord}_{p^{a_p}}(b)$. Let $\lambda(N)$ be the Carmichael lambda function, i.e., the exponent of the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^\times$. Clearly $\mathrm{ord}_N(b) \le \lambda(N)$, and it turns out that $\lambda(N)$ can be much smaller than N. However,

$\lambda(N) \gg N^{1-\varepsilon}$ for most N (see [4]), and since

$$\mathrm{ord}_N(b) \geq \frac{\lambda(N)}{N} \prod_{p \mid N} \mathrm{ord}_p(b)$$

it suffices to show that most integers are essentially given by a product of primes p such that $\mathrm{ord}_p(b) \geq p/\log p$. We will only give the details for Theorem 3 since the other case is very similar.

If p is prime such that $\mathrm{ord}_p(A) \leq p/\log p$, or p ramifies in K, we say that p is "bad". We let P_B denote the set of all bad primes, and we let $P_B(z)$ be the set of primes $p \in P_B$ such that $p \geq z$. Since only finitely many primes ramify in K, Theorem 2 implies that the number of bad primes $p \leq x$ is $O(x/\log^{2-\varepsilon} x)$. A key observation is the following:

LEMMA 12. *We have*

$$\sum_{p \in P_B} \frac{1}{p} < \infty.$$

In particular, *if we let*

$$\beta(z) = \sum_{p \in P_B(z)} 1/p,$$

then $\beta(z)$ tends to zero as z tends to infinity.

Proof. Immediate from partial summation and the $O(x/\log^{2-\varepsilon} x)$ estimate in Theorem 2. ■

Given $N \in \mathbb{Z}$, write $N = s^2 N_G N_B$ where $N_G N_B$ is square-free and N_B is the product of "bad" primes dividing N. By the following lemma, we find that few integers have a large square factor:

LEMMA 13. *We have*

$$|\{N \leq x : s^2 \mid N,\, s \geq y\}| = O(x/y).$$

Proof. The number of $N \leq x$ such that $s^2 \mid N$ for $s \geq y$ is bounded by $\sum_{s \geq y} x/s^2 \ll x/y$. ■

Next we show that there are few N for which N_B is divisible by $p \in P_B(z)$. In other words, for most N, N_B is a product of small "bad" primes.

LEMMA 14. *The number of $N \leq x$ such that $p \in P_B(z)$ divides N_B is $O(x\beta(z))$.*

Proof. Let $p \in P_B(z)$. The number of $N \leq x$ such that $p \mid N$ is less than x/p. Thus, the total number of $N \leq x$ such that some $p \in P_B(z)$ divides N, is bounded by

$$\sum_{p \in P_B(z)} \frac{x}{p} = x \sum_{p \in P_B(z)} \frac{1}{p} = x\beta(z). \ ■$$

Combining the previous results we find that the number of $N = s^2 N_G N_B \le x$ such that N_B is z-smooth and $s \le y$ is

$$x(1 + O(\beta(z) + 1/y)).$$

For such N we have $N_B \le \prod_{p \le z} p \ll e^z$. Letting $z = \log\log x$ and $y = \log x$ we get

$$N_G = \frac{N}{s^2 N_B} \ge \frac{N}{\log^3 x}$$

for $N \le x$ with at most $O(x(\beta(\log\log x) + (\log x)^{-1})) = o(x)$ exceptions. Now, the following proposition shows that, for most N, $\mathrm{ord}_N(A)$ is essentially given by $\prod_{p|N} \mathrm{ord}_p(A)$.

PROPOSITION ([7, Proposition 11]). *Let $D_A = 4(\mathrm{tr}(A)^2 - 4)$. For almost all* (5) $N \le x$,

$$\mathrm{ord}_N(A) \ge \frac{\prod_{p|d_0} \mathrm{ord}_p(A)}{\exp(3(\log\log x)^4)}$$

where d_0 is given by writing $N = ds^2$, with $d = d_0 \gcd(d, D_A)$ square-free.

Finally, since $\mathrm{ord}_p(A) \ge p/\log p \ge p^{1-\varepsilon}$ for $p \mid N_G$ and p sufficiently large, we find that

$$\mathrm{ord}_N(A) \gg \frac{\prod_{p|N_G} \mathrm{ord}_p(A)}{\exp(3(\log\log x)^4)} \gg \frac{N_G^{1-\varepsilon}}{\exp(3(\log\log x)^4)} \gg N^{1-2\varepsilon}$$

for all but $o(x)$ integers $N \le x$.

References

[1] E. Artin, *The Collected Papers of Emil Artin*, Addison-Wesley, Reading, 1965.

[2] G. Cooke and P. J. Weinberger, *On the construction of division chains in algebraic number rings, with applications to* SL_2, Comm. Algebra 3 (1975), 481–524.

[3] P. Erdős and M. R. Murty, *On the order of a* $(\mathrm{mod}\, p)$, in: Number Theory (Ottawa, ON, 1996), Amer. Math. Soc., Providence, RI, 1999, 87–97.

[4] P. Erdős, C. Pomerance and E. Schmutz, *Carmichael's lambda function*, Acta Arith. 58 (1991), 363–385.

[5] M. Goldfeld, *On the number of primes p for which $p + a$ has a large prime factor*, Mathematika 16 (1969), 23–27.

[6] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. 225 (1967), 209–220.

[7] P. Kurlberg and Z. Rudnick, *On quantum ergodicity for linear maps of the torus*, Comm. Math. Phys. 222 (2001), 201–227.

[8] H. W. Lenstra, Jr., *On Artin's conjecture and Euclid's algorithm in global fields*, Invent. Math. 42 (1977), 201–224.

[9] F. Pappalardi, *On the order of finitely generated subgroups of* $\mathbf{q}^*$ $(\mathrm{mod}\, p)$ *and divisors of* $p - 1$, J. Number Theory 57 (1996), 207–222.

(5) By "for almost all $N \le x$" we mean that there are $o(x)$ exceptional integers N that are smaller than x.

[10] H. Roskam, *A quadratic analogue of Artin's conjecture on primitive roots*, ibid. 81 (2000), 93–109.

[11] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. 54 (1981), 323–401.

[12] P. J. Weinberger, *On Euclidean rings of algebraic integers*, in: Analytic Number Theory, Proc. Sympos. Pure Math. 24 (St. Louis, MO, 1972), Amer. Math. Soc., Providence, RI, 1973, 321–332.

Department of Mathematics
Chalmers University of Technology
SE-412 96 Gothenburg, Sweden
E-mail: kurlberg@math.chalmers.se
URL: www.math.chalmers.se/˜kurlberg

Received on 15.4.2002 (4262)