

# ON THE ORDER OF UNIMODULAR MATRICES MODULO INTEGERS

PÄR KURLBERG

PRELIMINARY VERSION

## 1. INTRODUCTION

Given an integer  $b$  and a prime  $p$  such that  $p \nmid b$ , let  $\text{ord}_p(b)$  be the multiplicative order of  $b$  modulo  $p$ . In other words,  $\text{ord}_p(b)$  is the smallest non negative integer  $k$  such that  $b^k \equiv 1 \pmod{p}$ . Clearly  $\text{ord}_p(b) \leq p-1$ , 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  $b \in \mathbf{Z}$  is not a square, then  $b$  is a primitive root for a positive proportion<sup>1</sup> of the primes.

What about the “typical” behaviour of  $\text{ord}_p(b)$ ? For instance, are there good lower bounds on  $\text{ord}_p(b)$  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  $\text{ord}_p(b)$  is at least  $p^{1/2} \exp((\log p)^\delta)$  for a full density subset of the primes. However, we expect the typical order to be much larger. In [5] Hooley proved that the Generalized Riemann Hypothesis (GRH) implies Artin’s conjecture. Moreover, if  $f : \mathbf{R}^+ \rightarrow \mathbf{R}^+$  is an increasing function tending to infinity, it is possible to modify Hooley’s argument to show that GRH implies that the order of  $b$  modulo  $p$  is greater than  $p/f(p)$  for full density subset of the primes.

In this paper we will investigate a related question, namely lower bounds on the order of unimodular matrices modulo  $N \in \mathbf{Z}$ . That is, if  $A \in SL_2(\mathbf{Z})$ , what can be said about lower bounds for  $\text{ord}_N(A)$ , 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 [6] Rudnick and I proved that if  $A$  is hyperbolic<sup>2</sup>, then quantum ergodicity for toral automorphisms follows from  $\text{ord}_N(A)$  being slightly larger than  $N^{1/2}$ , and we then showed that this condition does hold for a full density subset of the integers.

---

Author supported in part by the National Science Foundation (DMS 0071503).

<sup>1</sup>The constant is given by an Euler product that depends on  $b$ .

<sup>2</sup> $A$  is hyperbolic if  $|\text{tr}(A)| > 2$ .

Again, we expect that the typical order is much larger. In order to give lower bounds on  $\text{ord}_N(A)$ , it is essential to have good lower bounds on  $\text{ord}_p(A)$  for  $p$  prime, and this is our first goal.

**Theorem 1.** *Let  $A \in SL_2(\mathbf{Z})$  be hyperbolic, and let  $f : \mathbf{R}^+ \rightarrow \mathbf{R}^+$  be an increasing function tending to infinity slower than  $\log x$ . Assuming GRH, there are at most  $O(\frac{x}{\log x f(x)^{1-\epsilon}})$  primes  $p \leq x$  such that  $\text{ord}_p(A) < p/f(p)$ . In particular, the set of primes  $p$  such that  $\text{ord}_p(A) \geq p/f(p)$  has density one.*

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

**Theorem 2.** *Let  $A \in SL_2(\mathbf{Z})$  be hyperbolic. Assuming GRH, the number of  $N \leq x$  such that  $\text{ord}_N(A) \ll N^{1-\epsilon}$  is  $o(x)$ . That is, the set of integers  $N$  such that  $\text{ord}_N(A) \gg N^{1-\epsilon}$  has density one.*

*Remarks:* If  $A$  is elliptic ( $|\text{tr}(A)| < 2$ ) then  $A$  has finite order (in fact, at most 6). If  $A$  is parabolic ( $|\text{tr}(A)| = 2$ ), then  $\text{ord}_p(A) = p$  unless  $A$  is congruent to the identity matrix modulo  $p$ , and hence there exists a constant  $c_A > 0$  so that  $\text{ord}_N(A) > c_A N$ . 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

$$(1) \quad \text{ord}_p(b) \gg p^\eta$$

for a full proportion of the primes and  $\eta > 1/2$  would be quite interesting. In this direction, Goldfeld proved [4] that if  $\eta < 3/5$ , then (1) holds for a positive, but not full, proportion of the primes.

Clearly  $\text{ord}_p(A)$  is related to  $\text{ord}_p(\epsilon)$ , where  $\epsilon$  is one of the eigenvalues of  $A$ . Since  $A$  is assumed to be hyperbolic,  $\epsilon$  is a power of a fundamental unit in a real quadratic field. The question of densities of primes  $p$  such that  $\text{ord}_p(\lambda)$  is maximal, for  $\lambda$  a fundamental unit in a real quadratic field, does not seem to have received much attention until quite recently; in [8] Roskam proved that GRH implies that the set of primes  $p$  for which  $\text{ord}_p(\lambda)$  is maximal has positive density. (The work of Weinberger [2], Cooke and Weinberger [10] and Lenstra [7] does treat the case  $\text{ord}_p(\lambda) = p - 1$ , but not the case  $\text{ord}_p(\lambda) = p + 1$ .)

## 2. PRELIMINARIES

**2.1. Notation.** If  $\mathfrak{O}_F$  is the ring of integers in a number field  $F$ , we let  $\zeta_F(s) = \sum_{\mathfrak{a} \in \mathfrak{O}_F} N(\mathfrak{a})^{-s}$  denote the zeta function of  $F$ . By GRH we

mean that all nontrivial zeroes of  $\zeta_F(s)$  lie on the line  $\text{Re}(s) = 1/2$  for all number fields  $F$ .

Let  $\epsilon$  be an eigenvalue of  $A$ , satisfying the equation

$$(2) \quad \epsilon^2 - \text{tr}(A)\epsilon + \det(A).$$

Since  $A$  is hyperbolic,  $K = \mathbf{Q}(\epsilon)$  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,  $\epsilon$  is a unit in  $\mathfrak{O}_K$ . For  $n \in \mathbf{Z}^+$  we let  $\zeta_n = e^{2\pi i/n}$  be a primitive  $n$ -th root of unity, and  $\alpha_n = \epsilon^{1/n}$  be an  $n$ -th root of  $\epsilon$ . Further, with  $Z_n = K(\zeta_n)$ ,  $K_n = K(\zeta_n, \alpha_n)$ , and  $L_n = K(\alpha_n)$ , we let  $\sigma_p$  denote the Frobenius element in  $\text{Gal}(K_n/\mathbf{Q})$  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  $SL_2(F_p)$ .  $\langle A \rangle_p$  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  $\pi(x) = |\{p \leq x : p \text{ is prime}\}|$  be the number of primes up to  $x$ .

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

Reduce equation (2) modulo  $p$  and let  $\bar{\epsilon}$  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  $\epsilon$  modulo  $p$ .) If  $p$  splits in  $K$  then  $\bar{\epsilon} \in F_p$ , and if  $p$  is inert, then  $\bar{\epsilon} \in F_{p^2} \setminus F_p$ . In the latter case,  $\bar{\epsilon} \in F_{p^2}^1$  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  $\text{ord}_p(\epsilon)|p-1$ , whereas if  $p$  is inert in  $K$  then  $\text{ord}_p(\epsilon)|p+1$ .

**Lemma 3.** *Let  $p$  be unramified in  $K_n$ , and let  $C_n = \{1, \gamma\} \subset \text{Gal}(K_n/\mathbf{Q})$ , where  $\gamma$  is given by  $\gamma(\zeta_n) = \zeta_n^{-1}$  and  $\gamma(\alpha_n) = \alpha_n^{-1}$ . Then the condition that  $n|i_p$  is equivalent to  $\sigma_p \in C_n$ . Moreover,  $C_n$  is invariant under conjugation.*

*Proof. The split case:* Since  $n|i_p$  and  $i_p|p-1$  we have  $\zeta_n \in F_p$ , i.e.  $F_p$  contains all  $n$ -th roots of unity. Moreover,  $\bar{\epsilon}$  is an  $n$ -th power of some element in  $F_p$ , and thus the equation  $x^n - \epsilon$  splits completely in  $F_p$ . In other words,  $p$  splits completely in  $K_n$  and  $\sigma_p$  is trivial.

*The inert case:* Since  $n$  divides  $i_p$ ,  $\bar{\epsilon}$  is an  $n$ -th power of some element in  $F_{p^2}^1$  and hence  $\alpha_n \in F_{p^2}$ . Moreover,  $n|p^2-1$  implies that  $\zeta_n \in F_{p^2}$ .

Now,  $N_{F_p}^{F_{p^2}}(\alpha_n) = 1$  and  $N_{F_p}^{F_{p^2}}(\zeta_n) = \zeta_n^{p+1} = 1$  implies that

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

For  $p$  that does not ramify in  $K_n$  we thus have

$$(3) \quad \sigma_p(\zeta_n) = \zeta_n^{-1}, \quad \sigma_p(\alpha_n) = \alpha_n^{-1}$$

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

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

Composing  $\gamma$  and  $\tau$  then gives

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

and

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

which shows that  $\gamma$  is invariant under conjugation.  $\square$

**2.3. The Chebotarev density Theorem.** In [9] Serre proved that the Generalized Riemann Hypothesis (GRH) implies the following version of the Chebotarev density Theorem:

**Theorem 4.** *Let  $E/\mathbf{Q}$  be a finite Galois extension of degree  $[E : \mathbf{Q}]$  and discriminant  $D_E$ . For  $p$  a prime let  $\sigma_p \in G = \text{Gal}(E/\mathbf{Q})$  denote the Frobenius conjugacy class, and let  $C \subset G$  be a union of conjugacy classes. If the nontrivial zeroes of  $\zeta_E(s)$  lie on the line  $\text{Re}(s) = 1/2$ , then for  $x \geq 2$ ,*

$$|\{p \leq x : \sigma_p \in C\}| = \frac{|C|}{|G|} \pi(x) + O\left(\frac{|C|}{|G|} x^{1/2} (\log D_E + [E : \mathbf{Q}] \log x)\right)$$

Now, primes that ramify in  $K_n$  divides  $nD_K$  (see Lemma 9), so as far as densities are concerned, ramified primes can be ignored. The bounds on the size of  $D_{K_n}$  (see Lemma 9) and Lemma 3 then gives the following:

**Corollary 5.** *If GRH is true then*

$$(4) \quad |\{p \leq x : n| i_p\}| = \frac{2}{[K_n : \mathbf{Q}]} \times \pi(x) + O(x^{1/2}(\log(xn)))$$

*Remark:* For theorems 1 and 2 to be true, it is enough to assume that the Riemann hypothesis holds for all  $\zeta_{K_n}$ ,  $n > 1$ .

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

**Lemma 6.** *If  $\epsilon$  is a fundamental unit in  $K$  and if  $n = 4$  or  $n = q$ , for  $q$  an odd prime, then  $\text{Gal}(K_n/K)$  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  $\beta = N_K^{Z_q}(\alpha_q) = \alpha_q^{[Z_q : K]} \zeta_q^t \in K \subset \mathbf{R}$  for some integer  $t$ . Since  $q$  is odd we may assume that  $\alpha_q \in \mathbf{R}$ , and this forces  $\zeta_q^t = 1$ , which in turn implies that  $\alpha_q^{[Z_q : K]} \in K$ . Because  $\epsilon$  is a fundamental unit this means that  $q|[Z_q : K]$ . On the other hand,  $[Z_q : K]|\phi(q)$ , 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  $\alpha_2 = \sqrt{\epsilon} \in Z_4$  implies that  $\sqrt{-\epsilon} \in Z_4$ . However, either  $\sqrt{\epsilon}$  or  $\sqrt{-\epsilon}$  is real and generates a *real* degree two extension of  $K$ , whereas  $K(i)$  is a non-real 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  $t \in \mathbf{Z}$ , 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  $\sigma_1 \in \text{Gal}(K_n/Z_n)$  with any nontrivial element  $\sigma_2 \in \text{Gal}(K_n/L_n)$  is nontrivial (we may regard  $\text{Gal}(K_n/Z_n)$  and  $\text{Gal}(K_n/L_n)$  as subgroups of  $\text{Gal}(K_n/K)$ ). Hence  $\text{Gal}(K_n/K)$  is nonabelian.  $\square$

**Lemma 7.** *If  $\epsilon$  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  $q^k|n$  is a prime power then  $q^k|[Z_n(\alpha_{q^k}) : Z_n]$  if  $q$  is odd, and  $q^{k-1}|[Z_n(\alpha_{q^k}) : Z_n]$  if  $q = 2$ .

If  $q$  is odd then Lemma 6 implies that  $\alpha_q \notin Z_n$  since  $\text{Gal}(Z_n/K)$  is abelian. Hence, if  $m \in \mathbf{Z}$  and  $\alpha_{q^k}^m \in Z_n$ , we must have  $q^k|m$ . Now, if  $\sigma \in \text{Gal}(Z_n(\alpha_{q^k})/Z_n)$  then  $\sigma(\alpha_{q^k}) = \alpha_{q^k} \zeta_{q^k}^{t_\sigma}$  for some integer  $t_\sigma$ . 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  $\beta$  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  $q^k|[Z_n(\alpha_{q^k}) : Z_n]$ .

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

*Remark:*  $K_2/Q$  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 8.** *We have*

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

*Proof.* We first note that  $[Z_n : K]$  equals  $\phi(n)$  or  $\phi(n)/2$  depending on whether  $K \subset \mathbf{Q}(\zeta_n)$  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  $\epsilon$  is one we may write  $\epsilon = \gamma^k$  for some  $k \in \mathbf{Z}$ . (Note that  $k$  does not depend on  $n$ .) As  $[Z_n(\gamma^{1/n}) : Z_n(\epsilon^{1/n})] \leq k$ , Lemma 7 gives that  $[Z_n(\epsilon^{1/n}) : Z_n] \geq n/k$ . The upper and lower bounds now follows from

$$[K_n : \mathbf{Q}] = [K_n : Z_n][Z_n : K][K : \mathbf{Q}]$$

$\square$

### 2.3.2. Bounds on discriminants.

**Lemma 9.** *If  $p$  ramifies in  $K_n$  then  $p|nD_K$ . Moreover,*

$$\log(\text{disc}(K_n/\mathbf{Q})) \ll_K [K_n : K] \log(n)$$

*Proof.* First note that

$$\text{disc}(K_n/\mathbf{Q}) = N_{\mathbf{Q}}^K(\text{disc}(K_n/K)) \times \text{disc}(K/\mathbf{Q})^{[K_n : K]}.$$

From the multiplicativity of the different we get

$$\text{disc}(K_n/K) = \text{disc}(Z_n/K)^{[K_n : Z_n]} \times N_K^{Z_n}(\text{disc}(K_n/Z_n)),$$

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

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

and similarly it can be shown that

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

Thus  $\text{disc}(K_n/\mathbf{Q})$  divides

$$N_{\mathbf{Q}}^K(N_K^{K_n}(n\mathfrak{O}_{K_n}) \times N_K^{Z_n}(n\mathfrak{O}_{Z_n})^{[K_n : Z_n]}) \times \text{disc}(K/\mathbf{Q})^{[K_n : K]}.$$

$$= n^{4[K_n:K]} \times \text{disc}(K/\mathbf{Q})^{[K_n:K]}$$

which proves the two assertions.  $\square$

### 3. PROOF OF THEOREM 1

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

**Lemma 10.** *The number of primes  $p$  such that  $\text{ord}_p(A) \leq y$  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  $A \pmod{p}$  is  $n$ , then certainly  $p$  divides  $\det(A^n - I) \neq 0$ . Putting  $M = \prod_{n=1}^y \det(A^n - I)$  we see that any prime  $p$  for which  $A$  has order  $n \leq y$  must divide  $M$ . Finally, the number of prime divisors of  $M$  is bounded by

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

$\square$

*First step:* We consider primes  $p$  such that  $i_p \in (x^{1/2} \log x, x)$ . By Lemma 10 the number of such primes is

$$(5) \quad O\left(\left(\frac{x}{x^{1/2} \log x}\right)^2\right) = O\left(\frac{x}{\log^2 x}\right).$$

*Second step:* Consider  $p$  such that  $q|i_p$  for some prime  $q \in (\frac{x^{1/2}}{\log^3 x}, x^{1/2} \log x)$ . We may bound this by considering primes  $p \leq x$  such that  $p \equiv \pm 1 \pmod{q}$  for  $q \in (\frac{x^{1/2}}{\log^3 x}, x^{1/2} \log x)$ . Since  $q \leq x^{1/2} \log x$ , Brun's sieve gives (up to an absolute constant) the bound

$$\frac{x}{\phi(q) \log(x)}$$

and the total contribution from these primes is at most

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

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

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

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 equation (6) is  $O(\frac{x \log \log x}{\log^2 x})$ .

*Third step:* Now consider  $p$  such that  $q|i_p$  for some prime  $q \in (f(x)^2, \frac{x^{1/2}}{\log^3 x})$ . We are now in the range where GRH is applicable; by Corollary 5 and Lemma 8 we have

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

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

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

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 equation (7) is

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

*Fourth step:* For the remaining primes  $p$ , any prime divisor  $q|i_p$  is smaller than  $f(x)^2$ . Hence  $i_p$  must be divisible by some integer  $d \in (f(x), f(x)^3)$ . Again Lemmas 5 and 8 give

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

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

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

Now,

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

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 equation (8) is

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

#### 4. PROOF OF THEOREM 2

With the results from the previous section we may now deduce Theorem 2. If  $p$  is prime such that  $\text{ord}_p(A) \leq p/\log(p)$ , 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 1 gives that the number of bad primes  $p \leq x$  is  $O(\frac{x}{\log^{2-\epsilon} x})$ . A key observation is the following:

**Lemma 11.** *We have*

$$(9) \quad \sum_{p \in P_B} \frac{1}{p} < \infty$$

*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  $O(\frac{x}{\log^{2-\epsilon} x})$  estimate in Theorem 1.  $\square$

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 12.**

$$|\{N \leq x : s^2 | N, s \geq y\}| = O\left(\frac{x}{y}\right)$$

*Proof.* The number of  $N \leq x$  such that  $s^2 | N$  for  $s \geq y$  is bounded by

$$\sum_{s \geq y} \frac{x}{s^2} \ll \frac{x}{y}$$

$\square$

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 13.** *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  $p|N$  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 get that the number of  $N = s^2 N_G N_B \leq x$  such that  $N_B$  is  $z$ -smooth and  $s \leq y$  is

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

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

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

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

**Proposition** ([6], Proposition 11). *Let  $D_A = 4(\text{tr}(A)^2 - 4)$ . For almost all<sup>3</sup>  $N \leq x$ ,*

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

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

Finally, since  $\text{ord}_p(A) \geq \frac{p}{\log p} \geq p^{1-\epsilon}$  for  $p|N_G$  and  $p$  sufficiently large, we thus find that

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

for most  $N$ .

---

<sup>3</sup>By “for almost all  $N \leq x$ ” we mean that there are  $o(x)$  exceptional integers  $N$  that are smaller than  $x$ .

## REFERENCES

- [1] E. Artin. *The collected papers of Emil Artin*. Addison-Wesley Publishing Co., Inc., Reading, Mass.-London, 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*, 3:481–524, 1975.
- [3] P. Erdős and M. R. Murty. On the order of  $a \pmod{p}$ . In *Number theory (Ottawa, ON, 1996)*, pages 87–97. Amer. Math. Soc., Providence, RI, 1999.
- [4] M. Goldfeld. On the number of primes  $p$  for which  $p + a$  has a large prime factor. *Mathematika*, 16:23–27, 1969.
- [5] C. Hooley. On Artin’s conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.
- [6] P. Kurlberg and Z. Rudnick. On quantum ergodicity for linear maps of the torus. *Comm. Math. Phys.*, 222(1):201–227, 2001.
- [7] H. W. Lenstra, Jr. On Artin’s conjecture and Euclid’s algorithm in global fields. *Invent. Math.*, 42:201–224, 1977.
- [8] H. Roskam. A quadratic analogue of Artin’s conjecture on primitive roots. *J. Number Theory*, 81(1):93–109, 2000.
- [9] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.
- [10] P. J. Weinberger. On Euclidean rings of algebraic integers. In *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, pages 321–332. Amer. Math. Soc., Providence, R. I., 1973.

DEPARTMENT OF MATHEMATICS, CHALMERS UNIVERSITY OF TECHNOLOGY,  
SE-412 96 GOTHENBURG, SWEDEN

URL: [www.math.chalmers.se/~kurlberg](http://www.math.chalmers.se/~kurlberg)

E-mail address: [kurlberg@math.chalmers.se](mailto:kurlberg@math.chalmers.se)