JOURNAL OF NUMBER THEORY **57**, 207–222 (1996)
ARTICLE NO. 0044

On the Order of Finitely Generated Subgroups of $\mathbb{Q}^*(\bmod p)$ and Divisors of $p-1$

FRANCESCO PAPPALARDI*

Dipartimento di Matematica, Terza Università degli Studi di Roma, Via Corrado Segre, 2, Rome 00146, Italy

Communicated by E. Bombieri

Received June 22, 1994; revised September 22, 1994

Let Γ be a finitely generated subgroup of $\mathbb{Q}^*$ with rank r. We study the size of the order $|\Gamma_p|$ of Γ mod p for density-one sets of primes. Using a result on the scarcity of primes $p \leqslant x$ for which $p-1$ has a divisor in an interval of the type $[y, y \exp \log^\tau y]$ ($\tau \sim 0.15$), we deduce that $|\Gamma_p| \geqslant p^{r/(r+1)} \exp \log^\tau p$ for almost all p and, assuming the Generalized Riemann Hypothesis, we show that $|\Gamma_p| \geqslant p/\psi(p)$ ($\psi \to \infty$) for almost all p. We also apply this to the Brown–Zassenhaus Conjecture concerned with minimal sets of generators for primitive roots.

1. INTRODUCTION

Let r be a positive integer. We say that r non-zero integers $a_1, ..., a_r$ are *multiplicatively independent* if whenever there exist $m_1, ..., m_r \in \mathbb{Z}$ such that

$$a_1^{m_1} \cdots a_r^{m_r} = 1,$$

it follows that $m_1 = \cdots = m_r = 0$. We assume that none of $a_1, ..., a_r$ is a perfect square or ± 1; let Γ denote the subgroup of $\mathbb{Q}^*$ generated by $a_1, ..., a_r$ and let $|\Gamma_p|$ denote the order of such a group Γ (mod p).

In the case $r=1$, $\Gamma = \langle a \rangle$, let $\operatorname{ord}_p(a)$ denote the order of a (mod p). The famous Artin Conjecture for primitive roots (see [1]) states that $\operatorname{ord}_p(a) = p-1$ for infinitely many primes p.

Artin's Conjecture has been proved under the assumption of the Generalized Riemann Hypothesis by C. Hooley (See [13]). In his paper it is implicitly shown (unconditionally) that

$$\operatorname{ord}_p(a) > \sqrt{p}/\log p \tag{1.1}$$

for all but $O(x/\log^3 x)$ primes $p \leqslant x$.

* Supported in part by C.I.C.M.A. and C.N.R.

0022-314X/96 $18.00

We also mention that Heat-Brown (see [12]) building on the work of Gupta and Murty (see [9]) has shown that if $\{a_1, a_2, a_3\}$ are any three multiplicatively independent integers different from ± 1 and such that none of

$$\{a_1, a_2, a_3, -3a_1 a_2, -3a_2 a_3, -3a_1 a_3, a_1 a_2 a_3\}$$

is a perfect square, then there exists at least one i for which the number of primes $p \leqslant x$ with $\mathrm{ord}_p(a_i) = p-1$ is $\gg (x/\log^2 x)$.

The following extends (1.1).

PROPOSITION 1.1. *With the above notation, we have that*

$$|\Gamma_p| > \frac{p^{r/(r+1)}}{\log p}$$

for all but $O(x/(\log x)^{2+1/r})$ *primes* $p \leqslant x$. *More generally, if* $\psi(x)$ *is any function that tends steadily to infinity with* x, *then*

$$|\Gamma_p| > \left(\frac{p}{\psi(p)}\right)^{r/(r+1)}$$

for all but $O(\pi(x)/\psi(x))$ *primes* $p \leqslant x$.

Proposition 1.1 is a consequence of the following result which is implicit in a paper of Matthews (see [14]).

LEMMA 1.2. *Suppose that* r *is a function of* t *such that* $rt^{-1/r}$ *is bounded. Then*

$$\#\{p \mid |\Gamma_p| \leqslant t\} \ll \frac{t^{1+1/r}}{\log t}\, 2^r r \sum_i \log a_i$$

uniformly with respect to t, r *and* $\{a_1, ..., a_r\}$.

Proof of Lemma 1.2. Consider the set

$$\mathscr{M} = \{a_1^{n_1} \cdot \cdots \cdot a_r^{n_r} \mid 0 \leqslant n_i \leqslant t^{1/r}\}.$$

As $a_1, ..., a_r$ are multiplicatively independent, no two elements of $\mathscr{M}$ can be equal; therefore the number of elements of $\mathscr{M}$ exceeds

$$([t^{1/r}]+1)^r > t.$$

If p is prime such that $|\Gamma_p| \leqslant t$, then two distinct elements of $\mathscr{M}$ are congruent (mod p). Hence, p divides

$$N = |a_1^{m_1} \cdots a_r^{m_r} - a_1^{m'_1} \cdots a_r^{m'_r}|$$

for some $m_1, m_2, ..., m_r$ and $m'_1, m'_2, ..., m'_r$ satisfying

$$0 \leqslant m_i, \ m'_i \leqslant t^{1/r}.$$

Note that we may also assume that for all $i = 1, ..., r$ one of m_i or m'_i is zero since if we could not assume so, then p would divide some a_i and the contribution of such p's is $\omega(a_1 \cdots a_r)$.

We will say that a $2r$-tuple of numbers $(m_1, m_2, ..., m_r, m'_1, m'_2, ..., m'_r)$ is *compatible* if (i) m_i or m'_i is zero for all $i = 1, ..., r$, (ii) there exists at least one non-zero component and (iii) all non-zero components lie in the interval $[0, t^{1/r}]$.

For a fixed compatible $2r$-tuple, the number of primes dividing N is bounded by

$$\frac{\log N}{\log \log N} \leqslant \frac{t^{1/r}}{\log t} \, r \sum_{i=1}^{r} \log a_i.$$

The last inequality holds since

$$N \leqslant (a_1 a_2 \cdots a_r)^{2t^{1/r}}.$$

Taking into account that the number of compatible $2r$-tuples is $(2t^{1/r})^r$ which is $\ll 2^r t$ for $rt^{-1/r} = O(1)$, the total number of primes p that we are counting cannot exceed

$$O\left(\frac{t^{1+1/r} r 2^r \sum_{i=1}^{r} \log a_i}{\log t}\right).$$

This completes the proof of the lemma. ∎

Proof of Proposition 1.1. We apply Lemma 1.2 with $t = x^{r/(r+1)}/\log x$ and we find that the set of primes for which $|\Gamma_p| < p^{r/(r+1)}/\log p \leqslant t$ is $O(\pi(x)/\log^{1+1/r} x)$. Therefore, for almost all primes we have the desired inequality. ∎

We say that a sequence of integers $\{a_1, a_2, ..., a_r, ...\}$ is a *multiplicatively independent sequence*, if for any r, $\{a_1, a_2, ..., a_r\}$ are multiplicatively independent integers. If $r = r(p)$ is a given function of p, we will still denote by $|\Gamma_p|$ the order of the group generated by a_i, $i \leqslant r(p)$ (mod p). Note that this is well defined for all primes that do not divide any of the $a'_i s$ and the number of such primes $p \leqslant x$ is $\ll \sum_{i \leqslant r(x)} \log a_i$.

In 1969, H. Brown and H. Zassenhaus (see [2]) considered a problem which is the r-uniform version of the Artin Conjecture and conjectured that if $a_1=2$, $a_2=3$, ..., a_r is the rth prime number and if $r(p)\geqslant \log p$ then $|\Gamma_p|=p-1$ for almost all primes p.

Applying the Theorem of Burgess and Elliott on the least primitive root (see [7]), it is easy show that if $r(p)\geqslant \log^2 p \log\log^4 p$ then $|\Gamma_p|=p-1$ for almost all primes p.

We ask for the uniform estimate obtained using the same method and firstly note that the contribution of the the sizes of the a_i's cannot be too small. In fact:

PROPOSITION 1.3. *Let*

$$\Upsilon(r)=\min\left\{\sum_{i=0}^{r}\log a_i \mid a_1, ..., a_r, \textit{ multiplicatively independent r-tuple}\right\},$$

we have that

$$\Upsilon(r)=r\log r+O(r).$$

Proof. For any multiplicatively independent $a_1, ..., a_r$, we can assume $a_1\geqslant 1, ..., a_r\geqslant r$ and therefore

$$\sum_{i=1}^{r}\log a_i\geqslant \sum_{i=1}^{r}\log i=\log r!=r\log r-r+O(\log r).$$

The last identity is the Stirling formula. Therefore

$$\Upsilon(r)\geqslant r\log r+O(r).$$

Choosing $a_1=2, ..., a_r=p_r$, the rth prime, and applying the Prime Number Theorem, we see that

$$\begin{aligned}\Upsilon(r)&\leqslant \sum_{i=0}^{r}\log p_i=p_r+O(p_r\exp-c_1\sqrt{\log p_r})\\&=r\log r+O(r\exp-c_2\sqrt{\log r}).\end{aligned}$$

Hence the claim. ∎

Due to this result, whenever r grows with p, we will assume from now on that $a_1, ..., a_r$ are such that

$$\sum_{i=0}^{r}\log a_i\ll r\log r. \tag{1.2}$$

If in the proof of Proposition 1.1, we take

$$t = \left(\frac{x\varepsilon(x)}{2^{r(x)}(r(x))^2 \log r(x)} \right)^{r(x)/r(x)+1},$$

we are led to the following statement:

LEMMA 1.4. *Let $r = r(p)$ be any given function of p in the range of Lemma 1.2 and let $\{a_1, a_2, ..., a_r, ...\}$ be a multiplicatively independent sequence satisfying (1.2). For any function $\varepsilon(p)$ of p that tends to zero as p tends to ∞, we have that*

$$|\Gamma_p| \geqslant \left(\frac{p\varepsilon(p)}{2^r r^2 \log r} \right)^{r/(r+1)} \tag{1.3}$$

for all but $O(x\varepsilon(x)/\log t)$ primes $p \leqslant x$, uniformly with respect to r.

Setting $r(p) = \sqrt{\log p/\log 2}$ we optimize (1.3). Therefore we have

THEOREM 1.5. *With the same notation as above, we have that if $r(p) \geqslant \sqrt{\log p/\log 2}$ then*

$$|\Gamma_p| \geqslant \frac{p\varepsilon(p)}{\exp(2\sqrt{\log 2 \log p}) \log p \log\log p}$$

for all but $O(x(x)\, \varepsilon(x))$ primes $p \leqslant x$. More generally, if $\alpha \in (0, 1/2]$ and $r(p) \geqslant \log^\alpha p/\sqrt{\log 2}$, then

$$|\Gamma_p| \geqslant \frac{p\varepsilon(p)}{\exp(\sqrt{\log 2}(\log^\alpha p + \log^{1-\alpha} p)) \log^{2\alpha} p \log\log p}$$

for all but $O(\pi(x)\, \varepsilon(x))$ primes $p \leqslant x$.

2. THE RESULTS

In this section we improve the results stated in the introduction. They will be proven in Section 4:

THEOREM 2.1. *Let r be a fixed positive integer, let $\tau = (1 - \log 2)/2$ and let ψ be any function of p that tends steadily to infinity with p. We have that*

$$|\Gamma_p| \geqslant p^{r/(r+1)} \exp\left(\frac{\log^\tau p}{\exp(\psi(p)\sqrt{\log\log p})} \right).$$

for almost all p.

The case in which r grows with p can be treated in an analogous fashion. In particular

THEOREM 2.2. *With the same notation as in Lemma* 1.4, *let* $2\alpha \leqslant \tau = (1-\log 2)/)$ *and* $r(p) \geqslant \log^\alpha p/\sqrt{\log 2}$. *For any function* $\psi(x)$ *that tends steadily to infinity with* x,

$$|\Gamma_p| \geqslant p\, \frac{\exp(\log^{\tau-2\alpha} p/\exp(\psi(p)\sqrt{\log\log p}))}{\exp(\sqrt{\log 2}(\log^{1-\alpha} p + \log^\alpha p))},$$

for almost all p.

We conclude establishing the version of Theorem 2.1 under the assumption of the Generalized Riemann Hypothesis.

THEOREM 2.3. *For any* d *square-free and for* $a \in \mathbb{Q}^*$, *let* $\zeta_d(s)$ *denote the Dedekind zeta function of the Kummer field*

$$\mathbb{Q}(\zeta_d, a^{1/d}).$$

Suppose that there exists an integer $a \in \Gamma$ *such that, for every square-free* d, *the Generalized Riemann Hypothesis holds for* $\zeta_d(s)$. *Then if* $\psi(x)$ *is any function that tends steadily to* ∞ *as* $x \to \infty$,

$$|\Gamma_p| \geqslant \frac{p}{\psi(p)}$$

for all but $O(\pi(x)\log\psi(x)/\psi(\sqrt{x}))$ *primes* $p \leqslant x$.

It is natural to consider an extension of Artin's Conjecture for the more general r-rank case. R. Gupta and R. Murty considered in [8] the analogue of this problem for the groups of rational points of an elliptic curve.

On the GRH it is possible to prove the "r-rank Hooley's Theorem" so to determine density of the set of primes p for which $\Gamma_p = \mathbb{F}_p^*$. The Conjecture of H. Brown and H. Zassenhaus can also be answered under the assumption of the Generalized Riemann Hypothesis. This will be done by the author in a subsequent paper where it will be shown that on the GRH, for any function $r = r(p)$ that tends steadily to infinity with p, the first $r(p)$ primes generate a primitive root for almost all primes p.

Next we consider the sum

$$R_\Gamma(x) = \sum_{p \leqslant x} \frac{1}{|\Gamma_p|}$$

In the case $\Gamma = \langle a \rangle$, this quantity was considered by R. Murty and S. Srinivasan in [15] where they proved that the sum is $O(x^{1/2})$ and conjectured that it is $O(x^{\varepsilon})$. They also noticed that if the sum is $O(x^{1/4})$, then Artin's Conjecture follows. Theorem 2.1 allows us to obtain the following improvement.

COROLLARY 2.4. *There exists an absolute constant $\tau_2 > 0$ (we can taken $\tau_2 = 0.0306$) such that*

$$R_\Gamma(x) \ll \frac{x^{1/(r+1)}}{\log^{1+\tau_2/(r+1)} x}.$$

3. THE KEY LEMMA

In this section we state and prove the technical result that will be used to prove the results in Section 2:

By way of notation we set

$$\xi = \xi(x) = \log\log x,$$

THEOREM 3.1. *Define*

$$S(x, y, z) = \#\{p \leqslant x \mid \exists u \mid p-1, \text{ with } u \in [y, yz]\},$$

where without loss of generality we may assume that $y \leqslant \sqrt{x}$.

For any $\delta \in [0, 1/2)$ we let

$$\tau_\delta = 1 - (1/2 + \delta)(1 - \log(1/2 + \delta))$$
$$\tilde{\tau}_\delta = \delta/2 \log(1 + \delta)$$

so that $\tau_0 = (1 - \log 2)/2 = 0{,}1535640972$ and $\tilde{\tau}_0 = 0$. For any function $\psi(x)$ that tends steadily to infinity with x we have, uniformly with respect to y,

$$S(x, y, z) \ll x \left\{ \frac{o(1)}{\log^{1+\tilde{\tau}_\delta}} + \frac{\log z \log^{1-\tau_\delta} x}{\log^2(y/z)} \left\{ \exp\left(\psi \sqrt{\xi}\right) \right\} \right\} \qquad (3.1)$$

Before starting the proof of Theorem 3.1, we need to state some preliminary lemmas:

LEMMA 3.2. *Let $\Psi(x, y)$ be the number of natural numbers up to x whose greatest prime divisor is less than y. Then*

$$\Psi(x, y) \ll x \exp\left\{ -c_4 \frac{\log x}{\log y} \right\}$$

where c_4 is an absolute constant.

LEMMA 3.3. *Let $\Omega(n)$ be the number of prime divisors of a natural number n counted with multiplicity.*

For fixed $\sigma \in (0, 1)$ let $\rho_\sigma = 1 - \sigma(1 - \log \sigma)$. For any function $\psi(x)$ that tends steadily to infinity with x, we have that the number of integers n up to x such that

$$\Omega(n) < \sigma\xi + \psi\sqrt{\xi}$$

is

$$O\left(\frac{x}{\log^{\rho_\sigma} x} \exp(c_5 \psi \sqrt{\xi})\right)$$

where c_5 depends only on σ.

LEMMA 3.4. *Fix $\sigma \geqslant 0$ and let $\tilde{\rho}_\sigma = \sigma/4 \log(1 + \sigma/2)$. For every function $\psi(z)$ that tends steadily to infinity with x, the number of primes p up to x for which*

$$\Omega(p-1) > (1+\sigma)\xi + \psi\sqrt{\xi}$$

is $o(x/\log^{1+\tilde{\rho}_\sigma} x)$.

LEMMA 3.5. *For any natural number $m < x$, denote by $N(x, m)$ the number of solutions of*

$$p - 1 = qm$$

where p and q are prime numbers $\leqslant x$. We have that

$$N(x, m) \ll \frac{x}{\phi(m) \log^2(x/m)}.$$

Lemma 3.2 is a classical result due to N. G. de Bruijn (see [3]), Lemma 3.3 can be deduced quite directly from the work of G. H. Hardy and S. Ramanujan (see [11]) and Lemma 3.4 is due to P. Erdös (see [4]), while Lemma 3.5 is a standard application of the Selberg bound (see Halbertstam and Richert [10] at page 177).

Note that the constant $\tilde{\rho}_\sigma$ in Lemma 3.4 is not sharp while ρ_σ is probabily optimal. Nevertheless for the purpose of our application $\tilde{\rho}_\sigma$ is adequate.

Proof of Theorem 3.1. Consider the set

$$\mathcal{S} = \{p \leqslant x \mid \exists u \mid p-1, \text{ with } u \in [y, yz]\}.$$

Since the primes p up to $x/\log x$ contribute for $O(x/\log^2 x)$, we can assume that $p \geqslant x/\log x$ and $p \in \mathcal{S}$ means that

$$p-1=uv \qquad \text{with} \quad u \in [y, yz] \quad \text{and} \quad v \in \left[\frac{x}{yz \log x}, \frac{x}{y}\right].$$

Now let $\psi_1 = \psi_1(x)$ be a function that tends steadily to infinity with x to be determined later. If both

$$\Omega(v) > (\tfrac{1}{2}+\delta)\xi + \psi_1 \sqrt{\xi}$$

and

$$\Omega(v) > (\tfrac{1}{2}+\delta)\xi + \psi_1 \sqrt{\xi}$$

then

$$\Omega(p-1) > (1+2\delta)\xi + 2\psi_1 \sqrt{\xi}.$$

The number of $p \in \mathcal{S}$ for which this holds is

$$\leqslant \#\{p \leqslant x \mid \Omega(p-1) > (1+2\delta)\xi + 2\psi_1 \sqrt{\xi}\}$$

which by Lemma 3.4, is

$$o\left(\frac{x}{\log^{1+\tilde{\tau}_\delta} x}\right), \tag{3.2}$$

where $\tilde{\tau}_\delta = \tilde{\rho}_{2\delta}$.

Therefore, we will assume that $\Omega(v) \leqslant (\frac{1}{2}+\delta)\xi + \psi_1(x)\sqrt{\xi}$, since the condition $\Omega(u) \leqslant (\frac{1}{2}+\delta)\xi + \psi_1(x)\sqrt{\xi}$ follows in a similar way.

For a fixed u, the number of v's for which the maximum prime divisor is less then t is, by Lemma 3.2,

$$\ll \frac{x}{u} \exp\left\{-c_4 \frac{\log(x/u)}{\log t}\right\} \leqslant \frac{x}{u} \exp\left\{-c_4 \frac{\log(x/yz)}{\log t}\right\}. \tag{3.3}$$

The last estimate holds since $u < yz$, hence $x/u \geqslant x/yz$.

If we set

$$\log t = \frac{c_4 \log(x/yz)}{3 \log x},$$

then (3.3) becomes

$$\ll \frac{x}{u} \exp\left\{-3 \frac{\log(x/yz)}{\frac{\log(x/yz)}{\log\log x}}\right\} \ll \frac{1}{u} \frac{x}{\log^3 x}.$$

Therefore, the number of $p \in \mathcal{S}$ for which all the prime divisors of v are less then t is

$$\ll {\sum_u}' \frac{1}{u} \frac{x}{\log^3 x} \ll \frac{x \log z}{\log^3 x} \ll \frac{x}{\log^2 x} \tag{3.4}$$

(here the dash on the sum sign means that the sum is extended to all the values of u for $p \in \mathcal{S}$ and indeed $\sum_u' 1/u \ll \int_y^{yz} dt/t \ll \log z$).

Therefore we can assume that

$$p-1 = uv_1 q,$$

with u and v_1 in the desired range, $q > \exp(c_4 \log(x/yz)/3\xi)$ and

$$\Omega(v_1) < \tfrac{1}{2}\xi + \psi_1(x)\sqrt{\xi}.$$

From Lemma 3.5, we see that for fixed u and v_1, the number of possible solutions is

$$\ll \frac{x}{uv_1 \log^2(x/uv_1)}.$$

Now note that since $uv_1 < x/q < x \exp(-c_4(\log(x/yz))/3 \log\log x)$,

$$\frac{1}{\log^2(x/uv_1)} \ll \frac{\xi^2}{\log^2(x/yz)} \ll \frac{\xi^2}{\log^2 y/z}.$$

The last estimate follows from the assumption $y \leqslant \sqrt{x}$.

As an application of Lemma 3.3 we know that

$$T(h) = \#\left\{n \leqslant h \mid \Omega(n) < \left(\frac{1}{2}+\delta\right)\xi(h) + \psi_1\sqrt{\xi(h)}\right\}$$

$$\ll \frac{h}{\log^{\tau_\delta} h} \exp(c_5 \psi_1(h)\sqrt{\xi(h)})$$

where $\tau_\delta = \rho_{1/2+\delta}$. Partial summation implies that

$$\sum_{\Omega(n) < (1/2+\delta)\xi + \psi_1\sqrt{\xi}} \frac{1}{n} = \frac{T(x)}{x} + \int_1^x \frac{T(t)}{t^2}\, dt \ll (\log^{1-\rho_\delta} x) \exp(c_6 \psi_1 \sqrt{\xi}).$$

Therefore the number of $p \in \mathscr{S}$ with the required properties is

$$\ll \frac{x(\log\log x)^2}{\log^2(y/z)} \left(\sum_{\Omega(v_1) < 1/2\xi + \psi_1\sqrt{\xi}} \frac{1}{v_1} \right) \left(\sum_u{}' \frac{1}{u} \right)$$

$$\ll \frac{x \log z}{\log^2(y/z)} \log^{1-\tau\delta} x \{\exp(2c_6\psi_1\sqrt{\xi})\}. \tag{3.5}$$

The estimate in (3.1) follows by taking $\psi_1(x) = \psi(x)/3c_6$.

Finally, (3.2), (3.4) and (3.5) together complete the proof. ∎

Remark. Theorem 3.1 is a $p-1$-version of a Theorem due to Erdös and Hall (see [5]). A general statement on estimates of the number of $n \leqslant x$ with a divisor in a given range has been proven by Tenenbaum (see [17]).

4. Conclusion

Proof of Theorem 2.1. If we let $m_p = (p-1)/|\Gamma_p|$, then the proof of Proposition 1.1 implies that we can choose $\psi_1(x)$ that tends steadily to infinity with x such that for all but $O(\pi(x)/\psi_1(x))$ primes p up to x

$$m_p < x^{1/(r+1)}\psi_1(x).$$

Now we apply Theorem 3.1 with $yz = x^{1/(r+1)}\psi_1(x)$ and $\delta = 0$ and we get that for every function $\psi_2(x)$ that tends steadily to infinity with x

$$S(x, y, z) \ll \pi(x) \left\{ o(1) + \frac{\log z \log^{2-\tau} x \exp(\psi_2\sqrt{\xi})}{(\log x - \log z)^2} \right\}. \tag{4.1}$$

So the value $\log z = \log^\tau x/\exp(2\psi_2\sqrt{\xi})$ makes the right side of (4.1) $o(\pi(x))$.

Finally for almost all primes p,

$$m_p < y = x^{1/(r+1)}\psi_1(x) \exp\left(- \frac{\log^\tau x}{\exp(2\psi_2\sqrt{\xi})} \right).$$

Choosing $\psi_2 = \psi/3$ and ψ_1 sufficiently slow we get the claim. ∎

Proof of Theorem 2.2. As in the proof of Theorem 2.1 we let $m_p = (p-1)/|\Gamma_p|$. Then for all but $O(\pi(x)/\psi_1(x))$ primes p up to x

$$m_p < \psi_1(x) \exp(\sqrt{\log 2}(\log^\alpha x + \log^{1-\alpha} x)) \log^{2\alpha} x \log\log x, \tag{4.2}$$

where $\psi_1(x)$ is a function that tends steadily to infinity to be determined later.

Now we apply Theorem 3.1 with yz equal to the right hand side of (4.2) and $\delta=0$ and see that for every function $\psi_2(x)$ that tends steadily to infinity with x,

$$S(x, y, z)=o(\pi(x))+O\left(\frac{\log z \log^{1-\tau} x \exp(\psi_2\sqrt{\log\log x})}{(\log^{1-\alpha} x-\log z)\log^{1-\alpha} x}\right). \tag{4.3}$$

Now, if we set

$$\log z=\frac{\log^{\tau-2\alpha} x}{\exp(2\psi_2\sqrt{\log\log x})},$$

we see that the right hand side of (4.3) is $o(\pi(x))$.

Finally for almost all primes p,

$$m_p<y=\psi_1(x)\,\frac{\exp(\sqrt{\log 2}(\log^{\alpha} x+\log^{1-\alpha} x))\log^{2\alpha} x\log\log x}{\exp(\log^{\tau-2\alpha} x/\exp(2\psi_2\sqrt{\log\log x}))}.$$

Choosing $\psi_2=\psi/3$ and ψ_1 sufficiently slow we get the claim. ∎

Proof of Corollary 2.4. Let us break the sum into three parts:

$$\sum_{|\Gamma_p|\leqslant y}\frac{1}{|\Gamma_p|}+\sum_{y<|\Gamma_p|\leqslant z}\frac{1}{|\Gamma_p|}+\sum_{z<|\Gamma_p|\leqslant x}\frac{1}{|\Gamma_p|}. \tag{4.4}$$

By Lemma 1.2, the number of primes p for which $|\Gamma_p|\leqslant u$ is $O(u^{(r+1)/r}/\log u)$. Hence, by partial summation, the first sum is

$$O\left(\frac{y^{1/r}}{\log y}\right).$$

The third sum in (4.4) is trivially

$$O\left(\frac{1}{z}\,\frac{x}{\log x}\right),$$

while the middle sum is

$$\leqslant\frac{1}{y}\,S(x, x/z, z/y).$$

If we set

$$y=\frac{x^{r/r+1}}{\log^{\gamma} x},\qquad z=x^{r/r+1}\exp(\log^{\varepsilon} x),$$

then Theorem 3.1 implies that (4.4) is

$$\ll \frac{x^{1/(r+1)}}{(\log x)}\left(\frac{1}{\log^{\gamma/r} x}+\frac{1}{\log^{\tau_\delta - 2\varepsilon-\gamma} x}+\frac{o(1)}{\log^{\tilde{\tau}_\delta-\gamma} x}\right).$$

We optimize this by choosing δ_0 such that $\tilde{\tau}_{\delta_0}=\tau_{\delta_0}=\tau_2$ and $\gamma=\tau_2 r/(r+1)$. A calculation shows that $\tau_2=0.0306$ and this completes the proof. ∎

Proof of Theorem 2.3. We start by noticing that

$$|\Gamma_p| \geqslant \operatorname{ord}_p(a).$$

If $\operatorname{ord}_p(a)\geqslant p/\psi(p)$ then $(p-1)/\operatorname{ord}_p(a)\leqslant \psi(p)\leqslant \psi(\sqrt{x})$ say.

On the other hand, by Theorem 2.1, for all except $O(\pi(x)\log\psi(x)/\psi(\sqrt{x}))$ primes p up to x, we have that

$$(p-1)/\operatorname{ord}_p(a)\geqslant \sqrt{x}\exp(-\log^{\tau} x)$$

for some $\tau>0$.

So we want to estimate the sum

$$\sum_{\psi(\sqrt{x})\leqslant d\leqslant \sqrt{x}\exp(-\log^{\tau} x)} \#\{p\leqslant x \mid d=(p-1)/\operatorname{ord}_p(a)\}. \tag{4.5}$$

The condition

$$a^{(p-1)/d}\equiv 1 \pmod p$$

implies that $p\equiv 1 \pmod d$ and that a is a dth root in $\mathbb{F}_p^*$ so p splits completely in the extension $K_d=\mathbb{Q}(\zeta_d, a^{1/d})$ of $\mathbb{Q}$.

We denote by $\pi_d(x)$ the number of such primes p up to x. $\pi_d(x)$ is estimated by the Chebotarev Density Theorem. More precisely, we find, assuming the Generalized Riemann Hypothesis, that

$$\pi_d(x)=\frac{\operatorname{li}(x)}{[K_d:\mathbb{Q}]}+O(x^{1/2}\log dx)$$

(see for example [13] or [8]).

Therefore the sum in (4.5) is bounded by

$$\sum_{\psi(\sqrt{x})\leqslant d\leqslant \sqrt{x}\exp(-\log^{\tau} x)} \left\{\frac{\operatorname{li}(x)}{[K_d:\mathbb{Q}]}+O(x^{1/2}\log dx)\right\}$$

which is

$$\ll \pi(x)\left(\sum_{d\geqslant \psi(\sqrt{x})}\frac{1}{[K_d:\mathbb{Q}]}\right)+O\left(\frac{\pi(x)}{\psi(x)}\right).$$

Finally the claim would follow if we show that

$$\sum_{d>t} \frac{1}{[K_d:\mathbb{Q}]} \ll \frac{\log t}{t}. \tag{4.6}$$

From Hooley's work in [13], we find (regardless whether d is square-free or not) that

$$[K_d:\mathbb{Q}] \gg d\varphi(d).$$

Then the sum in (4.6) is

$$\ll \sum_{d>t} \frac{1}{d\varphi(d)} \ll \log t \sum_{d>t} \frac{1}{d^2},$$

since $\varphi(d) \gg d/\log d$ and this concludes the proof. ∎

Remark. Theorem 2.3 can be proven under the weaker Hypothesis that for all positive integers d, the Dedekind zeta function of the Galois field

$$\mathbb{Q}(\zeta_d, a_1^{1/d}, ..., a_r^{1/d})$$

has no zeroes to the right of the line $\Re(s) = r/(r+1)$.

Such an assumption allows one to determine an error term in the Chabotarev Density Theorem for the field $\mathbb{Q}(\zeta_d, a_1^{1/d}, ..., a_r^{1/d})$ of the order of $x^{r/(r+1)}$ and the proof is completed using the same argument.

We conclude by summarizing the results we established in this work for the classical case $r=1$:

THEOREM 4.1. *Let a be an integer which is not ± 1 nor a perfect square, and let* $\operatorname{ord}_p(a)$ *be the order of a* mod *p. Then for all $p \leqslant x$*

(i) $\operatorname{ord}_p(a) \geqslant \sqrt{p}/\psi(x)$ *with at most* $O(\pi(x)/(\psi(x))^2)$ *exceptions*;

(ii) $\operatorname{ord}_p(a) \geqslant \sqrt{p} \exp \log^\alpha p$ *with at most* $O(x/(\log x)^{1+\beta})$ *exceptions*;

(iii) $\sum_{p \leqslant x} 1/\operatorname{ord}_p(a) \ll \sqrt{x}/(\log x)^{1+\gamma}$;

(iv) *if, for any d square-free, we assume generalized Riemann Hypothesis for the Dedekind zeta function of the Kummer field* $\mathbb{Q}(\zeta_d, a^{1/d})$, *then* $\operatorname{ord}_p(a) \geqslant p/\psi(p)$ *with at most* $O(\pi(x) \log \psi(x)/\psi(x))$ *exceptions*;

where α, β and γ are suitably chosen positive number $(\alpha < (1-\log 2)/)$ *and* $\psi(x)$ *is any function that tends steadily to ∞ as $x \to \infty$.*

Let $K/\mathbb{Q}$ be a finite extension and let $\alpha_1, ..., \alpha_r \in \mathcal{O}_K$ be multiplicatively independent integers which are not ± 1 or perfect squares. We can again denote by Γ the subgroup of K^* generated by $\alpha_1, ..., \alpha_r$ and by $|\Gamma_{\mathfrak{p}}|$ the order of Γ modulo the prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$.

The same questions as in the rational case can be asked in this general setup. Estimates of $|\Gamma_{\mathfrak{p}}|$ have many applications. I. Shparlinski gives an account of some of these in [16]. He notices that argument of Lemma 1.2 yields

$$|\Gamma_{\mathfrak{p}}| > \left(\frac{N_{K/\mathbb{Q}}(\mathfrak{p})}{\psi(N_{K/\mathbb{Q}}(\mathfrak{p}))}\right)^{r/(r+1)}$$

($\psi \to \infty$), for almost all prime ideals $\mathfrak{p}$.

The results of this paper extend to the general case. It is enough to notice that almost all prime ideals $\mathfrak{p}$ with $N_{K/\mathbb{Q}}(\mathfrak{p}) \leqslant x$ have degree one.

Acknowledgments

A non-uniform version of Theorem 3.1 is due to Erdös and Murty (see [6]). I thank Professor Ram Murty for his suggestions and for a number of interesting observations. I thank Professor Igor Shparlinski for his comments during the final preparation of this paper.

References

1. E. Artin, Collected Papers, Addison-Wesley, Reading, MA, 1965.
2. H. Brown and H. Zassenhaus, Some empirical observations on primitive roots, *J. Number Theory* **3** (1971), 306–309.
3. N. G. de Bruijn, On the number of positive integers $\leqslant x$ and free of prime factors $> y$, *Indag. Math.* **13**, (1951), 50–60.
4. P. Erdös, On the normal number of prime factors of $p-1$ and some related problems concerning Euler's ϕ-function, *Quart. J. Math. Oxford Ser.* **6** (1935), 205–213.
5. P. Erdös and R. R. Hall, On the Möbius function, *J. Reine Angew. Math.* **315** (1980).
6. P. Erdös and M. R. Murty, On the order of a (mod p), unpublished, 1990.
7. D. A. Burgess and T. A. Elliott, The average of the least primitive root, *Mathematika* **15** (1968), 39–50.
8. R. Gupta and M. R. Murty, Primitive points on elliptic curves, *Comp. Mathematica* **58** (1986), 13–44.
9. R. Gupta and M. R. Murty, A remark on the Artin's conjecture, *Invent. Math.* **78**, No. 1 (1984), 127–130.
10. H. Halbertstam and H. E. Richert, "Sieve Methods," Academic Press, London/New York, 1974.
11. G. H. Hardy and S. Ramanujan, On the normal number of prime factors of a number n, *Quart. J. Math. Oxford Ser.* **48** (1917), 76–92.
12. D. R. Heat-Brown, Artin's Conjecture for primitive roots, *Quart. J. Math. Oxford Ser. (2)* **145** (1986), 27–38.
13. C. Hooley, "Application of Sieve Methods to the Theory of Numbers," Cambridge Univ. Press, Cambridge, U.K., 1976.
14. C. R. Matthews, Counting points modulo p for some finitely generated subgroups of algebraic group, *Bull. London Math. Soc.* **14** (1982), 149–154.

15. M. R. Murty and S. Srinivasan, Some remarks on Artin's conjecture, *Canad. Math. Bull.* **30**, No. 1 (1987), 80–85.
16. I. E. Shparlinski, "On Some Applications of Finitely Generated Semi-Groups," Proceedings of the First Algorithmic Number Theory Symposium (L. M. Adleman and M. Huang, Eds.), Ithaca, NY, 1994.
17. G. Tenenbaum, Sur la probabilité qu'un entier possède un diviseur dans un intervalle donné, *Comp. Math.* **51** (1984), 243–263.