Uniform Distribution Theory **1** (2006), no.1, 65–85

uniform distribution theory

ON THE DISTRIBUTION OF THE ORDER OF NUMBER FIELD ELEMENTS MODULO PRIME IDEALS

Volker Ziegler*

ABSTRACT. Let α be an algebraic integer in a number field K not a root of unity nor zero. In this paper we investigate under the assumption of the generalized Riemann hypothesis (GRH) the number of prime ideals $\mathfrak{p}$, such that the order $\mathrm{ord}_{\mathfrak{p}}(\alpha)$ lies in a fixed arithmetic progression. We also investigate the case, where $\mathfrak{p}$ has to satisfy some congruence conditions.

Communicated by Werner Georg Nowak

1. Introduction

Let $\mathcal{P}_g$ be the set of rational primes p such that g is a primitive root modulo p. In 1927 Artin conjectured that the set $\mathcal{P}_g$ is infinite, if $g \neq -1, 0, 1$ or if g is not a perfect square. Moreover, Artin conjectured that the set $\mathcal{P}_g$ has a natural density. But in the late 50's of the twentieth century, it turned out that the conjectured density, the Artin constant, is not consistent with numerical experiments (see Lehmer [10]). For more details on the history of Artin's constant and its correction factor see Stevenhagen [19].

In 1967 Hooley [6] proved Artin's conjecture under the assumption of the generalized Riemann hypothesis (GRH). In particular, Hooley also computed the natural density of $\mathcal{P}_g$. Let $\mathcal{P}_g(x)$ be the number of primes $p \in \mathcal{P}_g$ with $p \leq x$. Then

$$\mathcal{P}_g(x) = \frac{x}{\log(x)} \sum_{n=1}^{\infty} \frac{\mu(n)}{[\mathbb{Q}(\zeta_n, g^{1/n}) : \mathbb{Q}]} + O\left(\frac{x}{\log^2(x)}\right),$$

2000 Mathematics Subject Classification: Primary: 11N05, 11N13; Secondary: 11N36.

Keywords: Artin's conjecture, distribution of primes.

*The author gratefully acknowledges support from the Austrian Science Fund (FWF) under project Nr. P18079-N12.

where ζ_n is a n-th root of untiy. Moreover, Hooley showed if $g \neq \pm 1$ nor a perfect square then

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{[\mathbb{Q}(\zeta_n, g^{1/n}) : \mathbb{Q}]} = C(g_1, h)A(h),$$

where

$$A(h) = \prod_{p|h} \left(1 - \frac{1}{p-1}\right) \prod_{p \nmid h} \left(1 - \frac{1}{p(p-1)}\right),$$

$g = g_0^h$, g_0 not a perfect power, g_1 the square-free part of g and $C(g_1, h) = 1$ if $g_1 \not\equiv 1 \mod 4$ and

$$C(g_1, h) = 1 - \mu(|g_1|) \prod_{\substack{p|h \\ p|g_1}} \frac{1}{p-2} \prod_{\substack{p \nmid h \\ p|g_1}} \frac{1}{p^2-p-1}$$

otherwise. Note that for all products p denotes a rational prime. Usually $C(g_1, h)$ is called the correction factor and $A(1) \approx 0.3739558$ is called the Artin constant. It is easy to see that $A(h)$ and $C(g_1, h)$ are not zero and therefore $\mathcal{P}_g$ is infinite under (GRH).

Inspired by Hooley's proof many generalizations and variations have been considered. Let us give some examples. First, one may impose restrictions on the primes in $\mathcal{P}_g$, i.e. we only consider primes that lie in a given arithmetic progression. A second generalization is the following. Let K be some number field, α a fixed algebraic integer of K and $\mathcal{P}_\alpha(K)$ the set of primes $\mathfrak{p}$ for which the fixed algebraic integer α has order $\mathrm{N}\mathfrak{p} - 1$ in $\mathcal{O}/\mathfrak{p}\mathcal{O}$, where $\mathcal{O}$ is the ring of integers of K and $\mathrm{N}\mathfrak{p}$ is the Norm of $\mathfrak{p}$. Cooke and Weinberger [3] computed the natural density of $\mathcal{P}_\alpha(K)$ under the assumption of (GRH). Recently, Chinen and Murata [1, 2], respectively Moree [13, 14, 15] considered the distribution of the order of g modulo p, i.e. they investigated the set $\mathcal{P}_g(a, d)$ of primes p, for which $\mathrm{ord}_p(g) \equiv a \mod d$. By $\mathrm{ord}_p(g)$ we denote the smallest positive integer k such that $g^k \equiv 1 \mod p$, provided $p \nmid g$. For further variations and an introduction to Artin's conjecture see [12].

The aim of this paper is to consider the set of primes $\mathcal{P}_\alpha(K, F, C, a, d)$. Let K be some number field, F/K a Galois extension and C a union of conjugacy classes of $\mathrm{Gal}(F/K)$. Then $\mathcal{P}_\alpha(K, F, C, a, d)$ denotes the set of primes $\mathfrak{p}$ of K such that $(\mathfrak{p}, F/K) \in C$, $\mathfrak{p} \nmid (\alpha)$ and $\mathrm{ord}_{\mathfrak{p}}(\alpha) \equiv a \mod d$, where $(\mathfrak{p}, F/K)$ denotes the Frobenius automorphisms of $\mathfrak{p}$ and $\mathrm{ord}_{\mathfrak{p}}(\alpha)$ denotes the order of the algebraic integer α in $\mathcal{O}/\mathfrak{p}\mathcal{O}$. Now we can state the main theorem of this paper:

Theorem 1. *Let K be a number field, F/K a Galois extension and C a union of conjugacy classes of $\mathrm{Gal}(F/K)$. Let α be an algebraic integer of K not a root of unity nor zero and let a and d be rational integers. Let $\mathcal{P}_\alpha(K,F,C,a,d)(x)$ be the number of prime ideals with $\mathrm{N}\mathfrak{p} \le x$ and $\mathfrak{p} \in \mathcal{P}_\alpha(K,F,C,a,d)$. Then we have assuming (GRH)*

$$\mathcal{P}_\alpha(K,F,C,a,d)(x) = \frac{x}{\log(x)} \sum_{\substack{t=1\\(1+ta,d)=1}}^{\infty} \sum_{\substack{n=1\\(d,n)|a}}^{\infty} \frac{\mu(n)c(n,a,d,t)}{[F_{[d,n]t,nt}:K]} + O\left(\frac{x}{\log^{3/2}(x)}\right),$$

where $F_{s,t} := F(\zeta_s, \alpha^{1/t})$ and

$$\begin{aligned} c(n,a,d,t) &= |\{\sigma \in \mathrm{Gal}(F_{[d,n]t,nt}/K) \,:\, \sigma|_F \in C, \sigma|_{K_{nt,nt}} = \mathrm{id}, \sigma|_{\mathbb{Q}(\zeta_{dt})} = \sigma_{1+ta}\}| \\ &\le |C|. \end{aligned}$$

By σ_b we denote the automorphism induced by $\zeta_{dt} \mapsto \zeta_{dt}^b$. The constant implied by the O-term depends only on K, F, d and α.

In order to prove this theorem we closely follow the ideas of Moree [14]. Also ideas of Cooke and Weinberger [3] and Lenstra [11] are an essential part of the proof. In particular, these ideas are used to adapt Moree's method of proof to the algebraic integer case. In the next section we recall some facts on algebraic number theory and prove some auxiliary results, concerning degrees and discriminants of certain fields. We also investigate some properties of the Artin symbol. At the end of that section we state some results on the sums $\sum 1/(n\phi(n))$ and $\sum 1/\phi(n)$. By an application of Hooley's method (section 3) we determine the asymptotic behavior of the function $R_\alpha(K,F,C,t)(x)$. This function counts the primes $\mathfrak{p}$ with $\mathrm{N}\mathfrak{p} \le x$ such that $(\mathfrak{p}, F/K) \in C$, $\mathfrak{p} \nmid (\alpha)$ and $r_\mathfrak{p}(\alpha) := [(\mathcal{O}/\mathfrak{p}\mathcal{O})^* : \langle\bar{\alpha}\rangle] = t$, where $\bar{\alpha}$ is the reduction modulo $\mathfrak{p}$ of α and $\langle\bar{\alpha}\rangle$ is the group generated by $\bar{\alpha}$. We will show in section 4 that $\mathcal{P}_\alpha(K,F,C,a,d)(x)$ can be written as an infinite sum of R-functions defined above:

$$\mathcal{P}_\alpha(K,F,C,a,d)(x) = \sum_{t=1}^{\infty} R_\alpha(K,F_d,C_{a,d,t},t)(x),$$

where F_d respectively $C_{a,d,t}$ depends only on d respectively a,d and t. Moreover, we show that this sum restricted to $t \ge \sqrt{\log(x)}$ can be estimated by $O\left(\frac{x}{\log^{3/2}(x)}\right)$. In section 5 we complete the proof of Theorem 1. The last section shows how we can deduce the results of Moree [14, Theorem 1 and 2] using Theorem 1.

2. Preliminaries

In this section we investigate several lemmas that will help us to prove Theorem 1. The concern of the following lemmas is the relative degree of extensions and properties of Artin symbols. We also remind the reader of some facts about the distribution of primes and the sums $\sum 1/\phi(n)$ and $\sum 1/(n\phi(n))$.

First we want to fix some notations for the rest of the paper. As mentioned above K is a fixed number field, F/K a Galois extension with Galois group G and $C \subset G$ is a union of conjugacy classes of G. For a fixed $\alpha \in K$ we write $K_{t_1,t_2} := K(\zeta_{t_1}, \alpha^{1/t_2})$ and $F_{t_1,t_2} := FK_{t_1,t_2}$. In most cases we will be concerned with fields of the form $K_{t,t}$ and $F_{t,t}$. Remember that a and d denote positive integers. The ring of integers of K is denoted by $\mathcal{O}$. Let $\alpha \in \mathcal{O}$ not zero and $\mathfrak{p} \nmid (\alpha)$ some prime ideal of $\mathcal{O}$. We obviously have $\mathrm{ord}_{\mathfrak{p}}(\alpha) r_{\mathfrak{p}}(\alpha) = \mathrm{N}\mathfrak{p} - 1 = p^{f(\mathfrak{p})} - 1$, where p is the rational prime below $\mathfrak{p}$ and $f(\mathfrak{p})$ is the residue class degree of $\mathfrak{p}$ over p.

Note that by $e(\mathfrak{p})$ respectively $f(\mathfrak{p})$ we always denote the ramification index respectively the residue class degree of $\mathfrak{p}$ over p, the rational prime below $\mathfrak{p}$. It is well known that the primes $\mathfrak{p}$ which are ramified or have residue class degree $f(\mathfrak{p}) \geq 2$ over $\mathbb{Q}$ have zero density, i.e. $|\{\mathfrak{p} \,:\, \mathrm{N}\mathfrak{p} \leq x, e(\mathfrak{p})f(\mathfrak{p}) \geq 2\}| = o(x/\log(x))$. Indeed we can show more:

Lemma 1.

$$|\{\mathfrak{p} \,:\, \mathrm{N}\mathfrak{p} \leq x, e(\mathfrak{p})f(\mathfrak{p}) \geq 2\}| = O\left(\frac{\sqrt{x}}{\log(x)}\right)$$

Proof. We know that $|\{\mathfrak{p} \,:\, \mathrm{N}\mathfrak{p} \leq x, e(\mathfrak{p}) \geq 2\}| = O(1)$, so we investigate the set of primes $\mathfrak{p}$ with $f(\mathfrak{p}) \geq 2$. We find

$$|\{\mathfrak{p} : \mathrm{N}\mathfrak{p} \leq x, f(\mathfrak{p}) \geq 2\}| \leq [K:\mathbb{Q}]|\{p \in \mathbb{P} : p^2 \leq x\}| = O\left(\pi(\sqrt{x})\right) = O\left(\frac{\sqrt{x}}{\log(x)}\right),$$

where $\mathbb{P}$ denotes the set of rational primes. □

We also need a quantitative version of Chebotarev's density theorem. Since the unconditional form of this theorem is not sufficient for our purposes we use following version (see [7, 18]), which depends on (GRH).

Theorem 2. *Let $\pi(K,F,C)(x)$ denote the number of primes $\mathfrak{p}$ in K which are unramified in F/K, $\mathrm{N}\mathfrak{p} \leq x$ and $(\mathfrak{p}, F/K) \in C$. Then*

$$\pi(K,F,C)(x) = \mathrm{Li}(x)\frac{|C|}{|G|} + O\left(\frac{|C|}{|G|}\sqrt{x}\log\left(|d_F|x^{[F:\mathbb{Q}]}\right)\right)$$

under the assumption of (GRH), where d_F denotes the absolute discriminant of F.

By $\mathrm{Li}(x) := \int_2^x \frac{dx}{\log x}$ we denote the logarithmic integral. After these analytic preliminaries we pay our attention on algebraic topics. We start with the following lemma which describes the divisors t of $|r_{\mathfrak{p}}(\alpha)$ in terms of Artin symbols.

Lemma 2. *Let $e(\mathfrak{p})f(\mathfrak{p}) = 1$ and $\mathfrak{p} \nmid (\alpha)$. Then*

$$t|r_{\mathfrak{p}}(\alpha) \iff \left(\frac{\mathfrak{p}}{K_{t,t}/K}\right) = \mathrm{id}_K\,.$$

P r o o f. First, note that since $f(\mathfrak{p}) = 1$ we have $\mathrm{N}(\mathfrak{p}) = p$. Because of

$$t|r_{\mathfrak{p}}(\alpha)|\mathrm{N}\mathfrak{p} - 1 = p - 1$$

we have $\mathrm{N}\mathfrak{p} \equiv 1 \mod t$. Since $\mathcal{O}/\mathfrak{p}\mathcal{O} \simeq \mathbb{F}_p$ there exists a primitive root of $\mathcal{O}/\mathfrak{p}\mathcal{O}$. Therefore α has to be at least a t-th power of this primitive root, i.e. $\alpha^{(\mathrm{N}\mathfrak{p}-1)/t} \equiv 1 \mod \mathfrak{p}$. Now remember that $\mathfrak{p}$ is unramified and is of degree 1. We get

$$t|r_{\mathfrak{p}}(\alpha) \iff p \equiv 1 \mod t \text{ and } x^t \equiv \alpha \mod \mathfrak{p} \text{ is solvable.}$$

The $\Leftarrow$ conclusion directly follows from the definition of $r_{\mathfrak{p}}(\alpha)$ and the fact that $\mathcal{O}/\mathfrak{p}\mathcal{O}^*$ is cyclic.

Since t and $\mathfrak{p}$ are relative prime we obtain by [16, Lemma 4.8], that $\mathfrak{p}$ splits completely in $K(\zeta_t)$, i.e. $(\mathfrak{p}, K(\zeta_t)/K) = \mathrm{id}_K$ is equivalent to $p \equiv 1 \mod t$. Similarly we obtain by [16, Theorem 4.15] that $(\mathfrak{q}, K_{t,t}/K(\zeta_t)) = \mathrm{id}_{K(\zeta_t)}$ for every prime ideal $\mathfrak{q}$ above $\mathfrak{p}$ is the same as saying $x^t \equiv \alpha \mod \mathfrak{p}$ is solvable. Therefore we conclude

$$\mathfrak{p} \text{ splits completely in } K_{t,t} \iff \left(\frac{\mathfrak{p}}{K_{t,t}/K}\right) = \mathrm{id}_K \iff t|r_{\mathfrak{p}}(\alpha).$$

□

We have seen in the lemma above that we have to work with fields of the form $K_{rt,t}$. Lemma 3 and Lemma 5 give us information on the degree and the discriminant of such fields.

Lemma 3. *Let K be a number field and let $\alpha = \alpha_0^h$, with $\alpha_0 \in K$ not an exact power nor zero nor a root of unity. Then*

$$\frac{k\phi(kr)}{[K:\mathbb{Q}]!2h} \le [K_{kr,k} : K] \le k\phi(kr).$$

The right hand side inequality is deduced from

$$[K_{kr,k} : K] = [K(\zeta_{rk}, \alpha^{1/k}) : K(\zeta_{kr})][K(\zeta_{kr}) : K] \le k\phi(kr).$$

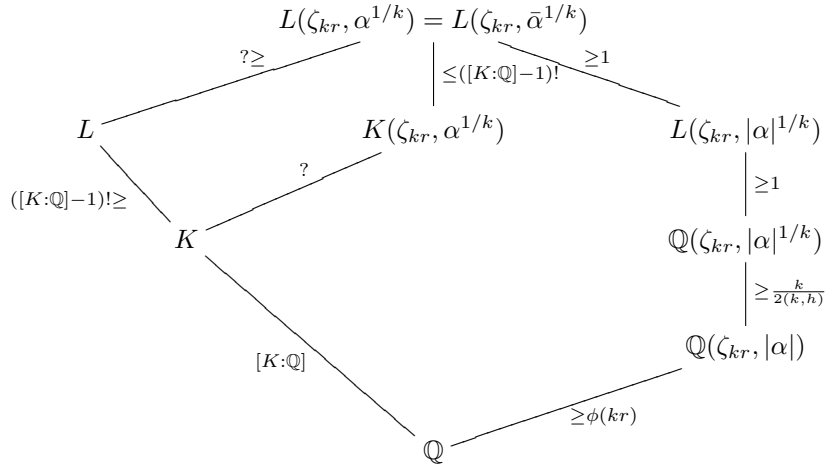
Before we start with the proof of the left hand side in Lemma 3, we prove following lemma due to Schinzel [17] in the case of $K = \mathbb{Q}$.

Lemma 4. *Let K be a totally real number field and consider the normal extension $K_{n,n} := K(\zeta_n, \alpha^{1/n})/K_n := K(\zeta_n)$, where $\alpha = \pm\alpha_0^h$ with h maximal, $\alpha_0 \neq 1$ and $\alpha_0 > 0$. Then $[K_{n,n} : K_n] \geq \frac{n}{2(n,h)}$.*

P r o o f. We follow the ideas of the proof of Lemma 4 in [17]. Let $n_1 = n/(n,h)$, then we know that $(\alpha^{1/n})^{n_1} \in K$. First, let us assume that the $+$ sign holds. Let $0 < t \in \mathbb{Z}$ be minimal such that $\alpha_0^{t/n_1} \in K(\zeta_n)$. Now we have $K \subset K(\alpha_0^{t/n_1}) \subset K(\zeta_n)$. By the fundamental theorem of Galois theory every intermediate field of an Abelian extension is also Abelian, therefore also normal. We conclude that with $K(\zeta_n)/K$ also $K(\alpha_0^{t/n_1})/K$ is normal. Because $K(\alpha_0^{t/n_1})$ has one real embedding, we know that all conjugates of α_0^{t/n_1} are real. Therefore the real extension $K(\alpha_0^{t/n_1})/K$ is of degree 1 or 2, hence $t = n_1$ or $t = n_1/2$. In other words we have proved the lemma in this case.

In the case for which the $-$ sign holds, the proof is analogous. We conclude that $\zeta_{2n}\alpha_0^{t/n_1} \in K(\zeta_n)$, hence $\alpha_0^{t/n_1} \in K(\zeta_{2n})$. Now one can complete the proof by the same arguments as above. □

Now we complete the proof of Lemma 3. In order to get an estimation of the degree we utilize the following diagram:



By L we denote the normal closure of K over $\mathbb{Q}$. All degrees can be estimated trivially or by Lemma 4 applied to $K = \mathbb{Q}(|\alpha|)$, $n = kr$ and $|\alpha|^r$ instead of α. If we go from $\mathbb{Q}$ to $L(\zeta_{kr}, \alpha^{1/k})$ along different paths in the diagram we obtain the lemma. □

Lemma 5. *Let K be a number field with absolute discriminant d_K. Then*

$$\log\left(|d_{K_{kr,k}}|\right) \leq \phi(rk)k\left(\log(|\mathrm{N}_{K/\mathbb{Q}}(\alpha)|) + [K:\mathbb{Q}](2\log(k)+\log(r)) + \log(|d_K|)\right)$$

and

$$\log\left(|d_{K_{k,k}}|\right) \leq \phi(k)k\left(\log(|\mathrm{N}_{K/\mathbb{Q}}(\alpha)|) + 2[K:\mathbb{Q}]\log(k) + \log(|d_K|)\right)$$

P r o o f. First we estimate the relative discriminant $d_{K_{rk,k}/K}$. Since $K_{rk,k}$ is the compositum of $K(\zeta_{kr})$ and $K(\alpha^{1/k})$ we have

$$d_{K_{rk,k}/K} | d_{K(\zeta_{kr})/K}^{[K_{rk,k}:K(\zeta_{kr})]} d_{K(\alpha^{1/k})/K}^{[K_{rk,k}:K(\alpha^{1/k})]}$$

and moreover

$$\begin{aligned} d_{K(\zeta_{rk})/K} \supseteq & d_{\mathbb{Q}(\zeta_{rk})/\mathbb{Q}} \supseteq \left((rk)^{\phi(rk)}\right), \\ d_{K(\alpha^{1/k})/K} \supseteq & \left(\prod_{\substack{i,j\leq k \\ i\neq j}} (\alpha^{1/k}\zeta_k^i - \alpha^{1/k}\zeta_k^j)\right) \supseteq \left(\alpha^{k-1}k^{\phi(k)}\right). \end{aligned}$$

Therefore we have

$$d_{K_{rk,k}/K} \supseteq \left((rk)^{\phi(rk)k} k^{\phi(k)\phi(rk)} \alpha^{(k-1)\phi(rk)}\right).$$

In order to obtain the absolute discriminant we use the formula

$$d_{F/k} = \mathrm{N}_{K/k}\mathrm{N}_{F/K}\left(\mathcal{D}_{F/K}\mathcal{D}_{K/k}\right) = \left(\mathrm{N}_{K/k} d_{F/K}\right) d_{K/k}^{[F:K]},$$

where $\mathcal{D}_{F/K}$ respectively $\mathcal{D}_{K/k}$ denotes the relative different of F/K respectively K/k, with $F \supset K \supset k$. Now we have

$$|d_{K_{rk,k}}| = |d_{K_{rk,k}/\mathbb{Q}}| = \left|\mathrm{N}_{K/\mathbb{Q}}\left(d_{K_{rk,k}/K}\right)\right| |d_{K/\mathbb{Q}}|^{[K_{rk,k}:K]}.$$

By the estimation above we get

$$\begin{aligned} \log|d_{K_{rk,k}}| \leq & (k-1)\phi(rk)\log(|\mathrm{N}_{K/\mathbb{Q}}(\alpha)|) + [K:\mathbb{Q}](\phi(rk)(k+\phi(k)))\log(k) \\ & + [K:\mathbb{Q}]\phi(rk)k\log(r) + \phi(rk)k\log(|d_K|) \\ \leq & \phi(rk)k\left(\log(|\mathrm{N}_{K/\mathbb{Q}}(\alpha)|) + [K:\mathbb{Q}](2\log(k)+\log(r)) + \log(|d_K|)\right). \end{aligned}$$

□

Since we have to consider sums of the type $\sum \mu(n)/[K_{nt,nt} : K]$ and because of Lemma 3 the following lemma will be helpful.

Lemma 6. *Let* $A(\alpha, t) = \sum_{n=1}^{\infty} \frac{\mu(n)}{[K_{nt,nt}:K]}$. *Then*

$$\sum_{t=1}^{y} A(\alpha, t) = 1 + O\left(\frac{1}{y}\right),$$

P r o o f. First we prove that $A(\alpha, t)$ converges absolutely and $A(\alpha, t) = O\left(\frac{1}{t\phi(t)}\right)$. This is obvious since $[K_{nt,nt} : K] \geq n\phi(n)t\phi(t)/(2h[K : \mathbb{Q}]!)$ and the next lemma.

Lemma 7. *The sum* $\sum_{n=1}^{\infty} \frac{1}{n\phi(n)}$ *converges and we have*

$$\sum_{n>x} \frac{1}{n\phi(n)} = O(1/x).$$

P r o o f. For a proof of Lemma 7 see [8, page 184]. □

By the second statement of Lemma 7 we know that

$$\sum_{t=1}^{\infty} A(\alpha, t) \tag{1}$$

converges absolutely and

$$\sum_{t=1}^{y} A(\alpha, t) = 1 + O\left(\frac{1}{y}\right),$$

provided the sum (1) is equal to 1. Since the sum converges absolutely we have

$$\begin{aligned}\sum_{t=1}^{\infty} A(\alpha, t) &= \sum_{t=1}^{\infty}\sum_{n=1}^{\infty} \frac{\mu(n)}{[K_{nt,nt} : K]} = \sum_{n=1}^{\infty}\sum_{d|n} \frac{\mu(d)}{[K_{n,n} : K]} \\ &= \sum_{n=1}^{\infty} \frac{1}{[K_{n,n} : K]} \sum_{d|n} \mu(d) = \frac{1}{[K_{1,1} : K]} = 1.\end{aligned}$$

□

Lemma 7 yields information on the sum $\sum 1/(n\phi(n))$. For later investigations we also need properties of the sum $\sum 1/\phi(n)$. This sum has been considered by Landau [8].

Lemma 8. *We have*

$$\sum_{n<x} \frac{1}{\phi(n)} = O(\log(x)).$$

3. Application of Hooley's method

The aim of this section is to compute the asymptotics of the function $R_\alpha(K,F,C,t)(x)$, i.e., we prove

Proposition 1. *Let K, F and C be as in Theorem 1 and let $t \leq x^{1/3}$ be some positive integer. Then*

$$\begin{aligned} R_\alpha(K,F,C,t)(x) &:= \left| \left\{ \mathfrak{p} \ : \ \mathrm{N}\mathfrak{p} \leq x, \mathfrak{p} \nmid (\alpha), r_{\mathfrak{p}}(\alpha) = t, \left(\frac{\mathfrak{p}}{F/K} \right) \in C \right\} \right| \\ &= \mathrm{Li}(x) \sum_{n=1}^{\infty} \frac{\mu(n)c(n)}{[F_{nt,nt} : K]} + O\left(\frac{x}{\log^2(x)} \right) + O\left(\frac{x \log(\log(x))}{\phi(t) \log^2(x)} \right), \end{aligned}$$

where $c(n) = |\{\sigma \in \mathrm{Gal}(F_{nt,nt}/K) \ : \ \sigma|_F \in C, \sigma|_{K_{nt,nt}} = \mathrm{id}\}| \leq |C|$.

By the inclusion exclusion principle and by Lemma 1, Lemma 2 and the fact that there are only finitely many $\mathfrak{p}$ with $\mathfrak{p}|(\alpha)$ we obtain (see [6, 13])

$$\begin{aligned} R_\alpha(K,F,C,t)(x) = \sum_{n=1}^{\infty} \mu(n) \left| \left\{ \mathfrak{p} : \mathrm{N}\mathfrak{p} \leq x, \left(\frac{\mathfrak{p}}{K_{nt,nt}/K} \right) = \mathrm{id}_K, \left(\frac{\mathfrak{p}}{F/K} \right) \in C \right\} \right| \\ + O\left(\frac{\sqrt{x}}{\log(x)} \right). \end{aligned} \tag{2}$$

In order to obtain an asymptotic for (2) we follow Hooley [6] and get

$$\begin{aligned} &R_\alpha(K,F,C,t)(x) = M_\alpha(K,F,C,t,\xi_1)(x) + O(M_\alpha(K,F,C,t,\xi_1,\xi_2)(x)) \\ &+ O(M_\alpha(K,F,C,t,\xi_2,\xi_3)(x)) + O(M_\alpha(K,F,C,t,\xi_3,x-1)(x)) + O\left(\frac{\sqrt{x}}{\log(x)} \right), \end{aligned}$$

where

$$\begin{aligned} M_\alpha(K,F,C,t,\xi)(x) &:= \left| \left\{ \mathfrak{p} : \mathrm{N}\mathfrak{p} \leq x, \left(\frac{\mathfrak{p}}{F/K} \right) \in C, t | r_{\mathfrak{p}}(\alpha), tq \nmid r_{\mathfrak{p}}(\alpha), q \leq \xi \right\} \right|, \\ M_\alpha(K,F,C,t,\xi,\eta)(x) &:= \left| \left\{ \mathfrak{p} : \mathrm{N}\mathfrak{p} \leq x, \left(\frac{\mathfrak{p}}{F/K} \right) \in C, tq | r_{\mathfrak{p}}(\alpha), \xi \leq q \leq \eta \right\} \right|, \end{aligned}$$

$\xi_1 = 1/6 \log(x)$, $\xi_2 = \frac{\sqrt{x}}{\log^2(x)}$, $\xi_3 = \sqrt{x} \log(x)$ and q denotes a rational prime. We start with the estimation of $M_\alpha(K,F,C,t,\xi_3,x-1)(x)$.

Lemma 9.

$$M_\alpha(K,F,C,t,\xi_3,x-1)(x) = O\left(\frac{x}{\log^2(x)}\right).$$

P r o o f. Let M denote the set of primes counted by $M(x) := M_\alpha(K,F,C,t,\xi_3, x-1)(x)$. By Lemma 1 we may assume $e(\mathfrak{p})f(\mathfrak{p}) = 1$. From the proof of Lemma 2 we know that $(\mathfrak{p}, K_{t,t}/K) = \mathrm{id}_K$ is equivalent to $\mathrm{N}\mathfrak{p} = p \equiv 1 \mod t$ and $\alpha^{(\mathrm{N}\mathfrak{p}-1)/t} = \alpha^{(p-1)/t} \equiv 1 \mod \mathfrak{p}$. Therefore we get the estimation

$$M(x) \le \left|\left\{\mathfrak{p} \,:\, \mathrm{N}\mathfrak{p} \le x, \alpha^{(\mathrm{N}\mathfrak{p}-1)/tq} \equiv 1 \mod \mathfrak{p}, \xi_3 \le q \le x-1\right\}\right|.$$

Then we have $\mathfrak{p} \supseteq \left(\alpha^{(\mathrm{N}\mathfrak{p}-1)/tq} - 1\right)$ for each $\mathfrak{p} \in M$. By combining all possibilities we get

$$\prod_{\mathfrak{p}\in M} \mathfrak{p} \supseteq \prod_{\substack{\zeta_3 \le q \le x-1 \\ q \text{ prime}}} \left(\alpha^{(\mathrm{N}\mathfrak{p}-1)/tq} - 1\right)$$

and if we apply the norm from K to $\mathbb{Q}$ to this relation we obtain

$$2^{M(x)} \le \prod_{\mathfrak{p}\in M} \mathrm{N}\mathfrak{p} \le \prod_{1\le m<\sqrt{x}/\log x} \mathrm{N}_{K/\mathbb{Q}}\left(\alpha^m - 1\right). \tag{3}$$

Let $A := \max_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})}\{|\sigma\alpha|\}$. Then

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha^m - 1) \le (A^m + 1)^{[K:\mathbb{Q}]} \le (2A)^{m[K:\mathbb{Q}]}$$

and by (3) we obtain

$$2^{|M|} \le (2A)^{[K:\mathbb{Q}]\sum m},$$

where the sum in the exponent is taken over all m with $1 \le m < \frac{\sqrt{x}}{\log x}$. Now we solve this inequality for $M(x)$ and obtain

$$M(x) \le \frac{\log(2A)}{\log(2)}[K:\mathbb{Q}] \sum_{m=1}^{\lfloor\sqrt{x}/\log(x)\rfloor} m = O\left(\frac{x}{\log^2(x)}\right).$$

□

Next, we consider the expression $M_\alpha(K,F,C,t,\xi_2,\xi_3)(x)$:

Lemma 10. *Let $t \le x^{1/3}$. Then*

$$M_\alpha(K,F,C,t,\xi_2,\xi_3)(x) = O\left(\frac{x\log(\log(x))}{\phi(t)\log^2(x)}\right).$$

P r o o f. Let us write $M(x) := M_\alpha(K, F, C, t, \xi_2, \xi_3)(x)$. From the proof of Lemma 2 we know

$$\begin{aligned} M(x) \leq & \sum_{\xi_2 \leq q < \xi_3} |\{\mathfrak{p} \,:\, \mathrm{N}\mathfrak{p} \leq x,\, e(\mathfrak{p})f(\mathfrak{p}) = 1, \mathfrak{p} \nmid (\alpha), \mathrm{N}\mathfrak{p} \equiv 1 \mod tq\}| \\ \leq & [K:\mathbb{Q}] \sum_{\xi_2 \leq q < \xi_3} |\{p \in \mathbb{P} \,:\, p \leq x,\, p \equiv 1 \mod tq\}| \,. \end{aligned}$$

We use the Brun-Titchmarsh inequality (see e.g. [4]) in order to estimate the last sum and get

$$\begin{aligned} M(x) \leq & [K:\mathbb{Q}] \sum_{\substack{\xi_2 \leq q < \xi_3 \\ q \text{ prime}}} \frac{3x}{\phi(tq)\log(x/tq)} \\ \leq & \frac{[K:\mathbb{Q}]}{\phi(t)} O\left(\frac{x}{\log x} \sum_{\substack{\xi_2 \leq q < \xi_3 \\ q \text{ prime}}} \frac{1}{\phi(q)} \right) \\ = & O\left(\frac{x \log(\log(x))}{\phi(t)\log^2(x)} \right), \end{aligned}$$

where the last equation is due to Hooley [6, page 211]. □

Note that the Lemmas 9 and 10 are unconditional, contrary to the next lemma.

Lemma 11. *Assume (GRH) and $t \leq x^{1/3}$. Then*

$$M_\alpha(K, F, C, t, \xi_1, \xi_2)(x) = O\left(\frac{x}{\log^2(x)} \right).$$

P r o o f. Again we write $M(x) := M_\alpha(K, F, C, t, \xi_1, \xi_2)(x)$. Then we have

$$\begin{aligned} M(x) \leq & \sum_{\xi_1 \leq q \leq \xi_2} \left| \left\{ \mathfrak{p} : \mathrm{N}\mathfrak{p} \leq x, \left(\frac{\mathfrak{p}}{F/K} \right) \in C, \left(\frac{\mathfrak{p}}{K_{tq,tq}/K} \right) = \mathrm{id}_K \right\} \right| \\ & + O\left(\frac{\sqrt{x}}{\log(x)} \right) \\ \leq & \sum_{\xi_1 \leq q \leq \xi_2} \left| \left\{ \mathfrak{p} : \mathrm{N}\mathfrak{p} \leq x, \left(\frac{\mathfrak{p}}{K_{tq,tq}/K} \right) = \mathrm{id}_K \right\} \right| + O\left(\frac{\sqrt{x}}{\log(x)} \right). \end{aligned}$$

Since Theorem 2, Lemmas 3 and 5 we have (remember $\alpha = \alpha_0^h$ with α_0 not an exact power)

$$\begin{aligned}
M(x) \leq & \sum_{\xi_1 \leq q \leq \xi_2} \frac{\mathrm{Li}(x)([K:\mathbb{Q}])!2h}{\phi(tq)tq} \\
& + O\left(\sum_{\xi_1 \leq q \leq \xi_2} \frac{[K:\mathbb{Q}]!2h}{\phi(tq)tq}\sqrt{x}\log\left(x^{[K_{tq,tq}:\mathbb{Q}]}d_{K_{tq,tq}}\right)\right) \\
=& O\left(\frac{1}{t\phi(t)}\frac{x}{\log(x)}\sum_{\xi_1 \leq q \leq \xi_2}\frac{1}{q^2}\right) + O\left(\sqrt{x}\log(x)\sum_{\xi_1 \leq q \leq \xi_2}\frac{[K_{tq,tq}:\mathbb{Q}]}{\phi(tq)tq}\right) \\
& + O\left(\sqrt{x}\sum_{\xi_1 \leq q \leq \xi_2}\left(\log(|\mathrm{N}_{K/\mathbb{Q}}(\alpha)|) + 2[K:\mathbb{Q}]\log(tq) + \log(|d_K|)\right)\right) \\
=& O\left(\frac{x}{\log(x)}\frac{1}{\xi_1}\right) + O\left(\sqrt{x}\pi(\xi_2)\log(x)\right) + O\left(\sqrt{x}\sum_{q\leq\xi_2}\log(q)\right) \\
=& O\left(\frac{x}{\log^2(x)}\right) + O\left(\sqrt{x}\sum_{q\leq\xi_2}\log(q)\right),
\end{aligned}$$

where $\pi(x)$ denotes the number of rational primes $\leq x$. Note that we also used the estimation $\sum_{x\geq n} 1/n^2 = O(1/x)$. It is well known (see e.g. [5, Theorem 414]) that $\theta(x) := \sum_{q\leq x}\log(q) = O(x)$, where the sum is taken over all primes $q \leq x$. Therefore we get

$$M(x) = O\left(\frac{x}{\log^2(x)}\right) + O\left(\sqrt{x}\theta(\xi_2)\right) = O\left(\frac{x}{\log^2(x)}\right)$$

□

Now we estimate the main term $M_\alpha(K, F, C, t, \xi_1)(x)$.

Lemma 12. *Assume (GRH) and $t \leq x^{1/3}$. Then*

$$M_\alpha(K, F, C, t, \xi_1)(x) = \mathrm{Li}(x)\sum_{n=1}^{\infty}\frac{\mu(n)c(n)}{[F_{nt,nt}:K]} + O\left(\frac{x}{\log^2(x)}\right).$$

P r o o f. Let $M(x) := M_\alpha(K, F, C, t, \xi_1)(x)$. By the inclusion exclusion principle and Lemma 1 we have

$$\begin{aligned} M(x) &= \sum_{n \in P(\xi_1)} \mu(n) \left| \left\{ \mathfrak{p} \,:\, \mathrm{N}\mathfrak{p} \le x, \left(\frac{\mathfrak{p}}{F/K} \right) \in C, \left(\frac{\mathfrak{p}}{K_{nt,nt}/K} \right) = \mathrm{id}_{K_{nt,nt}} \right\} \right| \\ &\quad + O\left(\frac{\sqrt{x}}{\log(x)} \right) \\ &= \sum_{n \in P(\xi_1)} \mu(n) \left| \left\{ \mathfrak{p} \,:\, \mathrm{N}\mathfrak{p} \le x, \left(\frac{\mathfrak{p}}{F_{nt,nt}/K} \right) \in \tilde{C} \right\} \right| + O\left(\frac{\sqrt{x}}{\log(x)} \right), \end{aligned}$$

where $\tilde{C}$ is the union of conjugacy classes of $\mathrm{Gal}(F_{nt,nt}/K)$ such that $\sigma \in \tilde{C}$ if and only if $\sigma|_F \in C$ and $\sigma|_{K_{nt,nt}} = \mathrm{id}_{K_{nt,nt}}$. Furthermore $P(\xi_1)$ denotes the set of all rational numbers that can be written as a product of primes q with $q \le \xi_1$. By Chebotarev's density theorem (see Theorem 2) we have

$$\begin{aligned} M(x) - \mathrm{Li}(x) &\sum_{n \in P(\xi_1)} \frac{\mu(n)c(n)}{[F_{nt,nt} : K]} \\ &= O\left(\sum_{n \in P(\xi_1)} \frac{|\tilde{C}|}{[F_{nt,nt} : K]} \sqrt{x} \log\left(x^{[F_{nt,nt}:\mathbb{Q}]} d_{F_{nt,nt}} \right) \right) \\ &= O\left(\sum_{n \in P(\xi_1)} \sqrt{x} \log(x) \right) + O\left(\sqrt{x} \sum_{n \in P(\xi_1)} \log(|d_{F_{nt,nt}}|) \right) \\ &= O\left(x^{5/6} \log(x) \right) + O\left(\sqrt{x} \sum_{n \in P(\xi_1)} \log(n) \right) + O\left(\sqrt{x} \sum_{n \in P(\xi_1)} \log(t) \right) \\ &= O\left(x^{5/6} \log(x) \right) + O\left(\sqrt{x} \log\left(\Gamma(x^{1/3}) \right) \right) = O\left(x^{5/6} \log(x) \right), \end{aligned}$$

since every element of $P(\xi_1)$ is less than $x^{1/3}$ (see e.g. [6, page 212]). Note that $\log\left(\Gamma(x^{1/3})\right) = O\left(x^{1/3} \log(x)\right)$ by Stirling's formula. Let us consider the sum

over all $n \in P(\xi_1)$:

$$\begin{aligned}\sum_{n\in P(\xi_1)} \frac{\mu(n)c(n)}{[F_{nt,nt}:K]} &= \sum_{n=1}^{\infty} \frac{\mu(n)c(n)}{[F_{nt,nt}:K]} + O\left(\sum_{n>\xi_1} \frac{\mu(n)c(n)}{[F_{nt,nt}:K]}\right)\\ &= \sum_{n=1}^{\infty} \frac{\mu(n)c(n)}{[F_{nt,nt}:K]} + O\left(\sum_{n>\xi_1} \frac{1}{n\phi(n)}\right)\\ &= \sum_{n=1}^{\infty} \frac{\mu(n)c(n)}{[F_{nt,nt}:K]} + O\left(\frac{1}{\log(x)}\right).\end{aligned}$$

The last equality holds because of Lemma 7. If we combine these estimations the proof of this lemma is complete. □

Proposition 1 follows now by the combination of the Lemmas 1, 9, 10, 11 and 12. □

4. Large indices

In this section we want to write the function $\mathcal{P}_\alpha(K,F,C,a,d)(x)$ as a sum of R-functions which we considered in section 3. Let $r_{\mathfrak{p}}(\alpha) = t$, since $r_{\mathfrak{p}}(\alpha)\operatorname{ord}_{\mathfrak{p}}(\alpha) = \mathrm{N}\mathfrak{p} - 1$ the condition $\operatorname{ord}_{\mathfrak{p}}(\alpha) \equiv a \mod d$ can also be written as $r_{\mathfrak{p}}(\alpha) = t$ and $ta + 1 \equiv \mathrm{N}\mathfrak{p} \mod dt$. If we sum the number of primes with these additional properties over all $t \geq 1$ we obtain

$$\mathcal{P}_\alpha(K,F,C,a,d)(x) = \sum_{t=1}^{\infty} V_\alpha(K,F,C,a,d,t)(x) + O\left(\frac{\sqrt{x}}{\log(x)}\right), \tag{4}$$

where

$$V_\alpha(K,F,C,a,d,t)(x) := \left|\left\{\mathfrak{p} \,:\, \mathrm{N}\mathfrak{p} \leq x, \mathfrak{p} \nmid (\alpha), \begin{pmatrix}\mathfrak{p}\\ F/K\end{pmatrix} \in C, r_{\mathfrak{p}}(\alpha) = t, \mathrm{N}\mathfrak{p} = p \equiv ta+1 \mod td\right\}\right|.$$

It is well known (see e.g. [9, page 200]) that $p \equiv a \mod d$ and $p \nmid d$ is equivalent to $(p, \mathbb{Q}(\zeta_d)/\mathbb{Q}) = \sigma_a$, where σ_a is induced by $\zeta_d \mapsto \zeta_d^a$. Note that if $1 + ta$ and d are not relative prime then the function $V_\alpha(K,F,C,a,d,t)(x)$ counts at most $[K:\mathbb{Q}]$ primes. Moreover these primes lie above a single prime

that divides d. On the other hand if $1+ta$ and d are relative prime the condition $\mathrm{N}\mathfrak{p} = p \equiv ta+1 \mod td$ can be written as

$$\left(\frac{\mathfrak{p}}{K(\zeta_{td})/K}\right)\Big|_{\mathbb{Q}(\zeta_{td})} = \left(\frac{\mathrm{N}\mathfrak{p}}{\mathbb{Q}(\zeta_{td})/\mathbb{Q}}\right) = \sigma_{1+ta}. \tag{5}$$

Now we can write the V-functions as a special R-function and obtain by Proposition 1 also an asymptotic formula for the V-functions.

Proposition 2. *The V-functions can be written as R-functions, i.e.*

$$V_\alpha(K, F, C, a, d, t)(x) = R_\alpha(K, F_d, C_{a,d,t}, t)(x),$$

where $F_d = F(\zeta_d)$ and

$$C_{a,d,t} := \left\{\sigma \in \mathrm{Gal}(F_d/K) \,:\, \left(\frac{\mathfrak{p}}{F_d/K}\right)\Big|_F \in C, \left(\frac{\mathfrak{p}}{F_d/K}\right)\Big|_{\mathbb{Q}(\zeta_{td})} = \sigma_{1+ta}\right\}.$$

Moreover, if we assume (GRH) and $t \le x^{1/3}$, then we have

$$\begin{aligned} V_\alpha(K, F, C, a, d, t)(x) = \mathrm{Li}(x) \sum_{\substack{n=1 \\ (d,n)|a}}^{\infty} \frac{\mu(n)c(n,a,d,t)}{[F_{[d,n]t,nt} : K]} + O\left(\frac{x}{\log^2(x)}\right) \\ + O\left(\frac{x\log(\log(x))}{\phi(t)\log^2(x)}\right), \end{aligned}$$

where $[d,n]$ denotes the least common multiple of d and n and where

$$\begin{aligned} c(n,a,d,t) &= |\{\sigma \in \mathrm{Gal}(F_{[d,n]t,nt}/K) \,:\, \sigma|_F \in C, \sigma|_{K_{nt,nt}} = \mathrm{id}, \sigma|_{\mathbb{Q}(\zeta_{dt})} = \sigma_{1+ta}\}| \\ &\le |C|. \end{aligned}$$

P r o o f. By the discussion above we see that the V-functions are special R-functions of the form described in the proposition. To obtain the statement about the asymptotic we apply Proposition 1. Note that $F(\zeta_d)_{nt,nt} = F_{[d,n]t,nt}$. Then we get

$$\begin{aligned} V_\alpha(K, F, C, a, d, t)(x) = \mathrm{Li}(x) \sum_{n=1}^{\infty} \frac{\mu(n)c(n,a,d,t)}{[F_{[d,n]t,nt} : K]} + O\left(\frac{x}{\log^2(x)}\right) \\ + O\left(\frac{x\log(\log(x))}{\phi(t)\log^2(x)}\right). \end{aligned}$$

Therefore we have to prove that $c(n,a,d,t)>0$ can only occur if $(d,n)|a$. First we note that $\sigma\in\mathrm{Gal}(F_{[d,n]t,nt}/K)$ is counted by $c(n,a,d,t)$, only if $\sigma|_{\mathbb{Q}(\zeta_{nt})}=\mathrm{id}_{\mathbb{Q}(\zeta_{nt})}$ and $\sigma|_{\mathbb{Q}(\zeta_{dt})}=\sigma_{1+ta}$, i.e.

$$\sigma|_{\mathbb{Q}(\zeta_{(d,n)t})}=\mathrm{id}_{\mathbb{Q}(\zeta_{(d,n)t})}=\sigma_{1+ta}|_{\mathbb{Q}(\zeta_{(d,n)t})}.$$

Therefore we have $\zeta_{(d,n)t}=\zeta_{(d,n)t}^{1+ta}$ or equivalently $\zeta_{(d,n)t}^{ta}=1$. But this is $(d,n)t|ta$, hence $(d,n)|a$. □

Next, we want to show that it is sufficient to compute the sum (4) only for "small" t. In particular we prove a variant of [13, Lemma 7] respectively [1, Lemma 2.4].

Lemma 13. *Let us assume (GRH) holds. Then we have*

$$\left|\{\mathfrak{p}\ :\ \mathrm{N}\mathfrak{p}\leq x,\mathfrak{p}\nmid(\alpha),r_{\mathfrak{p}}(\alpha)>\sqrt{\log(x)}\}\right|=O\left(\frac{x}{\log^{3/2}(x)}\right).$$

P r o o f. We follow a proof of Moree [13, Lemma 7]. Let $y=\lfloor\sqrt{\log(x)}\rfloor$. Then we have

$$\begin{aligned}E_\alpha(x):=&\left|\{\mathfrak{p}\ :\ \mathrm{N}\mathfrak{p}\leq x,\mathfrak{p}\nmid(\alpha)r_{\mathfrak{p}}(\alpha)>\sqrt{\log(x)}\}\right|\\=&|\{\mathfrak{p}\ :\ \mathrm{N}\mathfrak{p}\leq x\}|-\sum_{t=1}^{y}R_\alpha(K,K,\{\mathrm{id}_K\},t)(x)+O\left(\frac{\sqrt{x}}{\log(x)}\right).\end{aligned}$$

An application of Theorem 2 and Proposition 1 yields

$$\begin{aligned}E_\alpha(x)=&\frac{x}{\log(x)}+O\left(\frac{x}{\log^2(x)}\right)-\mathrm{Li}(x)\sum_{t=1}^{y}\sum_{n=1}^{\infty}\frac{\mu(n)c(n)}{[K_{nt,nt}:K]}\\&+O\left(\frac{x\log(\log(x))}{\log^2(x)}\sum_{t=1}^{y}\frac{1}{\phi(t)}+\frac{xy}{\log^2(x)}\right)\\=&\frac{x}{\log(x)}-\mathrm{Li}(x)+O\left(\frac{\mathrm{Li}(x)}{y}+\frac{x\log(\log(x))}{\log^2(x)}\sum_{t=1}^{y}\frac{1}{\phi(t)}+\frac{xy}{\log^2(x)}\right),\end{aligned}$$

because of Lemma 6. Note that in this case $c(n) = 1$ for each n (see Proposition 1). Now the proposition follows from the fact that $\sqrt{\log(x)} - 1 < y \leq \sqrt{\log(x)}$,

$$\sum_{t=1}^{y} \frac{1}{\phi(t)} = O(\log(y)) = O(\log(\log(x)))$$

(see Lemma 8) and

$$x/\log(x) - \mathrm{Li}(x) = O(x/\log^2(x)).$$

□

Now we can prove the main result of this section, which states that it is sufficient to sum up the sum (4) only for small indices t, i.e., we prove the following:

Proposition 3. *Let $x_1 = \sqrt{\log(x)}$ and assume (GRH). Then*

$$\mathcal{P}_\alpha(K, F, C, a, d)(x) = \sum_{\substack{t \leq x_1 \\ (1+ta,d)=1}} V_\alpha(K, F, C, a, d, t)(x) + O\left(\frac{x}{\log^{3/2}(x)}\right). \quad (6)$$

P r o o f. In the discussion at the beginning of this section we have already mentioned that in the case of $(1+ta, d) > 1$ the function $V_\alpha(K, F, C, a, d, t)(x)$ counts at most $[K : \mathbb{Q}]$ primes $\mathfrak{p}$ and these fulfill $\mathfrak{p}|(d)$. For fixed d we have

$$\sum_{(1+ta,d)>1} V_\alpha(K, F, C, a, d, t)(x) = O(1).$$

Moreover, by Lemma 13 we have

$$\sum_{t>x_1} V_\alpha(K, F, C, a, d, t)(x) = O\left(\frac{x}{\log^{3/2} x}\right).$$

By these two estimations and by (4) we obtain the proposition. □

5. Proof of the Main Theorem

The proof of Theorem 1 is now rather easy. We only have to combine the various lemmas and propositions. First, we have by Proposition 3 combined with Proposition 2 the relation

$$
\begin{aligned}
&\mathcal{P}_\alpha(K,F,C,a,d)(x)\\
=&\frac{x}{\log(x)}\sum_{\substack{t\le x_1\\(1+ta,d)=1}}\left(\left(\sum_{\substack{n=1\\(d,n)|a}}^{\infty}\frac{\mu(n)c(n,a,d,t)}{[F_{[d,n]t,nt}:K]}\right)+O\left(\frac{x}{\log^2(x)}+\frac{x\log(\log(x))}{\phi(t)\log^2(x)}\right)\right)\\
&+O\left(\frac{x}{\log^{3/2}(x)}\right)\\
=&\frac{x}{\log(x)}\sum_{\substack{t\le x_1\\(1+ta,d)=1}}\sum_{\substack{n=1\\(d,n)|a}}^{\infty}\frac{\mu(n)c(n,a,d,t)}{[F_{[d,n]t,nt}:K]}+O\left(\frac{x}{\log^{3/2}(x)}+\frac{x\log(\log(x))}{\log^2(x)}\sum_{t\le x_1}\frac{1}{\phi(t)}\right)\\
=&\frac{x}{\log(x)}\sum_{\substack{t=1\\(1+ta,d)=1}}^{\infty}\sum_{\substack{n=1\\(d,n)|a}}^{\infty}\frac{\mu(n)c(n,a,d,t)}{[F_{[d,n]t,nt}:K]}+O\left(\frac{x}{\log(x)}\sum_{t>x_1}\sum_{n=1}^{\infty}\frac{1}{[F_{[d,n]t,nt}:K]}\right)\\
&+O\left(\frac{x}{\log^{3/2}(x)}\right).
\end{aligned}
$$

Note that the last equation holds because of Lemma 8. It remains to estimate the first O-term in the last equation. We have

$$
\begin{aligned}
O\left(\sum_{t>x_1}\sum_{n=1}^{\infty}\frac{1}{[F_{[d,n]t,nt}:K]}\right)&=O\left(\sum_{t>x_1}\sum_{n=1}^{\infty}\frac{1}{n\phi(n)t\phi(t)}\right)\\
&=O\left(\sum_{t>x_1}\frac{1}{t\phi(t)}\right)=O\left(\frac{1}{x_1}\right)=O\left(\frac{1}{\sqrt{\log(x)}}\right),
\end{aligned}
$$

because of Lemma 7. Therefore the considered O-term can be estimated by $O\left(\frac{x}{\log^{3/2}(x)}\right)$ and Theorem 1 is proved. □

6. Two corollaries

In this last section we want to show that the results of Moree [14, Theorem 1 and 2] can easily be deduced from Theorem 1. Note that Moree proved these corollaries for rational g. For technical reasons we assume g to be integral. Let us note that for rational $g = g_0/g_1$ with $(g_0, g_1) = 1$ we define $\mathrm{ord}_g(p) = \min\{k : 0 < k \in \mathbb{Z},\ g_0^k \equiv g_1^k \mod p\}$. Moreover, the constant implied by the O-term would depend also on g_0 and g_1 in the rational case.

Corollary 1. *Let g be a fixed integer. Then the number of primes $p \le x$ such that $\operatorname{ord}_p(g) \equiv a \mod d$ is given by*

$$\mathcal{P}_g(a,d)(x) = \frac{x}{\log(x)} \sum_{\substack{t=1\\(1+ta,d)=1}}^{\infty} \sum_{\substack{n=1\\(d,n)|a}}^{\infty} \frac{\mu(n)\tilde{c}_g(1+ta,dt,nt)}{[\mathbb{Q}_{[d,n]t,nt}:\mathbb{Q}]} + O\left(\frac{x}{\log^{3/2}(x)}\right),$$

where, for $(b,f)=1$,

$$\tilde{c}_g(b,f,v) = \begin{cases} 1 & \text{if } \sigma_b|_{\mathbb{Q}(\zeta_f)\cap\mathbb{Q}_{v,v}} = \mathrm{id},\\ 0 & \text{otherwise,}\end{cases}$$

where σ_b is induced by $\zeta_f \mapsto \zeta_f^b$.

Proof. Apply Theorem 1 with $g=\alpha$, $K=F=\mathbb{Q}$ and $C=\{\mathrm{id}_{\mathbb{Q}}\}$. Then we only have to check that $c(n,a,d,t)=\tilde{c}_g(1+ta,dt,nt)$, which is easily done (see also the proof of Corollary 2). □

Corollary 2. *Let g be a fixed integer. Then the number of primes $p \le x$ and $p \equiv a_1 \mod d_1$ such that $\operatorname{ord}_p(g) \equiv a_2 \mod d_2$ is given by*

$$\begin{aligned}\mathcal{P}_g(a_1,d_1,a_2,d_2)(x) &= \frac{x}{\log(x)} \sum_{\substack{t=1,(1+ta_2,d_2)=1\\1+ta_2\equiv a_1 \mod (d_1,d_2t)}}^{\infty} \sum_{\substack{n=1\\(d,n)|a}}^{\infty} \frac{\mu(n)\tilde{c}_g(a_1,d_1,1+ta_2,d_2t,nt)}{[\mathbb{Q}_{nt,nt}(\zeta_{d_1},\zeta_{d_2t}):\mathbb{Q}]}\\ &\quad + O\left(\frac{x}{\log^{3/2}(x)}\right),\end{aligned}$$

where, for $(b_1,f_1)=(b_2,f_2)=1$ and $b_1 \equiv b_2 \mod (f_1,f_2))$, we have

$$\tilde{c}_g(b_1,f_1,b_2,f_2,v) = \begin{cases} 1 & \text{if } \tau|_{\mathbb{Q}(\zeta_{[f_1,f_2]})\cap\mathbb{Q}_{v,v}} = \mathrm{id},\\ 0 & \text{otherwise,}\end{cases}$$

where $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_{f_1},\zeta_{f_2})/\mathbb{Q})$ is induced by $\zeta_{f_1} \mapsto \zeta_{f_1}^{b_1}$ and $\zeta_{f_2} \mapsto \zeta_{f_2}^{b_2}$.

Proof. This time we apply Theorem 1 to $K=\mathbb{Q}$, $F=\mathbb{Q}(\zeta_{d_1})$, $C=\{\sigma_{a_1}\}$, $d=d_2$ and $a=a_2$. Note that $F_{[d_2,n]t,nt} = \mathbb{Q}(\zeta_{d_1},\zeta_{d_2t},\zeta_{nt},g^{1/nt}) = \mathbb{Q}_{nt,nt}(\zeta_{d_1},\zeta_{d_2t})$. First, we prove if $c(n,a_2,d_2,t) > 0$, then $1+ta_2 \equiv a_1 \mod (d_1,d_2t)$. Since $c(n,a_2,d_2,t)>0$ there exists a $\sigma \in \mathrm{Gal}(\mathbb{Q}_{nt,nt}(\zeta_{d_1},\zeta_{d_2t})/\mathbb{Q})$ such that $\sigma|_{\mathbb{Q}(\zeta_{d_1})} = \sigma_{a_1}$ and $\sigma|_{\mathbb{Q}(\zeta_{d_2t})} = \sigma_{1+ta_2}$, i.e. $\zeta_{(d_1,d_2t)}^{a_1} = \zeta_{(d_1,d_2t)}^{1+ta_2}$ or equivalently $a_1 \equiv 1+ta_2 \mod (d_1,d_2t)$.

Assume now $a_1 \equiv 1+ta_2 \mod (d_1,d_2t)$, then $c(n,a_2,d_2,t)=1$ if and only if there exists a $\sigma \in \mathrm{Gal}(\mathbb{Q}_{nt,nt}(\zeta_{d_1},\zeta_{d_2t}))$ such that $\sigma|_{\mathbb{Q}(\zeta_{d_1})} = \sigma_{a_1}$, $\sigma|_{\mathbb{Q}_{nt,nt}} = \mathrm{id}$ and $\sigma|_{\mathbb{Q}(\zeta_{d_2t})} = \sigma_{1+a_2t}$. By these conditions σ is uniquely determined. Now let

$\tau = \sigma|_{\mathbb{Q}(\zeta_{[d_1,d_2t]})}$. This τ is the same as the one defined in the corollary, with $b_1 = a_1$, $b_2 = 1 + a_2t$, $f_1 = d_1$ and $f_2 = d_2t$. Moreover, since σ is a lifting of τ, we deduce that τ has to be the identity on $\mathbb{Q}_{nt,nt}$, i.e., $\tau|_{\mathbb{Q}(\zeta_{[f_1,f_2]})\cap\mathbb{Q}_{v,v}} = \mathrm{id}$, with $v = nt$. □

REFERENCES

[1] CHINEN, K. – MURATA, L.: *On a distribution property of the residual order of a(mod p)*, J. Number Theory **105** (2004), no. 1, 60–81.

[2] CHINEN, K. – MURATA, L.: *On a distribution property of the residual order of a(mod p). II*, J. Number Theory **105** (2004), no. 1, 82–100.

[3] COOKE, G. – WEINBERGER, P.J.: *On the construction of division chaines in algebraic number fields, with applications to SL_2*, Commun. Algebra **3** (1975), 481–524.

[4] H. HALBERSTAM, H. – RICHERT, H.-E.: *Sieve Methods*, London Mathematical Society Monographs, No. **4**, Academic Press, London, New York, 1974.

[5] HARDY, G. – WRIGHT, E.: *An Introduction to the Theory of Numbers*, **5**th ed., Oxford at the Clarendon Press, Oxford, 1979.

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

[7] LAGARIAS, J. – ODLYZKO, A.: *Effective versions of the Chebotarev density theorem*, in: Algebraic number fields; L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), pp. 409–464. Academic Press, London, 1977.

[8] LANDAU, E.: *Über die zahlentheoretische Funktion $\varphi(n)$ und ihre Beziehung zum Goldbach'schen Satz*, Göttinger Nachrichten (1900), 177–186.

[9] LANG, S.: *Algebraic Number Theory*, Graduate Texts in Mathematics, Vol. **110** (second edition), Springer-Verlag, New York, 1994.

[10] LEHMER, D.H. – LEHMER, E.: *Heuristics, anyone?*, in: Studies in mathematical analysis and related topics (Essays in honor of George Pólya), pp. 202–210. Stanford University Press, Stanford, 1962.

[11] LENSTRA, H.: *On Artin's conjecture and Euclid's algorithm in global fields*, Invent. Math. **42** (1977), 201–224.

[12] MOREE, P.: *Artin's primitive root conjecture -a survey -*, availabel at: arXiv:math.NT/0412262.

[13] MOREE, P.: *On the distribution of the order and index of g (mod p) over residue classes*, J. Number Theory **114** (2005), 238–271.

[14] MOREE, P.: *On the distribution of the order and index of g (mod p) over residue classes. II*, J. Number Theory **117** (2006), 330–354.

[15] MOREE, P.: *On the distribution of the order and index of g (mod p) over residue classes. III*, J. Number Theory **120** (2006), 132–160.

[16] NARKIEWICZ, W.: *Elementary and Analytic Theory of Algebraic Numbers*, Monografie matematyczne, Vol. **54**, PWN - Polish Scientific Publishers, Warsaw, 1974.

[17] SCHINZEL, A.: *A refinement of a theorem of Gerst on power residues*, Acta Arith. **17** (1970), 161–168.

[18] SERRE, J.-P.: *Quelques applications du théorème de densité de Chebotarev*, Publ. Math., Inst. Hautes Étud. Sci. **54** (1981), 123–201.

[19] STEVENHAGEN, P.: *The correction factor in Artin's primitive root conjecture*, Journal de Theorie des Nombres **15** (2003), no. 1, 383–391.

Received August 4, 2006
Revised November 10, 2006

Volker Ziegler
BOKU Wien - University of Natural Resources and Applied Life Sciences, Vienna
Institute of Mathematics
Gregor-Mendelstrasse 33
A-1180 Vienna
AUSTRIA
E-mail: ziegler@finanz.math.tugraz.at