Available online at www.sciencedirect.com

SCIENCE DIRECT®

ELSEVIER

Journal of Number Theory 117 (2006) 330–354

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

On the distribution of the order and index of $g(\bmod p)$ over residue classes II

Pieter Moree

Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Deutschland, Germany

Received 1 August 2004; revised 29 March 2005

Available online 6 September 2005

Communicated by M. Pohst

Abstract

For a fixed rational number $g \notin \{-1, 0, 1\}$ and integers a and d we consider the set $N_g(a, d)$ of primes p for which the order of $g(\bmod p)$ is congruent to $a(\bmod d)$. It is shown, assuming the generalized Riemann hypothesis (GRH), that this set has a natural density $\delta_g(a, d)$. Moreover, $\delta_g(a, d)$ is computed in terms of degrees of certain Kummer extensions. Several properties of $\delta_g(a, d)$ are established in case d is a power of an odd prime. The result for $a = 0$ sheds some new light on the well-researched case where one requires the order to be divisible by d (with d arbitrary).

MSC: 11N37; 11N69; 11R45

1. Introduction

Let $g \notin \{-1, 0, 1\}$ be a rational number (this assumption on g will be maintained throughout this paper). For u a rational number, let $v_p(u)$ denote the exponent of p in the canonical factorisation of u (throughout the letter p will be used to indicate prime numbers). If $v_p(g) = 0$, then there exists a smallest positive integer k such that $g^k \equiv 1(\bmod p)$. We put $\mathrm{ord}_p(g) = k$. This number is the (*residual*) *order* of $g(\bmod p)$.

E-mail address: moree@mpim-bonn.mpg.de.

0022-314X/$ - see front matter
doi:10.1016/j.jnt.2005.06.006

The index of the subgroup generated by $g \bmod p$ inside the multiplicative group of residues $\bmod p$, $|(\mathbb{Z}/p\mathbb{Z})^\times : \langle g(\bmod p)\rangle|$, is denoted by $r_g(p)$ and called the *(residual) index* $\bmod p$ of g. Note that $\mathrm{ord}_g(p) r_g(p) = p-1$.

We let $N_g(a_1, d_1; a_2, d_2)(x)$ count the number of primes $p \leqslant x$ with $p \equiv a_1(\bmod d_1)$ and $\mathrm{ord}_g(p) \equiv a_2(\bmod d_2)$. For convenience denote $N_g(0,1;a,d)(x)$ by $N_g(a,d)(x)$. Although our main interest is in the behaviour of $N_g(a,d)(x)$ it turns out that sometimes it is fruitful to partition $N_g(a,d)(x)$ in sets of the form $N_g(a_1,d_1;a_2,d_2)(x)$ with a well-chosen d_1. Let $r|s$ be positive integers. By $K_{s,r}$ we denote the number field $\mathbb{Q}(\zeta_s, g^{1/r})$, where $\zeta_s = \exp(2\pi i/s)$. The main result of this paper is as follows (for notational convenience (a,b), $[a,b]$ will be written for the greatest common divisor, respectively, lowest common multiple of a and b and by (GRH) we indicate that GRH is assumed).

Theorem 1 (*GRH*). *Let* $(a_1, d_1) = 1$. *Then*

$$N_g(a_1,d_1;a_2,d_2)(x) = \delta_g(a_1,d_1;a_2,d_2)\frac{x}{\log x} + O_{d_1,d_2,g}\left(\frac{x}{\log^{3/2} x}\right),$$

for a number $\delta_g(a_1,d_1;a_2,d_2)$ *that is given by* (14).

Specialising to $a_1 = 0$ and $d_1 = 1$ the following result is obtained.

Theorem 2 (*GRH*). *We have*

$$N_g(a,d)(x) = \delta_g(a,d)\frac{x}{\log x} + O_{d,g}\left(\frac{x}{\log^{3/2} x}\right),$$

with

$$\delta_g(a,d) = \sum_{\substack{t=1 \\ (1+ta,d)=1}}^{\infty} \sum_{\substack{n=1 \\ (n,d)|a}}^{\infty} \frac{\mu(n) c_g(1+ta, dt, nt)}{[K_{[d,n]t,nt} : \mathbb{Q}]}, \tag{1}$$

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

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

where σ_b *is the automorphism of* $\mathbb{Q}(\zeta_f)$ *that sends* ζ_f *to* ζ_f^b.

In part I [M-I] this result was established, by a slightly different method, in case $3 \leqslant d \leqslant 4$ and explicit formulae for $\delta_g(a,3)$ and $\delta_g(a,4)$ were derived. By a different method some of the results for $d = 4$ with error term $O_g(x/(\log x \log\log x))$ and restricted values of g are established in [CM,MC], see also Corollary 1 of [M-I]. Chinen and Murata evaluate $\delta_g(a, 4)$ as a fourfold sum, whereas the present author evaluated it as a single sum.

It turns out that the numbers c_g appearing in (1) have a strong tendency to equal one. This motivates the following definition:

$$\delta_g^{(0)}(a,d) = \sum_{\substack{t=1 \\ (1+ta,d)=1}}^{\infty} \sum_{\substack{n=1 \\ (n,d)|a}}^{\infty} \frac{\mu(n)}{[K_{[d,n]t,nt} : \mathbb{Q}]}. \tag{2}$$

For example, if $d|a$, then σ_{1+ta} is the identity element of the Galois group of $\mathbb{Q}(\zeta_{dt})$ over $\mathbb{Q}$ and then trivially $\delta_g(a,d) = \delta_g^{(0)}(a,d)$.

Generically, the degree $[K_{[d,n]t,nt} : \mathbb{Q}]$ appearing in (2) equals $\varphi([d,n]t)nt$. On substituting this value in (2) a number $\delta(a,d)$ is obtained that no longer depends on g:

$$\delta(a,d) = \sum_{\substack{t=1 \\ (1+ta,d)=1}}^{\infty} \sum_{\substack{n=1 \\ (n,d)|a}}^{\infty} \frac{\mu(n)}{\varphi([d,n]t)nt}. \tag{3}$$

In [M-Av] it is shown that $\delta(a,d)$ is the average density of elements in a finite field having order $\equiv a \pmod{d}$. The number $\delta(a,d)$ can be a regarded as a naïve heuristic for $\delta_g(a,d)$. In part III it is shown that for 'generic' g we have $\delta_g(a,d) = \delta(a,d)$. In Section 6 this is established for odd prime powers in a more direct way (using that in this case the coefficients c_g are easily explicitly evaluated).

Theorem 3 (*GRH*). *Let $s \geqslant 1$ and q be an odd prime. Then for almost all integers g with $|g| \leqslant x$ we have $\delta_g(a, q^s) = \delta(a, q^s)$.*

In fact $\delta_g(a,q)$ can be explicitly evaluated (Theorem 4). For reasons of space this is only worked out in the case $g \in \mathcal{G}$, where $\mathcal{G}$ is the set of rational numbers g that cannot be written as $-g_0^h$ or g_0^h with $h > 1$ an integer and g_0 a rational number. Note that almost all integers g with $|g| \leqslant x$ are in $\mathcal{G}$. See Section 4.2 for a proof of Theorem 4.

Theorem 4 (*GRH*). *Let $q \nmid a$ be an odd prime and suppose that $g \in \mathcal{G}$. Put*

$$\varepsilon_g(\chi) = \begin{cases} 1 & \text{if } 2 \nmid D(g); \\ \frac{\chi(2)}{4} & \text{if } 4 \| D(g); \\ \frac{\chi(2)^2}{16} & \text{if } 8 | D(g), \end{cases}$$

where $D(g)$ denotes the discriminant of $\mathbb{Q}(\sqrt{g})$. If $q \nmid D(g)$, then $\delta_g(a,q)$ equals $\delta_g^0(a,q)$ which on its turn equals

$$\frac{q^2}{(q-1)(q^2-1)} - \frac{1}{(q-1)^2}\sum_{\chi\in G_q}\chi(-a)A_\chi\left(1+\varepsilon_g(\chi)\prod_{p|2D(g)}\frac{p(\chi(p)-1)}{p^3-p^2-p+\chi(p)}\right),$$

where the sum is over all characters of the character group G_q of Dirichlet characters modulo q and

$$A_\chi = \prod_{p:\chi(p)\neq 0}\left(1+\frac{[\chi(p)-1]p}{[p^2-\chi(p)](p-1)}\right).$$

If $q|D(g)$, then

$$\delta_g(a,q) = \frac{q^2}{(q-1)(q^2-1)} - \frac{1}{(q-1)^2}\sum_{\chi\in G_q}\chi(-a)A_\chi \times\left(1+\varepsilon_g(\chi)\left\{1+2\sum_b\overline{\chi(b)}\right\}\prod_{p|2D(g)/q}\frac{p(\chi(p)-1)}{p^3-p^2-p+\chi(p)}\right),$$

where the second sum is over all $1\leqslant b\leqslant q-1$ for which $(\frac{1-b}{q})=-1$.

The latter result together with Theorem 5 (proven in Section 5) allows one to explicitly evaluate $\delta_g(a,q^s)$ for any $g\in\mathcal{G}$ and $s\geqslant 1$.

Theorem 5 (*GRH*). *Let q be an odd prime. Then $\delta_g(a,q^s)=\delta_g(a,q)q^{1-s}$ for $s\geqslant 1$.*

Since the constants A_χ can be evaluated with high numerical precision (Section 2.1), the same applies to $\delta_g(a,q^s)$.

From [M-Av] it follows that in case q is an odd prime and $q\nmid a$:

$$q^{s-1}\delta(a,q^s) = \frac{q^2}{(q-1)(q^2-1)} - \frac{1}{(q-1)^2}\sum_{\chi\in G_q}\chi(-a)A_\chi. \tag{4}$$

This identity together with Theorem 4 results in the following corollary of Theorem 4:

Corollary 1 (*GRH*). *Let $q\nmid a$ be an odd prime and suppose that $g\in\mathcal{G}$. If $D(g)$ has a prime divisor $p\equiv 1(\mathrm{mod}\, q)$, then $\delta_g(a,q^s)=\delta(a,q^s)$.*

This corollary can be used to infer Theorem 3, on using that almost all integers g with $|g|\leqslant x$ satisfy $g\in\mathcal{G}$ and have $D(g)$ with at least one prime divisor p with

$p \equiv 1 (\mathrm{mod}\, q)$ (see Lemma 10). From Theorems 4 and 5 and (4) one sees that if $D(g)$ is large, then $|\delta_g(a, q^s) - \delta(a, q^s)|$ will be small.

In case $a = 0$ the density $\delta_g(a, d)$ can unconditionally be shown to exist and be evaluated, see, e.g., [M-div,O,Wie]. It turns out to be a positive rational number. Theorem 2 in case $a = 0$ gives rise, after some manipulation, to a double sum in which the summation parameters are rather restricted (cf. Eq. (24)). It turns out that a corresponding simple identity can be obtained (Proposition 4), which because of the restrictedness of the involved parameters can be unconditionally evaluated. This then gives some new insights in this (well-researched) case [M-div]. See also Section 7. In the final section the outcome of some relevant numerical experiments is recorded.

This paper is part of a trilogy, each paper considering a larger class of moduli d. Due to the inherent arithmetic complexity, results in later papers are less explicit than those in the earlier ones. Thus, only part of the results in the earlier papers follows from those of the later ones.

2. Preliminaries

2.1. Some notation

We recall some notation from our earlier papers [M-I,M-Av] on this topic. For any Dirichlet character χ of $(\mathbb{Z}/d\mathbb{Z})^*$, we let h_χ denote the Dirichlet convolution of χ and μ. As usual we let $L(s, \chi)$ denote the Dirichlet L-series for χ. For properties of h_χ the reader is referred to [M-I]. From [M-I], we furthermore recall that

$$C_\chi(h, r, s) = \sum_{(r,v)=1,\ s|v}^{\infty} \frac{h_\chi(v)(h, v)}{v\varphi(v)} \quad \text{and} \quad A_\chi = \prod_{p:\chi(p)\neq 0} \left(1 + \frac{[\chi(p) - 1]p}{[p^2 - \chi(p)](p - 1)}\right).$$

The constants A_χ turn out to be the basic constants for this problem. In many cases $A_\chi \in \mathbb{C}\backslash\mathbb{R}$, see [M-Av, Table 3]. It can be shown that

$$A_\chi \prod_{p|d} \left(1 - \frac{1}{p(p-1)}\right) = A \frac{L(2, \chi)L(3, \chi)}{L(6, \chi^2)} \prod_{r=1}^{\infty} \prod_{k=3r+1}^{\infty} L(k, \chi^r)^{\lambda(k,r)},$$

where A denotes the Artin constant and the numbers $\lambda(k, r)$ are non-zero integers that can be related to Fibonacci numbers [M-Fib]. The latter expansion of A_χ can be used to approximate the constant A_χ with high numerical accuracy (see [M-Av, Section 6]).

In [M-I, Lemma 10] it is shown that $C_\chi(h, r, s) = cA_\chi$, where c can be explicitly written down and is in $\mathbb{Q}(\zeta_{o_\chi})$. Here o_χ is the order of the character χ, i.e. the smallest positive integer k such that $\chi^k = \chi_0$, the trivial character.

We recall from [M-I] that, if $(b, f) = 1$,

$$\sum_{\substack{t \equiv b (\mathrm{mod}\, f) \\ t | v}} \mu\left(\frac{v}{t}\right) = \frac{1}{\varphi(f)} \sum_{\chi \in G_f} \overline{\chi(b)} h_\chi(v), \tag{5}$$

where the sum is over the characters in the character group G_f of $(\mathbb{Z}/f\mathbb{Z})^*$. It is well-known that $G_f \cong (\mathbb{Z}/f\mathbb{Z})^*$.

2.2. Preliminaries on algebraic number theory

We first review some properties of the Kronecker symbol (a not so often discussed symbol in books on number theory). To this end we first recall the definition of the Legendre and the Jacobi symbol. By definition the Legendre symbol $(\frac{n}{p})$, where $p \geqslant 3$ is a prime number and $n \in \mathbb{Z}$, $p \nmid n$, is equal to 1 if n is a quadratic residue mod p, and to -1 otherwise.

Let $m > 0$ be an odd integer relatively prime to n. The Jacobi symbol $(\frac{n}{m})$ is defined as the product of the Legendre symbols $(\frac{n}{m}) = (\frac{n}{p_1}) \dots (\frac{n}{p_s})$, where $m = p_1 \dots p_s$ and each p_i is a prime.

The Kronecker symbol $(\frac{c}{d})$ is defined for $c \in \mathbb{Z}$, $c \equiv 0 (\mathrm{mod}\, 4)$ or $c \equiv 1 (\mathrm{mod}\, 4)$, c not a square, and $d \geqslant 1$ an integer; if $b = p_1 p_2 \dots p_s$ is the decomposition of b as a product of primes, we put $(\frac{a}{-b}) = (\frac{a}{b}) = (\frac{a}{p_1})(\frac{a}{p_2}) \dots (\frac{a}{p_s})$. If p is an odd prime $(\frac{a}{p}) = 0$ when p divides a, while $(\frac{a}{p})$ is the Legendre symbol $(\frac{a}{p})$ when p does not divide a and, finally, $(\frac{a}{2}) = 1$ when $a \equiv 1 (\mathrm{mod}\, 8)$, while $(\frac{a}{2}) = -1$ when $a \equiv 5 (\mathrm{mod}\, 8)$. Then if a and b are such that both the Jacobi and Kronecker symbols are defined, then these symbols coincide. If a is odd, then $(\frac{a}{2})$ equals the Jacobi symbol $(\frac{2}{|a|})$. If $b > 0$, $(a, b) = 1$, a is odd, then $(\frac{a}{b}) = (\frac{b}{|a|})$, where the symbol on the right-hand side is the Jacobi symbol. Most importantly, if $b > 0$, $(a, b) = 1$ and $a = 2^r \tilde{a}$ with $\tilde{a}$ odd, then

$$\left(\frac{a}{b}\right) = \left(\frac{2}{b}\right)^r (-1)^{\frac{\tilde{a}-1}{2}\frac{b-1}{2}} \left(\frac{b}{|a|}\right),$$

where the symbols on the right-hand side are Jacobi symbols. The definition of the Kronecker symbol can be compactly given as follows:

Definition 1. Let $c \equiv 0 (\mathrm{mod}\, 4)$ or $c \equiv 1 (\mathrm{mod}\, 4)$, c not a square. Put

$$\left(\frac{c}{2}\right) = \begin{cases} 0 & \text{if } c \equiv 0 (\mathrm{mod}\, 4); \\ 1 & \text{if } c \equiv 1 (\mathrm{mod}\, 8); \\ -1 & \text{if } c \equiv 1 (\mathrm{mod}\, 8). \end{cases}$$

If p is an odd prime, then $(\frac{c}{p})$ is the Legendre symbol. If $n = \prod_{i=1}^r p_i^{e_i}$, then $(\frac{c}{n}) = \prod_{i=1}^r (\frac{c}{p_i})^{e_i}$; in particular $(\frac{c}{1}) = 1$.

Note that this definition reduces the computation of the Kronecker symbol to that of the Legendre symbol.

Let K be an abelian number field. By the Kronecker–Weber theorem there exists an integer f such that $K \subseteq \mathbb{Q}(\zeta_f)$. The smallest such integer is called the conductor of K. Note that $K \subseteq \mathbb{Q}(\zeta_n)$ iff n is divisible by the conductor. Note also that the conductor of a cyclotomic field is never congruent to $2 (\bmod 4)$. The following lemma allows one to determine all quadratic subfields of a given cyclotomic field (for a proof see e.g. [Wei, p. 263]).

Lemma 1. *The conductor of a quadratic number field is equal to the absolute value of its discriminant.*

Consider the cyclotomic extension $\mathbb{Q}(\zeta_f)$ of the rationals. There are $\varphi(f)$ distinct automorphisms each determined uniquely by $\sigma_a(\zeta_f)=\zeta_f^a$, with $1 \leqslant a \leqslant f$ and $(a, f)=1$. We need to know when the restriction of such an automorphism to a given quadratic subfield of $\mathbb{Q}(\zeta_f)$ is the identity. In this direction we have:

Lemma 2. *Let $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_f)$ be a quadratic field of discriminant Δ_d and b be an integer with $(b, f) = 1$. We have $\sigma_b|_{\mathbb{Q}(\sqrt{d})} = \mathrm{id}$ iff $(\frac{\Delta_d}{b}) = 1$, with $(\frac{\cdot}{\cdot})$ the Kronecker symbol.*

Proof. Using Lemma 1 we see that we can restrict to the case where $f = |\Delta_d|$. Define χ by $\chi(b) = \sigma_b(\sqrt{d})/\sqrt{d}$, $1 \leqslant b \leqslant |\Delta_d|$, $(b, \Delta_d) = 1$. Then χ is the unique non-trivial character of the character group of $\mathbb{Q}(\sqrt{d})$. As is well-known (see e.g. [N, p. 437]), the primitive character induced by this is $(\frac{\Delta_d}{b})$. Using Lemma 1, we see that χ is a primitive character mod $|\Delta_d|$. Thus $\chi(b) = (\frac{\Delta_d}{b})$. Now $\sigma_b|_{\mathbb{Q}(\sqrt{d})} = \mathrm{id}$ iff $\chi(b) = (\frac{\Delta_d}{b}) = 1$. □

Remark 1. Another way to prove Lemma 2 is to note that $\sigma_b|_{\mathbb{Q}(\sqrt{d})} = \mathrm{id}$ iff there exists a prime $p \equiv b (\bmod f)$ that splits completely in $\mathbb{Q}(\sqrt{d})$. It is well-known that there exists a prime $p \equiv b (\bmod f)$ that splits completely in the field $\mathbb{Q}(\sqrt{d})$ iff $(\frac{\Delta_d}{p}) = 1$ (see e.g. [Wei, p. 236]). Since $(\frac{\Delta_d}{p}) = (\frac{\Delta_d}{b})$, the result follows.

Remark 2. The action of σ on $\sqrt{d}$ can also be determined by relating $\sqrt{d}$ to a Gauss sum 'living' in $\mathbb{Q}(\zeta_f)$. It is straightforward to determine the action of σ on such a Gauss sum.

2.3. Preliminaries on field degrees

In order to explicitly evaluate certain densities in this paper, the following result will play a crucial role. Let $g_1 \neq 0$ be a rational number. By $D(g_1)$ we denote the discriminant of the field $\mathbb{Q}(\sqrt{g_1})$. The notation $D(g_1)$ along with the notation g_0, h and n_r introduced in the next lemma will reappear again and again in the sequel.

Lemma 3 (*Moree [M-I]*). *Write $g = \pm g_0^h$, where g_0 is positive and not an exact power of a rational. Let $D(g_0)$ denote the discriminant of the field $\mathbb{Q}(\sqrt{g_0})$. Put*

$$m = \begin{cases} D(g_0)/2 & \text{if } v_2(h) = 0 \text{ and } D(g_0) \equiv 4 (\bmod 8); \\ D(g_0)/2 & \text{if } v_2(h) = 1 \text{ and } D(g_0) \equiv 0 (\bmod 8); \\ [2^{v_2(h)+2}, D(g_0)] & \text{otherwise.} \end{cases}$$

and

$$n_r = \begin{cases} m & \text{if } g < 0 \text{ and } r \text{ is odd}; \\ [2^{v_2(hr)+1}, D(g_0)] & \text{otherwise.} \end{cases}$$

We have

$$[K_{kr,k} : \mathbb{Q}] = [\mathbb{Q}(\zeta_{kr}, g^{1/k}) : \mathbb{Q}] = \frac{\varphi(kr)k}{\varepsilon(kr,k)(k,h)},$$

where for $g > 0$ or $g < 0$ and r even we have

$$\varepsilon(kr,k) = \begin{cases} 2 & \text{if } n_r | kr; \\ 1 & \text{if } n_r \nmid kr, \end{cases}$$

and for $g < 0$ and r odd we have

$$\varepsilon(kr,k) = \begin{cases} 2 & \text{if } n_r | kr; \\ \frac{1}{2} & \text{if } 2|k \text{ and } 2^{v_2(h)+1} \nmid k; \\ 1 & \text{otherwise.} \end{cases}$$

Remark 3. Note that $n_r = n_{2^{v_2(r)}}$. Note that if h is odd, then $n_r = [2^{v_2(r)+1}, D(g)]$.

From Lemma 3 many consequences can be deduced.

Lemma 4. *Let v, w and z be natural numbers with $v|w$ and with z an odd divisor of w. Then $[K_{zw,v} : \mathbb{Q}] = z[K_{w,v} : \mathbb{Q}]$.*

Proof. The proof easily follows from Lemma 3 on observing that the odd part of n_r is squarefree and that $\varphi(zw) = z\varphi(w)$. $\square$

Lemma 5. *The intersection $\mathbb{Q}(\zeta_f) \cap K_{v,v}$ is equal to $\mathbb{Q}(\zeta_{(f,v)})$ or a quadratic extension thereof. More precisely,*

$$[\mathbb{Q}(\zeta_f) \cap K_{v,v} : \mathbb{Q}(\zeta_{(f,v)})] = \frac{\varepsilon([f,v],v)}{\varepsilon(v,v)}.$$

Proof. Clearly, this intersection field is abelian and contains $\mathbb{Q}(\zeta_{(f,v)})$. We have

$$[K_{[f,v],v}:\mathbb{Q}] = \frac{\varphi(f)[K_{v,v}:\mathbb{Q}]}{[\mathbb{Q}(\zeta_f)\cap K_{v,v}:\mathbb{Q}]}. \tag{6}$$

On noting that $\varphi((f,v))\varphi([f,v]) = \varphi(f)\varphi(v)$, it follows from Lemma 3 and (6) that

$$[\mathbb{Q}(\zeta_f)\cap K_{v,v}:\mathbb{Q}(\zeta_{(f,v)})] = \frac{[\mathbb{Q}(\zeta_f)\cap K_{v,v}:\mathbb{Q}]}{\varphi((f,v))} = \frac{\varepsilon([f,v],v)}{\varepsilon(v,v)}. \tag{7}$$

It is not difficult to infer from Lemma 3 that the latter quotient is either 1 or 2 (so the apparent possibility 4 does never arise). We conclude that $\mathbb{Q}(\zeta_f)\cap K_{v,v}$ is equal to $\mathbb{Q}(\zeta_{(f,v)})$ or a quadratic extension thereof. □

Lemma 6. *Let q be an odd prime, $s\geqslant 0$ and suppose $q\nmid v$. Put $q^* = (\frac{-1}{q})q$. Consider the following conditions*:

(i) $q|D(g_0)$, $s=0$ *and* $\frac{n_1}{q}|v$;
(ii) *If* $g<0$ *and* $2|v$, *then* $2^{\nu_2(h)+1}|v$.

We have

$$\mathbb{Q}(\zeta_{q^{s+1}})\cap K_{q^s v,q^s v} = \begin{cases}\mathbb{Q}(\sqrt{q^*}) & \text{if both i and ii are satisfied;}\\ \mathbb{Q}(\zeta_{q^s}) & \text{otherwise.}\end{cases}$$

Proof. By Lemma 5 we have $[\mathbb{Q}(\zeta_{q^{s+1}})\cap K_{q^s v,q^s v}:\mathbb{Q}(\zeta_{q^s})]=\varepsilon(q^{s+1}v,q^s v)/\varepsilon(q^s v,q^s v)$ and hence, by Lemma 3, $\mathbb{Q}(\zeta_{q^{s+1}})\cap K_{q^s v,q^s v}$ is a quadratic extension of $\mathbb{Q}(\zeta_{q^0})=\mathbb{Q}$ if conditions (i) and (ii) are satisfied and $\mathbb{Q}(\zeta_{q^{s+1}})\cap K_{q^s v,q^s v}=\mathbb{Q}(\zeta_{q^s})$ otherwise. Since $\mathbb{Q}(\sqrt{q^*})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_q)$, the result now follows. □

Remark 4. If $g>0$ or $g<0$ and v is odd, then condition (ii) is vacuously satisfied.

Lemma 7. *Let n be squarefree. Put $t_d=\prod_{p|(t,d)} p^{\nu_p(t)}$. The density of primes p such that $p\equiv 1+ta(\operatorname{mod} dt)$ and p splits completely in $K_{nt,nt}$ equals zero if $(d,n)\nmid a$ or $(1+ta,d)>1$, otherwise it equals*

$$\frac{c_g(1+ta,dt,nt)}{[K_{[d,n]t,nt}:\mathbb{Q}]} = \frac{c_g(1+ta,dt_d,nt)}{[K_{[d,n]t,nt}:\mathbb{Q}]}. \tag{8}$$

Proof. This follows from Chebotarev's density theorem together with the observation that the two systems of congruences

$$\begin{cases} x\equiv 1+ta(\operatorname{mod} dt)\\ x\equiv 1(\operatorname{mod} nt)\end{cases} \quad\text{and}\quad \begin{cases} x\equiv 1+ta(\operatorname{mod} dt_d)\\ x\equiv 1(\operatorname{mod} nt)\end{cases}$$

are equivalent. □

Lemma 8. *Assume that* $(b, f_1 f_2) = 1$, $f_1 | f_2$ *and*

$$\frac{[K_{[f_1,v],v} : \mathbb{Q}]}{\varphi(f_1)} = \frac{[K_{[f_2,v],v} : \mathbb{Q}]}{\varphi(f_2)}. \tag{9}$$

Then $c_g(b, f_1, v) = c_g(b, f_2, v)$.

Proof. By (6) the assumption (9) implies that

$$[\mathbb{Q}(\zeta_{f_1}) \cap K_{v,v} : \mathbb{Q}] = [\mathbb{Q}(\zeta_{f_2}) \cap K_{v,v} : \mathbb{Q}].$$

This, together with the assumption that $f_1 | f_2$ ensures that $\mathbb{Q}(\zeta_{f_1}) \cap K_{v,v} = \mathbb{Q}(\zeta_{f_2}) \cap K_{v,v} = L$, say, whence $L = \mathbb{Q}(\zeta_{(f_1,f_2)}) \cap K_{v,v}$. Since the map $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{f_1})/\mathbb{Q})$ that sends ζ_{f_1} to $\zeta_{f_1}^b$ and the map $\sigma' \in \mathrm{Gal}(\mathbb{Q}(\zeta_{f_2})/\mathbb{Q})$ that sends ζ_{f_2} to $\zeta_{f_2}^b$ act in the same way when restricted to $\mathbb{Q}(\zeta_{(f_1,f_2)})$, it follows that $\sigma_b|_{\mathbb{Q}(\zeta_{f_1})\cap K_{v,v}} = \sigma'_b|_{\mathbb{Q}(\zeta_{f_2})\cap K_{v,v}}$ and hence $c_g(b, f_1, v) = c_g(b, f_2, v)$. □

2.4. Remaining preliminaries

The following result is due to Wirsing [Wir].

Lemma 9 (*Wirsing [Wir]*). *Suppose $f(n)$ is a multiplicative function such that $f(n) \geqslant 0$, for $n \geqslant 1$, and such that there are constants γ_1 and γ_2, with $\gamma_2 < 2$, such that for every prime p and every $v \geqslant 2$, $f(p^v) \leqslant \gamma_1 \gamma_2^v$. Assume that as $x \to \infty$,*

$$\sum_{p \leqslant x} f(p) \sim \tau \frac{x}{\log x},$$

where $\tau > 0$ is a constant. Then, as $x \to \infty$,

$$\sum_{n \leqslant x} f(n) \sim \frac{e^{-\gamma\tau}}{\Gamma(\tau)} \frac{x}{\log x} \prod_{p \leqslant x} \left(1 + \frac{f(p)}{p} + \frac{f(p^2)}{p^2} + \frac{f(p^3)}{p^3} + \cdots\right),$$

where γ is Euler's constant and $\Gamma(\tau)$ denotes the gamma-function.

We use it to establish the following lemma.

Lemma 10. *Let $d \geqslant 3$. The number of integers $1 \leqslant g \leqslant x$ such that $D(g)$ has no prime divisor p with $p \equiv 1 (\mathrm{mod}\, d)$ is $O_d(x \log^{-1/\varphi(d)} x)$. The same assertion holds with $D(g)$ replaced by $D(-g)$.*

Proof. Denote the number of integers counted in the formulation of the lemma by $T_d(x)$. We define a multiplicative function $f_d(n)$ as follows:

$$f_d(p^\alpha) = \begin{cases} 0 & \text{if } 2 \nmid \alpha \text{ and } p \equiv 1 (\mathrm{mod}\, d); \\ 1 & \text{otherwise.} \end{cases}$$

Note that $T_d(x)=\sum_{g\leqslant x} f_d(g)$. Using Lemma 9, it then follows that

$$T_d(x) = O_d\left(\frac{x}{\log x}\prod_{p\leqslant x}\left(1+\frac{f_d(p)}{p}+\frac{f_d(p^2)}{p^2}+\cdots\right)\right)$$
$$= O_d\left(\frac{x}{\log x}\prod_{\substack{p\leqslant x\\ p\not\equiv 1(\operatorname{mod} d)}}\left(1+\frac{1}{p}\right)\right).$$

Since by Mertens' theorem for arithmetic progressions (cf. [Wil]) we have

$$\prod_{\substack{p\leqslant x\\ p\equiv a(\operatorname{mod} d)}}\left(1+\frac{1}{p}\right)\sim c_{a,d}\log^{\frac{1}{\varphi(d)}} x, \quad x\to\infty,$$

for some $c_{a,d}>0$, the result follows. □

3. The proofs of Theorems 1 and 2

In this section we analyse the growth behaviour of the functions $N_g(a,d)(x)$ and $N_g(a_1,d_1;a_2,d_2)(x)$. Throughout we restrict to those primes p with $v_p(g)=0$. Let $\omega(d)=\sum_{p\mid d}1$ denote the number of distinct prime divisors of d.

Let

$$V_g(a,d;t)(x)=\#\{p\leqslant x:\ r_g(p)=t,\ \ p\equiv 1+ta(\operatorname{mod} dt)\}.$$

Note that $N_g(a,d)(x)=\sum_{t=1}^{\infty}V_g(a,d;t)(x)$. If $(1+ta,d)>1$ then there is at most one prime counted by $V_g(a,d;t)(x)$ and this prime has to divide d. It follows that $N_g(a,d)(x)=\sum_{\substack{t=1\\ (1+ta,d)=1}}^{\infty}V_g(a,d;t)(x)+O(\omega(d))$. Let $x_1=\sqrt{\log x}$. Assume GRH. By [M-I, Lemma 7] it follows that $\#\{p\leqslant x:\ r_g(p)>x_1\}=O_g(x\log^{-3/2}x)$. We thus infer that

$$N_g(a,d)(x)=\sum_{\substack{t\leqslant x_1\\ (1+ta,d)=1}}V_g(a,d;t)(x)+O_{g,d}\left(\frac{x}{\log^{3/2}x}\right). \tag{10}$$

For fixed t the term $V_g(a,d;t)$ can be estimated by a variation of Hooley's classical argument [H]. However, we need to carry this out with a certain uniformity. This requires one to merely keep track of the dependence on t of the various estimates. This results in the following lemma.

Lemma 11 (*GRH*). *For* $t \leqslant x^{1/3}$ *we have*

$$V_g(a,d;t)(x) = \frac{x}{\log x} \sum_{\substack{n=1 \\ (n,d)|a}}^{\infty} \frac{\mu(n) c_g(1+ta, dt, nt)}{[K_{[d,n]t,nt} : \mathbb{Q}]} + O_{g,d}\left(\frac{x \log\log x}{\varphi(t)\log^2 x} + \frac{x}{\log^2 x}\right).$$

Proof. Let $M_g'(x,y) = \#\{p \leqslant x : p \equiv 1 + ta (\operatorname{mod} dt),\ t | r_g(p),\ qt \nmid r_g(p),\ \forall q \leqslant y\}$ and $M_g(x,y,z) = \#\{p \leqslant x : \exists q,\ y \leqslant q \leqslant z,\ qt | r_g(p)\}$, where q denotes a prime number. Note that

$$V_g(a,d;t)(x) = M_g'(x,\xi_1) + O(M_g(x,\xi_1,\xi_2)) + O(M_g(x,\xi_2,\xi_3)) + O\left(M_g\left(x,\xi_3,\frac{x-1}{t}\right)\right).$$

We take $\xi_1 = \log x/6$, $\xi_2 = \sqrt{x}\log^{-2} x$ and $\xi_3 = \sqrt{x}\log x$. The three error terms were estimated in the proof of Theorem 4 of [M-I]. Taking them together it is found that

$$V_g(a,d;t)(x) = M_g'(x,\xi_1) + O_{g,d}\left(\frac{x \log\log x}{\varphi(t)\log^2 x} + \frac{x}{\log^2 x}\right). \tag{11}$$

By inclusion and exclusion it follows that

$$M_g'(x,\xi_1) = \sum_{P(n) \leqslant \xi_1} \mu(n) \#\{p \leqslant x : p \equiv 1 + ta (\operatorname{mod} dt),\ nt | r_g(p)\},$$

where $P(n)$ denotes the greatest prime factor of n. The integers n counted in the latter sum are all less than $x^{1/3}$ (cf. (6) of [H]). The counting functions in the latter sum can be estimated by an effective form of Chebotarev's density theorem, cf. Theorem 3 of [M-I] and the discussion immediately following this theorem. This yields that

$$\#\{p \leqslant x : p \equiv 1 + ta (\operatorname{mod} dt),\ nt | r_g(p)\} = \frac{c_g(1+ta, dt, nt)}{[K_{[d,n]t,nt} : \mathbb{Q}]} \operatorname{Li}(x) + O(\sqrt{x}\log x),$$

where the implied constant depends at most on g and d. Indeed, applying Theorem 3 of [M-I] results in an error term of $O(\sqrt{x}\log(d_L x^{[L:\mathbb{Q}]})/[L:\mathbb{Q}])$, with an absolute implied constant and $L = K_{[d,n]t,nt}$. On invoking Lemma 3 and [M-I, Lemma 2] it follows that this is $O_{d,g}(\sqrt{x}\log x)$. Proceeding as in [H, Section 6] it is then inferred that

$$M_g'(x,\xi_1) = \frac{x}{\log x} \sum_{n=1}^{\infty} \frac{\mu(n) c_g(1+ta, dt, nt)}{[K_{[d,n]t,nt} : \mathbb{Q}]} + O_{g,d}\left(\frac{x}{\log^2 x}\right). \tag{12}$$

If $nt|r_g(p)$, then $p \equiv 1 (\operatorname{mod} nt)$. By the Chinese remainder theorem it now follows that if $(n,d)|a$ then $\#\{p \leqslant x : p \equiv 1 + ta (\operatorname{mod} dt),\ nt|r_g(p)\}$ is finite for every x and hence $c_g(1+ta, dt, nt) = 0$ (an alternative way to see this is to note that in this case σ_{1+ta} does not act like the identity on $\mathbb{Q}(\zeta_{nt})$). It follows that in the sum in (12) we can restrict to those n satisfying $(n,d)|a$. On taking this into account and combining (11) and (12), the result follows. $\square$

It is now straightforward to establish Theorem 2.

Proof of Theorem 2. Recall that $x_1 = \sqrt{\log x}$. Combination of (10) and Lemma 11 yields

$$N_g(a,d)(x) = \frac{x}{\log x} \sum_{\substack{t \leqslant x_1 \\ (1+ta,d)=1}} \sum_{\substack{n=1 \\ (n,d)|a}}^{\infty} \frac{\mu(n) c_g(1+ta, dt, nt)}{[K_{[d,n]t,nt} : \mathbb{Q}]} + O_{g,d}\left(\frac{x}{\log^{3/2} x}\right). \quad (13)$$

Denote the latter double sum by $D(x)$. By Lemma 3 and [M-I, Lemma 5] we find

$$D(x) = \delta_g(a,d) + O\left(\sum_{t > x_1} \frac{h}{t\varphi(t)}\right) = \delta_g(a,d) + O\left(\frac{h}{\sqrt{\log x}}\right).$$

On inserting the latter estimate in (13) the proof is then completed. $\square$

A variation of the above (but notationally rather more awkward and hence we only sketch it) gives Theorem 1 with

$$\delta_g(a_1,d_1;a_2,d_2) = \sum_{\substack{t=1,\ (1+ta_2,d_2)=1 \\ 1+ta_2 \equiv a_1 (\operatorname{mod} (d_1,d_2 t))}}^{\infty} \sum_{n=1}^{\infty} \frac{\mu(n) c_g(a_1, d_1, 1+ta_2, d_2 t, nt)}{[K_{nt,nt}(\zeta_{d_1}, \zeta_{d_2 t}) : \mathbb{Q}]}, \quad (14)$$

where for $(b_1, f_1) = (b_2, f_2) = 1$ and $b_1 \equiv b_2 (\operatorname{mod} (f_1, f_2))$, we define

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

where τ is the (unique) automorphism of $\mathbb{Q}(\zeta_{[f_1,f_2]})$ determined by $\tau(\zeta_{f_1}) = \zeta_{f_1}^{b_1}$ and $\tau(\zeta_{f_2}) = \zeta_{f_2}^{b_2}$.

Proof of Theorem 1. This is a variation of the proof of Theorem 2. Most error terms can be estimated as before on dropping the condition that $p \equiv a_1 (\operatorname{mod} d_2)$, which brings us to the situation of Theorem 2.

We first generalise Lemma 11. For that we only have to replace $M'_g(x,\xi_1)$ $M''_g(x,\xi_1)$ say, where $M''_g(x,\xi_1)$ is defined as $M'_g(x,\xi_1)$ with $a=a_2$ and $d=d_2$, but where now furthermore the primes p are required to satisfy $p\equiv a_1 (\operatorname{mod} d_1)$. The estimation of $M''_g(x,\xi_1)$ can be carried out completely similarly to that of $M'_g(x,\xi_1)$.

The analogue of (10) is easily derived to be

$$N_g(a_1,d_1;a_2,d_2)(x)=\sum_{\substack{t\leqslant x_1,\ (1+ta_2,d_2)=1\\ 1+ta_2\equiv a_1 (\operatorname{mod}(d_1,d_2t))}} V_g(a_1,d_1;a_2,d_2;t)(x)+O_{g,d}\left(\frac{x}{\log^{3/2}x}\right).$$

From here on the proof is completed as before. □

4. The case where d is an odd prime

Let $d=q$ be an odd prime. In this case it turns out to be fruitful to consider separately the primes p with $p\equiv 1 (\operatorname{mod} q)$ and those with $p\not\equiv 1 (\operatorname{mod} q)$.

4.1. The case where $q|a$

Trivially $N_g(a,q)=N_g(0,q)$ and w.l.o.g. we may assume that $a=0$. Note that the primes counted by $N_g(0,q)(x)$ must satisfy $p\equiv 1 (\operatorname{mod} q)$. Let $j=v_q(p-1)$. Note that $p\notin N_g(0,q)$ iff $q^j|r_g(p)$. Thus, we infer that

$$\begin{aligned}N_g(0,q)(x) &= \#\{p\leqslant x:\ p\equiv 1 (\operatorname{mod} q)\}\\ &\quad -\sum_{j=1}^{\infty}\#\{p\leqslant x:\ p\equiv 1 (\operatorname{mod} q^j),\ \ p\not\equiv 1 (\operatorname{mod} q^{j+1}),\ \ q^j|r_g(p)\}.\end{aligned}$$

The density of primes p satisfying $p\equiv 1 (\operatorname{mod} q^j)$, $p\not\equiv 1 (\operatorname{mod} q^{j+1})$ and $q^j|r_g(p)$ can be computed by Chebotarev's density theorem and equals

$$\frac{1}{[K_{q^j,q^j}:\mathbb{Q}]}-\frac{1}{[K_{q^{j+1},q^j}:\mathbb{Q}]}.$$

A more refined analysis [Wie], cf. [O,P] (with weaker error term), shows that

$$N_g(0,q)(x)=\delta_g(0,q)\mathrm{Li}(x)+O_{g,q}\left(\frac{x(\log\log x)^4}{\log^3 x}\right),$$

with

$$\delta_g(0,q)=\frac{1}{q-1}-\sum_{j=1}^{\infty}\left(\frac{1}{[K_{q^j,q^j}:\mathbb{Q}]}-\frac{1}{[K_{q^{j+1},q^j}:\mathbb{Q}]}\right). \tag{15}$$

Note that $N_g(1,q;0,q)(x)=N_g(0,q)(x)$ and hence $\delta_g(1,q;0,q)=\delta_g(0,q)$. The density $\delta_g(0,q)$ can be explicitly evaluated using Lemma 3:

$$\delta_g(1,q;0,q)=\delta_g(0,q)=\frac{q^{1-v_q(h)}}{q^2-1}. \tag{16}$$

Let us now assume GRH. Using Theorem 2 it is inferred that

$$\delta_g(0,q)=\delta_g^{(0)}(0,q)=\sum_{t=1}^{\infty}\sum_{n=1}^{\infty}\frac{\mu(n)}{[K_{[q,n]t,nt}:\mathbb{Q}]}=S_1+S_q,$$

say, where in S_1 we take together those n with $q\nmid n$ and in S_q those with $q|n$. We have

$$S_1=\sum_{v=1}^{\infty}\frac{\sum_{n|v,\ q\nmid n}\mu(n)}{[K_{qv,v}:\mathbb{Q}]}=\sum_{j=0}^{\infty}\frac{1}{[K_{q^{j+1},q^j}:\mathbb{Q}]},$$

and similarly

$$S_q=\sum_{t=1}^{\infty}\sum_{\substack{n=1\\ q|n}}^{\infty}\frac{\mu(n)}{[K_{nt,nt}:\mathbb{Q}]}=-\sum_{t=1}^{\infty}\sum_{\substack{n=1\\ q\nmid n}}^{\infty}\frac{\mu(n)}{[K_{qnt,qnt}:\mathbb{Q}]}=-\sum_{j=1}^{\infty}\frac{1}{[K_{q^j,q^j}:\mathbb{Q}]}.$$

On adding S_q to S_1 we find (15) on noting that $[K_{q,1}:\mathbb{Q}]=q-1$.

4.2. The case where $q\nmid a$

In the remainder of this section we assume that $q\nmid a$. Recall that $q^*=(\frac{-1}{q})q$.

Proposition 1 (*GRH*). *Let q be an odd prime and $q\nmid a$. Then*

$$\delta_g(1,q;a,q)=\frac{1}{(q-1)^2}\left(1-\frac{q^{1-v_q(h)}}{q+1}\right).$$

In particular $\delta_g(1,q;a,q)\in\mathbb{Q}_{>0}$ and does not depend on a.

Proof. The density $\delta_g(1,q;a,q)$ equals, using (14) and Lemma 7,

$$\sum_{\substack{t=1,\ q|t\\ (1+ta,q)=1}}^{\infty}\ \sum_{\substack{n=1\\ q\nmid n}}^{\infty}\frac{\mu(n)c_g(1+ta,qt,nt)}{[K_{qnt,nt}:\mathbb{Q}]}=\sum_{\substack{t=1\\ q|t}}^{\infty}\sum_{\substack{n=1\\ q\nmid n}}^{\infty}\frac{\mu(n)c_g(1+ta,q^{1+\nu_q(t)},nt)}{[K_{qnt,nt}:\mathbb{Q}]}.$$

Suppose that $q\nmid n$. By Lemma 6 it follows that $\mathbb{Q}(\zeta_{q^{1+\nu_q(t)}})\cap K_{nt,nt}=\mathbb{Q}(\zeta_{q^{\nu_q(t)}})$. Since $1+ta\equiv 1(\operatorname{mod} q^{\nu_q(t)})$, the automorphism σ_{1+ta} in Theorem 2 acts like the identity on the latter field intersection and hence $c_g(1+ta,q^{1+\nu_q(t)},nt)=1$. We thus infer that

$$\delta_g(1,q;a,q)=\sum_{\substack{t=1\\ q|t}}^{\infty}\sum_{\substack{n=1\\ q\nmid n}}^{\infty}\frac{\mu(n)}{[K_{qnt,nt}:\mathbb{Q}]}. \tag{17}$$

In particular, it follows that $\delta_g(1,q;a,q)$ does not depend on a. We present two ways to complete the proof from this point onwards.

First way. From (17) we infer that

$$\begin{aligned}\delta_g(1,q;a,q)&=\sum_{t=1}^{\infty}\ \sum_{n=1,\ q\nmid n}^{\infty}\frac{\mu(n)}{[K_{q^2nt,qnt}:\mathbb{Q}]}\\ &=\sum_{v=1}^{\infty}\frac{\sum_{n|v,\ q\nmid n}\mu(n)}{[K_{q^2v,qv}:\mathbb{Q}]}=\sum_{j=1}^{\infty}\frac{1}{[K_{q^{j+1},q^j}:\mathbb{Q}]}.\end{aligned}$$

Using Lemma 3 the latter sum is easily evaluated.

Second way. Note that $\sum_{0\leqslant a\leqslant q-1}\delta_g(1,q;a,q)$ equals the density of primes p with $p\equiv 1(\operatorname{mod} q)$ and hence

$$\sum_{0\leqslant a\leqslant q-1}\delta_g(1,q;a,q)=\frac{1}{q-1}. \tag{18}$$

Since, provided that $q\nmid a$, $\delta_g(1,q;a,q)$ does not depend on a, we conclude from (18) that

$$\delta_g(1,q;a,q)=\frac{1}{q-1}\left(\frac{1}{q-1}-\delta_g(1,q;0,q)\right).$$

Now invoke (16). □

Remark 5. Using a different method in [M-I, Theorem 10] the values of $\delta_g(1,3^s;a,3)$ for $s\geqslant 1$ were calculated.

In order to determine $\delta_g(a,q)$ it turns out to be convenient to determine $\delta_g(a,q)-\delta_g(1,q;a,q)$ first.

Lemma 12 (*GRH*). *Let q be an odd prime and $q \nmid a$. Then*

$$\delta_g(a,q) - \delta_g(1,q;a,q) = \frac{1}{q-1} - \sum_{\substack{v=1\\ q\nmid v}}^{\infty} \frac{\sum_{t\equiv -\frac{1}{a} (\bmod q),\ t\mid v} \mu(\frac{v}{t})}{[K_{qv,v}:\mathbb{Q}]} - \sum_{\substack{v=1,\ q\nmid v\\ \sqrt{q^*}\in K_{v,v}}}^{\infty} \frac{\sum_{(\frac{ta+1}{q})=-1,\ t\mid v} \mu(\frac{v}{t})}{[K_{qv,v}:\mathbb{Q}]}.$$

Proof. By Theorems 1, 2 and Lemma 7 we infer that

$$\delta_g(a,q) - \delta_g(1,q;a,q) = \sum_{\substack{t=1,\ q\nmid t\\ (1+ta,q)=1}}^{\infty} \sum_{\substack{n=1\\ q\nmid n}}^{\infty} \frac{\mu(n) c_g(1+ta,q,nt)}{[K_{qnt,nt}:\mathbb{Q}]}.$$

Let us restrict now to values of n and t that occur in the latter double sum. We have, by Lemma 5,

$$\mathbb{Q}(\zeta_q) \cap K_{nt,nt} = \begin{cases} \mathbb{Q}(\sqrt{q^*}) & \text{if } \sqrt{q^*} \in K_{nt,nt};\\ \mathbb{Q} & \text{otherwise.}\end{cases}$$

Using Lemma 2, it then follows that

$$c_g(1+ta,q,nt) = \begin{cases} (1 + (\frac{q^*}{1+ta}))/2 & \text{if } \sqrt{q^*} \in K_{nt,nt};\\ 1 & \text{otherwise.}\end{cases}$$

By the properties of the Kronecker symbol we have $(\frac{q^*}{1+ta}) = (\frac{1+ta}{q})$, where the symbol $(1+ta/q)$ is just the Legendre symbol. We can thus write $\delta_g(a,q) - \delta_g(1,q;a,q) = J_1 - J_2$, where

$$J_1 = \sum_{\substack{t=1,\ q\nmid t\\ (1+ta,q)=1}}^{\infty} \sum_{\substack{n=1\\ q\nmid n}}^{\infty} \frac{\mu(n)}{[K_{qnt,nt}:\mathbb{Q}]} \quad \text{and} \quad J_2 = \sum_{\substack{t=1,\ q\nmid t\\ (\frac{1+ta}{q})=-1}}^{\infty} \sum_{\substack{n=1,\ q\nmid n\\ \sqrt{q^*}\in K_{nt,nt}}}^{\infty} \frac{\mu(n)}{[K_{qnt,nt}:\mathbb{Q}]}. \tag{19}$$

On writing $nt = v$ we obtain

$$\begin{aligned} J_1 &= \sum_{\substack{v=1\\ q\nmid v}}^{\infty} \frac{\sum_{t\mid v} \mu(\frac{v}{t})}{[K_{qv,v}:\mathbb{Q}]} - \sum_{\substack{v=1\\ q\nmid v}}^{\infty} \frac{\sum_{t\equiv -\frac{1}{a} (\bmod q),\ t\mid v} \mu(\frac{v}{t})}{[K_{qv,v}:\mathbb{Q}]} \\ &= \frac{1}{q-1} - \sum_{\substack{v=1\\ q\nmid v}}^{\infty} \frac{\sum_{t\equiv -\frac{1}{a} (\bmod q),\ t\mid v} \mu(\frac{v}{t})}{[K_{qv,v}:\mathbb{Q}]} \end{aligned} \tag{20}$$

and

$$J_2 = \sum_{\substack{v=1,\ q\nmid v\\ \sqrt{q^*}\in K_{v,v}}}^{\infty} \frac{\sum_{(\frac{1+ta}{q})=-1,\ t|v} \mu(\frac{v}{t})}{[K_{qv,v}:\mathbb{Q}]}.$$

On combining these expressions with $\delta_g(a,q) - \delta_g(1,q;a,q) = J_1 - J_2$, the result follows. □

Example. For $q = 3$ and $3 \nmid a$ we obtain, on GRH, that

$$\begin{aligned}\delta_g(2,3;1,3) &= \frac{1}{2} - \sum_{\substack{v=1\\ 3\nmid v}}^{\infty} \frac{\sum_{t\equiv 2(\mathrm{mod}\ 3),\ t|v} \mu(\frac{v}{t})}{[K_{3v,v}:\mathbb{Q}]} - \sum_{\substack{v=1,\ 3\nmid v\\ \sqrt{-3}\in K_{v,v}}}^{\infty} \frac{\sum_{t\equiv 1(\mathrm{mod}\ 3),\ t|v} \mu(\frac{v}{t})}{[K_{3v,v}:\mathbb{Q}]}.\\ &= \frac{1}{2} - \sum_{\substack{v=1\\ 3\nmid v}}^{\infty} \frac{\sum_{t|v} \mu(\frac{v}{t})}{[K_{3v,v}:\mathbb{Q}]} + \sum_{\substack{v=1,\ 3\nmid v\\ \sqrt{-3}\notin K_{v,v}}}^{\infty} \frac{\sum_{t\equiv 1(\mathrm{mod}\ 3),\ t|v} \mu(\frac{v}{t})}{[K_{3v,v}:\mathbb{Q}]}.\\ &= \sum_{\substack{v=1,\ 3\nmid v\\ \sqrt{-3}\notin K_{v,v}}}^{\infty} \frac{\sum_{t\equiv 1(\mathrm{mod}\ 3),\ t|v} \mu(\frac{v}{t})}{[K_{3v,v}:\mathbb{Q}]}.\end{aligned}$$

More generally, we have

$$\delta_g(2,3;a,3) = \sum_{\substack{v=1,\ 3\nmid v\\ \sqrt{-3}\notin K_{v,v}}}^{\infty} \frac{\sum_{t\equiv a(\mathrm{mod}\ 3),\ t|v} \mu(\frac{v}{t})}{[K_{3v,v}:\mathbb{Q}]}.$$

Rewriting this expression in terms of $h'_\chi s$ we obtain Theorem 11 of [**M-I**].

We now have the ingredients to establish the following result.

Theorem 6 (*GRH*). *Let q be an odd prime and $q \nmid a$. Then*

$$\delta_g^{(0)}(a,q) = \frac{1}{q-1} + \frac{1}{(q-1)^2}\left(1 - \frac{q^{1-v_q(h)}}{q+1}\right) - \sum_{\substack{v=1\\ q\nmid v}}^{\infty} \frac{\sum_{t\equiv -\frac{1}{a}(\mathrm{mod}\ q),\ t|v} \mu(\frac{v}{t})}{[K_{qv,v}:\mathbb{Q}]} \tag{21}$$

and

$$\delta_g(a,q) = \delta_g^{(0)}(a,q) - \sum_{\substack{v=1,\ q\nmid v\\ \sqrt{q^*}\in K_{v,v}}}^{\infty} \frac{\sum_{(\frac{ta+1}{q})=-1,\ t|v} \mu(\frac{v}{t})}{[K_{qv,v}:\mathbb{Q}]}. \tag{22}$$

If $q \nmid D(g_0)$, then $\delta_g(a,q) = \delta_g^{(0)}(a,q)$.

Proof. Considering the terms with $q|t$ and $q\nmid t$ in the double sum for $\delta_g(a,q)$ separately we have, using (17) and (19) that $\delta_g^{(0)}(a,q)=\delta_q(1,q;a,q)+J_1$. On using Proposition 1, (20) and Lemma 12 the first two assertions are established.

If $q\nmid D(g_0)$, then by Lemma 6 there is no integer v such that $q\nmid v$ and $\sqrt{q^*}\in K_{v,v}$ and hence the double sum in (22) equals zero. □

Remark 6. The double sum (22) can be rewritten, using Lemma 6, as

$$\sum_{v=1,\ q\nmid v}^{\infty}\left(\frac{2}{[K_{qv,v}:\mathbb{Q}]}-\frac{2}{(q-1)[K_{v,v}:\mathbb{Q}]}\right)\sum_{(\frac{ta+1}{q})=-1,\ t|v}\mu\left(\frac{v}{t}\right).$$

Remark 7. Note that the proof of Theorem 6 makes essential use of the law of quadratic reciprocity (this law enters in the proof of Lemma 12).

Using (5) and the following lemma, $\delta_g(a,q)$ and $\delta_g^{(0)}(a,q)$ can be expressed as simple linear combinations of the constants C_χ introduced in Section 2.1. Each such constant can be explicitly evaluated and is of the form cA_χ with $c\in\mathbb{Q}(\zeta_{o_\chi})$. This allows one to explicitly evaluate $\delta_g(a,q)$ and $\delta_g^{(0)}(a,q)$. For reasons of space we only will work this out in the case $g\in\mathcal{G}$, where $\mathcal{G}$ is the set of rational numbers g that cannot be written as $-g_0^h$ or g_0^h with $h>1$ an integer and g_0 a rational number.

Lemma 13 (*Moree [M-I, Lemma 11]*). *Let r,s be integers with $s|r$. Let χ be a Dirichlet character. Then, if $g>0$ or $g<0$ and s is even,*

$$\sum_{(r,v)=1}\frac{h_\chi(v)}{[K_{sv,v}:\mathbb{Q}]}=\frac{1}{\varphi(s)}\left(C_\chi(h,r,1)+C_\chi\left(h,r,\frac{n_s}{(n_s,s)}\right)\right).$$

When $g<0$ and s is odd, the latter sum equals

$$\frac{1}{\varphi(s)}\left(C_\chi(h,r,1)-\frac{1}{2}C_\chi(h,r,2)+\frac{1}{2}C_\chi(h,r,2^{\nu_2(h)+1})+C_\chi\left(h,r,\frac{n_s}{(n_s,s)}\right)\right).$$

Now we can formulate one of our main results.

Theorem 7 (*GRH*). *Let q be an odd prime and $q\nmid a$. We have*

$$\delta_g(a,q)=\sum_{\chi\in G_q}\chi(-a)c_\chi A_\chi,$$

where $c_\chi\in\mathbb{Q}(\zeta_{o_\chi})$ may depend on q and g (but not a) and can be explicitly evaluated.

Proof. We only deal with the case where $g>0$ or $g<0$ and h is odd (the remaining more space consuming case being left to the reader).

Using the identity (5) and Lemma 13 we can rewrite (21) as

$$\delta_g^{(0)}(a,q) = \frac{1}{q-1} + \frac{1}{(q-1)^2}\left(1 - \frac{q^{1-\nu_q(h)}}{q+1}\right) - \frac{1}{(q-1)^2}\sum_{\chi\in G_q}\chi(-a)\left(C_\chi(h,q,1) + C_\chi\left(h,q,\frac{n_q}{(n_q,q)}\right)\right).$$

Similarly, using Remark 6, we rewrite (22) as

$$\delta_g(a,q) = \delta_g^{(0)}(a,q) - \frac{2}{(q-1)^2}\sum_{\chi\in G_q}\chi(-a) \times\left(C_\chi\left(h,q,\frac{n_q}{(n_q,q)}\right) - C_\chi(h,q,n_1)\right)\sum_b \overline{\chi(b)},$$

where the sum is over the integers $1\leqslant b\leqslant q-1$ for which $(\frac{1-b}{q}) = -1$. Note that $n_1 = n_q$. If $q \nmid D(g_0)$, the latter double sum equals zero and we infer (as before) that $\delta_g(a,q) = \delta_g^{(0)}(a,q)$. If $q \mid D(g_0)$, then $C_\chi(h,q,n_1) = 0$ and we infer that

$$\delta_g(a,q) = \delta_g^{(0)}(a,q) - \frac{2}{(q-1)^2}\sum_{\chi\in G_q}\chi(-a)C_\chi\left(h,q,\frac{n_1}{q}\right)\sum_b \overline{\chi(b)}.$$

By [M-I, Lemma 10] we can write $C_\chi(h,r,s)$ as cA_χ with $c \in \mathbb{Q}(\zeta_{o_\chi})$, where c can be explicitly given. Using this the proof is easily completed. □

The following result is an easy consequence of the latter proof.

Proposition 2 (*GRH*). *If h is odd and $8 \mid D(g)$, then $\delta_g(a,q) = \delta_{-g}(a,q)$.*

Proof. The assumptions imply that $|n_1| = |n_q| = |D(\pm g)|$ and on noting that $C_\chi(h,r,s) = C_\chi(h,r,-s)$ the character sum expression for $\delta_g(a,q)$ given in the proof of Theorem 7 is seen to equal that of $\delta_{-g}(a,q)$ in case $q \nmid a$. If $q \mid a$, then by (16) we have $\delta_{\pm g}(0,q) = q/(q^2-1)$. □

Theorem 4 can be regarded as an example of Theorem 7 in the special (but important) case where $g \in \mathcal{G}$.

Proof of Theorem 4. By Lemma 3 we have

$$n_1 = n_q = \begin{cases} [2, D(g_0)] & \text{if } g > 0;\\ D(g_0)/2 & \text{if } g < 0 \text{ and } D(g) \equiv 4 \pmod 8;\\ [4, D(g_0)] & \text{if } g < 0 \text{ and } D(g) \not\equiv 4 \pmod 8.\end{cases}$$

Now note that $n_1 = n_q = [2, D(g)]$ and that $q|D(g_0)$ iff $q|D(g)$. Working out the formulae involving the C_χ's in the proof of Theorem 7 using [M-I, Lemma 10], the proof is then completed. □

5. The case where *d* is an odd prime power

The case where $d = q^s$ with q an odd prime is easily reduced to the case $d = q$ by the following result. Notice that Theorem 8 implies Theorem 5.

Theorem 8 (*GRH*). *Suppose that* $d|d_1$, *the quotient* d_1/d *is odd and* $\omega(d_1) = \omega(d)$. *Then* $\delta_g(a, d_1) = \frac{d}{d_1}\delta_g(a, d)$.

Remark 8. From formula (3) for $\delta(a, d)$ it is easily inferred that if $d|d_1$ and $\omega(d_1) = \omega(d)$, then

$$\delta(a, d_1) = \frac{d}{d_1}\,\delta(a, d). \tag{23}$$

Proof of Theorem 8. If $d|d_1$ and $\omega(d) = \omega(d_1)$ and for all n and t with $(1+ta, d) = 1$, $(n, d)|a$ and n is squarefree, we have $[K_{[d_1,n]t,nt} : \mathbb{Q}]/\varphi(d_1) = [K_{[d,n]t,nt} : \mathbb{Q}]/\varphi(d)$, then using Lemma 8 we infer that

$$\begin{aligned}\delta_g(a, d_1) &= \sum_{\substack{t=1\\(1+ta,d_1)=1}}^{\infty} \sum_{\substack{n=1\\(n,d_1)|a}}^{\infty} \frac{\mu(n)c_g(1+ta, d_1t, nt)}{[K_{[d_1,n]t,nt} : \mathbb{Q}]}\\ &= \frac{d}{d_1} \sum_{\substack{t=1\\(1+ta,d)=1}}^{\infty} \sum_{\substack{n=1\\(n,d)|a}}^{\infty} \frac{\mu(n)c_g(1+ta, dt, nt)}{[K_{[d,n]t,nt} : \mathbb{Q}]} = \frac{d}{d_1}\,\delta_g(a, d),\end{aligned}$$

where we invoked Lemma 4 and used that $\varphi(d_1)/\varphi(d) = d_1/d$. □

6. Connection between $\delta_g(a, q^s)$ and $\delta(a, q^s)$

Define $\overline{\delta}_g(d) = (\delta_g(0, d), \delta_g(1, d), \ldots, \delta_g(d-1, d))$ (if this exists) and

$$\overline{\delta}(d) = (\delta(0, d), \delta(1, d), \ldots, \delta(d-1, d)).$$

The next result implies that, under GRH, for almost all integers g we have $\overline{\delta}_g(q^s) = \overline{\delta}(q^s)$. Note that this result also implies the truth of Theorem 3.

Theorem 9 (*GRH*). *Let* $s \geqslant 1$ *and* q *be an odd prime. Then there are at most* $O_q(x \log^{-1/(q-1)} x)$ *integers* g *with* $|g| \leqslant x$ *such that* $\overline{\delta}_g(q^s) \neq \overline{\delta}(q^s)$.

Proof. By the results of the previous section it is enough to prove this in case $s = 1$. Since there are at most $O(\sqrt{x}\log x)$ integers $|g| \leqslant x$ that are not in $\mathcal{G}$, we can restrict ourselves to the case where $g \in \mathcal{G}$. For such a g we then have, using (16), that $\delta_g(0,q) = \delta(0,q)$. Now by Theorem 4 and (4) we infer that if $D(g)$ has a prime divisor p with $p \equiv 1 (\bmod q)$, then $\overline{\delta}_g(q) = \overline{\delta}(q)$ (since $\chi(p) = 1$ for every $\chi \in G_q$). It follows that the number of $g \in \mathcal{G}$ with $|g| \leqslant x$ such that $\overline{\delta}_g(q) \neq \overline{\delta}(q)$ is bounded above by the number of g with $|g| \leqslant x$ such that $D(g)$ has no prime factor p satisfying $p \equiv 1 (\bmod q)$. By Lemma 10 the proof is then completed. □

If it is not true that $\overline{\delta}_g(q^s) = \overline{\delta}(q^s)$, then our final result shows that $\overline{\delta}_g(q^s)$ will be close to $\overline{\delta}(q^s)$,

Proposition 3 (*GRH*). *Suppose that $g \in \mathcal{G}$. As $|g|$ tends to infinity, $\overline{\delta}_g(q^s)$ tends to $\overline{\delta}(q^s)$.*

Proof. A simple consequence of Theorems 4 and 5 and Eq. (4). □

7. Divisibility of the order reconsidered

The case $d|a$ has been well-researched since the late fifties of the previous century, especially by Wiertelak (vide [M-div] for references). It is thus perhaps surprising that Theorem 2 sheds some new light on this case.

As remarked in the introduction, under GRH $\delta_g(0,d)$ exists and equals $\delta_g^{(0)}(0,d)$. The expression for the latter quantity can be simplified further:

$$\begin{aligned}
\delta_g^{(0)}(0,d) &= \sum_{t=1}^{\infty}\sum_{n=1}^{\infty}\frac{\mu(n)}{[K_{[d,n]t,nt}:\mathbb{Q}]} = \sum_{\alpha|d}\sum_{t=1}^{\infty}\sum_{(n,d)=\alpha}\frac{\mu(n)}{[K_{[d,n]t,nt}:\mathbb{Q}]} \\
&= \sum_{\alpha|d}\mu(\alpha)\sum_{t=1}^{\infty}\sum_{(n,d)=1}\frac{\mu(n)}{[K_{[d,\alpha n]t,\alpha nt}:\mathbb{Q}]} \\
&= \sum_{\alpha|d}\mu(\alpha)\sum_{v=1}^{\infty}\frac{\sum_{(n,d)=1,\ n|v}\mu(n)}{[K_{dv,\alpha v}:\mathbb{Q}]} \\
&= \sum_{\alpha|d}\mu(\alpha)\sum_{v|d^{\infty}}\frac{1}{[K_{dv,\alpha v}:\mathbb{Q}]} = \sum_{v|d^{\infty}}\sum_{\alpha|d}\frac{\mu(\alpha)}{[K_{dv,\alpha v}:\mathbb{Q}]},
\end{aligned}$$

where in the derivation of the third equality the substitution $n \to \alpha n$ was made, in the fourth the substitution $v = nt$ and in the fifth the observation that

$$\sum_{(n,d)=1,\ n|v}\mu(n) = \begin{cases} 1 & \text{if } v|d^{\infty}; \\ 0 & \text{otherwise,} \end{cases}$$

Table 1
The constants A_χ for $d = 5$

χ	A_χ
ψ	$0.364689626478581\ldots + i \cdot 0.224041094424738\ldots$
ψ^2	$0.129307938528080\ldots$
ψ^3	$0.364689626478581\ldots - i \cdot 0.224041094424738\ldots$
ψ^4	1

was used. We thus obtain as a special case of Theorem 2 that, under GRH,

$$\delta_g(0,d) = \sum_{v|d^\infty} \sum_{\alpha|d} \frac{\mu(\alpha)}{[K_{dv,\alpha v} : \mathbb{Q}]}. \tag{24}$$

This seems to be the simplest formula known expressing $\delta_g(0,d)$ in terms of field degrees. It suggests the validity of the following result:

Proposition 4. *We have $N_g(0,d)(x) = \sum_{v|d^\infty} \sum_{\alpha|d} \mu(\alpha)\pi_{K_{dv,\alpha v}}(x)$, where $\pi_L(x)$ denotes the number of primes $p \leqslant x$ that split completely in the field L.*

Indeed, it is not difficult to prove the latter identity [M-div, Proposition 1]. It can be used to infer that $\delta_g(0,d)$ exists *unconditionally* and to give the simplest explicit formula for this quantity known so far [M-div, Theorem 2].

8. Some numerical experiments

Various numerical experiments were carried out to see if these seemed in agreement with the theoretical claims. In case $d = 3$ or 4 the reader is referred to part I. So let us restrict to $d = 5$. Let ψ be the character mod 5 determined uniquely by $\psi(2) = i$. The group G_5 consists of ψ, ψ^2, ψ^3 and ψ^4. Note that ψ^4 is the trivial character. From Table 3 of [M-Av] we have Table 1.

Using Table 1 and (4) one then computes $\delta(a,5)$ for $1 \leqslant a \leqslant 4$. Moreover, $\delta(0,5) = \frac{5}{24}$. These values are recorded in the first row of Table 2.

If an entry is in a row labelled $\approx \delta_g(*,d)$ and in column j, then the number given equals $N_g(j,5)(x)/\pi(x)$ rounded to six decimals with $x = 2038074743$ (and hence $\pi(x) = 10^8$). The theoretical values are given with six digit precision, with a bar over the last digit indicating that if the number is to be rounded off, it should be rounded upwards.

8.1. Comments to the table

(1) The experimental results suggest that the identity $\delta_g(a,q) = \delta(a,q)$ holds more often in case $a = 0$. Indeed, if $g \in \mathcal{G}$, then $\delta_g(0,q) = \delta(0,q) = q/(q^2-1)$ and it follows from [M-Av] that there are at most $O(\sqrt{x})$ integers g with $|g| \leqslant x$ such that $\delta_g(0,q) \neq \delta(0,q)$. On the other hand, I conjecture that for every prime q

Table 2
Experimental and theoretical densities for $d = 5$

	0	1	2	3	4
$\delta(*, 5)$	$0.20833\underline{3}$	$0.23542\underline{1}$	$0.17799\underline{3}$	$0.23400\overline{3}$	$0.14424\overline{8}$
$\approx \delta_{-11}(*, 5)$	0.208347	0.235422	0.178007	0.233974	0.144250
$\delta_{-11}(*, 5)$	$\delta(0, 5)$	$\delta(1, 5)$	$\delta(2, 5)$	$\delta(3, 5)$	$\delta(4, 5)$
$\approx \delta_{-5}(*, 5)$	0.208348	0.264146	0.194858	0.233282	0.099365
$\delta_{-5}(*, 5)$	$\delta(0, 5)$	$0.26413\underline{5}$	$0.19486\overline{5}$	$0.23329\overline{4}$	$0.09937\underline{1}$
$\approx \delta_{-2}(*, 5)$	0.208333	0.240695	0.178703	0.229275	0.142993
$\delta_{-2}(*, 5)$	$\delta(0, 5)$	$0.24068\overline{1}$	$0.17869\overline{1}$	$0.22926\underline{4}$	$0.14302\underline{9}$
$\approx \delta_{2}(*, 5)$	0.208333	0.240673	0.178706	0.229270	0.143017
$\delta_{2}(*, 5)$	$\delta(0, 5)$	$0.24068\overline{1}$	$0.17869\overline{1}$	$0.22926\underline{4}$	$0.14302\underline{9}$
$\approx \delta_{3}(*, 5)$	0.208341	0.238177	0.169810	0.235241	0.148432
$\delta_{3}(*, 5)$	$\delta(0, 5)$	$0.23815\underline{3}$	$0.16981\underline{1}$	$0.23525\underline{8}$	$0.14844\overline{3}$
$\approx \delta_{5}(*, 5)$	0.208348	0.232581	0.292840	0.054488	0.211742
$\delta_{5}(*, 5)$	$\delta(0, 5)$	$0.23258\overline{5}$	$0.29284\overline{8}$	$0.05449\overline{3}$	$0.21173\overline{7}$
$\approx \delta_{65537}(*, 5)$	0.208330	0.235483	0.177954	0.234002	0.144231
$\delta_{65537}(*, 5)$	$\delta(0, 5)$	$0.23542\underline{1}$	$0.17799\underline{3}$	$0.23400\overline{3}$	$0.14424\overline{8}$

there exists $\alpha_q > 0$ such that $\delta_g(a, q) \neq \delta(a, q)$ for at least $\gg x \log^{-\alpha_q} x$ integers g satisfying $|g| \leqslant x$.

(2) By Corollary 1 one expects that $\delta_{-11}(*, 5) = \delta(*, 5)$.

(3) By Proposition 2 one ought to have that $\delta_{-2}(j, 5) = \delta_2(j, 5)$.

(4) One expects, a priori, $\delta_{65537}(j, 5)$ to be close to $\delta(j, 5)$. It turns out that $\delta_{65537}(j, 5) \neq \delta(j, 5)$ for $1 \leqslant j \leqslant 4$, but this is not visible at the precision level of the table.

Acknowledgements

Work on this paper was begun at the Korteweg–de Vries Institute (Amsterdam), whilst the author was working in the NWO Pioneer-project of Prof. E. Opdam. I am grateful to Prof. Opdam for the opportunity to have been part of his group. Yves Gallot and Paul Tegelaar, as so often, kindly provided very helpful programming and computer assistance.

References

[CM] K. Chinen, L. Murata, On a distribution property of the residual order of $a \pmod p$. I, J. Number Theory 105 (2004) 60–81.

[H] C. Hooley, Artin's conjecture for primitive roots, J. Reine Angew. Math. 225 (1967) 209–220.

[M-Av] P. Moree, On the average number of elements in a finite field with order or index in a prescribed residue class, Finite Fields Appl. 10 (2004) 438–463.

[M-Fib] P. Moree, Convoluted convolved Fibonacci numbers, J. Integer Seq. 7 (2004) Article 04.2.2, 14 (electronic).

[M-I] P. Moree, On the distribution of the order and index of $g \pmod p$ over residue classes I, ArXiv:math.NT/0211259, J. Number Theory, to appear.

[M-div] P. Moree, On primes p for which d divides $\mathrm{ord}_p(g)$, Funct. Approx. Comment. Math. 33 (2005) 85–95 (see also arXiv:math.NT/0407421).

[MC] L. Murata, K. Chinen, On a distribution property of the residual order of $a(\bmod p)$. II, J. Number Theory 105 (2004) 82–100.

[N] W. Narkiewicz, Elementary and Analytic Theory of Numbers, second ed., Springer, Berlin, 1989.

[O] R.W.K. Odoni, A conjecture of Krishnamurthy on decimal periods and some allied problems, J. Number Theory 13 (1981) 303–319.

[P] F. Pappalardi, Squarefree values of the order function, New York J. Math. 9 (2003) 331–344.

[Wei] E. Weiss, Algebraic Number Theory, New York University Press, New York, 1963.

[Wie] K. Wiertelak, On the density of some sets of primes. IV, Acta Arith. 43 (1984) 177–190.

[Wil] K.S. Williams, Mertens' theorem for arithmetic progressions, J. Number Theory 6 (1974) 353–359.

[Wir] E. Wirsing, Das asymptotische Verhalten von Summen über multiplikative Funktionen, Math. Ann. 143 (1961) 75–102.