On the distribution of the order and index of $g(\text{mod } p)$ over residue classes III

Pieter Moree

Abstract

For a fixed rational number $g \notin \{-1,0,1\}$ and integers a and d we consider the sets $N_g(a,d)$, respectively $R_g(a,d)$, of primes p for which the order, respectively the index of $g(\text{mod } p)$ is congruent to $a(\text{mod } d)$. Under the Generalized Riemann Hypothesis (GRH), it is known that these sets have a natural density $\delta_g(a,d)$, respectively $\rho_g(a,d)$. It is shown that these densities can be expressed as linear combinations of certain constants introduced by Pappalardi. Furthermore it is proved that $\delta_g(a,d)$ and $\rho_g(a,d)$ equal their g-averages for almost all g.

1 Introduction

Let $g \notin \{-1,0,1\}$ be a rational number (this assumption on g will be maintained throughout this paper) and let a and d be positive integers. The central object of study of this paper and its predecessors [M-I, M-II] are the sets $N_g(a,d)$ and, to a lesser extent, due to its much greater simplicity of description, $R_g(a,d)$. Nevertheless, the main results for both sets (Theorems 2, 3, 4) are quite analogous in character. However, Theorem 1 does not have an analog for ρ, cf. Proposition 8. The set $N_g(a,d)$ consists of the primes p for which $\nu_p(g)=0$ and $\text{ord}_g(p) \equiv a(\text{mod } d)$ (here and in the sequel the letter p will be used to indicate prime numbers). The set $R_g(a,d)$ is similarly defined, but with $\text{ord}_g(p)$ replaced by $r_g(p)$, the residual index.

Pappalardi [P] established, under GRH, the existence of the natural density $\rho_g(a,d)$ of $R_g(a,d)$. In particular, he showed that

$$\rho_g(a,d) = \sum_{t \equiv a(\text{mod } d)} \sum_{n=1}^{\infty} \frac{\mu(n)}{[K_{nt,nt}:\mathbb{Q}]}, \tag{1}$$

Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Deutschland, E-mail: moree@mpim-bonn.mpg.de

Mathematics Subject Classification (2000). 11N37, 11N69, 11R45

where for $r|s$ we define $K_{s,r}$ to be the number field $\mathbb{Q}(\zeta_s, g^{1/r})$. In [M-II] it was shown that, under GRH, the set $N_g(a,d)$ has a natural density $\delta_g(a,d)$. In particular,

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

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

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

where σ_b is the automorphism of $\mathbb{Q}(\zeta_f)$ that sends ζ_f to ζ_f^b (if a and b are integers, then by (a,b) and $[a,b]$ we denote the greatest common divisor, respectively lowest common multiple of a and b). The rational number $c_g(1+ta,dt,nt)/[K_{[d,n]t,nt}:\mathbb{Q}]$ is the density of primes $p \equiv 1+ta(\text{mod } dt)$ that split completely in $K_{nt,nt}$. It turns out that the coefficient $c_g(.,.,.)$ has a strong tendency to equal 1 and this motivates the following definition:

Definition 1 *Put*

$$\delta_g^{(0)}(a,d) = \sum_{\substack{t=1 \\ (1+ta,d)=1}}^{\infty} \sum_{\substack{n=1 \\ (n,d)|a}}^{\infty} \frac{\mu(n)}{[K_{[d,n]t,nt}:\mathbb{Q}]}, \tag{3}$$

For example, it can be shown that (unconditionally) $\delta_g(0,d) = \delta_g^{(0)}(0,d)$. Other examples are provided by Proposition 9 and Lemma 18.

In case $d=2$ unconditional results can be obtained, cf. [O, Wi1, Wi2]. For an extensive analysis of the case $d=3$, see [M-I]. For the case $d=4$ see also [M-I] (for less general results obtained by a different method for this modulus see [CM]). The case where d is prime is investigated in [M-II]. In this paper the general case is investigated. Not so surprisingly the present results will be somewhat less explicit.

By the following result d can be taken close to squarefree.

Theorem 1 (GRH).
1) *If q is an odd prime dividing d_1, then $\delta_g(a,qd_1) = \delta_g(a,d_1)/q$.*
2) *If $8|d$, then $\delta_g(a,2d_1) = \delta_g(a,d_1)/2$.*
The same conclusion holds with δ_g replaced by $\delta_g^{(0)}$ or δ. In the latter case, the result holds true unconditionally.

By $k(d)$ we denote the squarefree part of d, that is $k(d) = \prod_{p|d} p$. Also we define

$$k_1(d) = \begin{cases} k(d) & \text{if } d \text{ is odd;} \\ 4k(d) & \text{otherwise,} \end{cases} \text{ and } k_2(d) = \begin{cases} k(d) & \text{if } d \text{ is odd;} \\ (4,d/2)k(d) & \text{otherwise.} \end{cases}$$

Note that, assuming GRH, we have $\rho_g(a,d) = \rho_g(a,d_1)d_1/d$, where $d_1 = k_2(d)$.

It turns out that the average density of elements in a finite field of prime cardinality having order, respectively index, congruent to $a(\text{mod } d)$ exists. Denote these densities by $\delta(a,d)$, respectively $\rho(a,d)$. These densities can be studied by quite elementary methods and are easier to study than $\delta_g(a,d)$ and $\rho_g(a,d)$. In this paper we will be particularly interested in the connection between $\delta_g(a,d)$ and $\delta(a,d)$ and the same for $\rho_g(a,d)$ and $\rho(a,d)$. The quantities $\delta(a,d)$ and $\rho(a,d)$ are studied in [M-Av]. In this paper we will show that, under GRH, $*(a,d)$ can also be regarded as the g-average of $*_g(a,d)$ (where for ease of notation we define $\delta^{(0)}(a,d)=\delta(a,d)$):

Proposition 1 (GRH). *With $*=\delta,\delta^{(0)}$ or ρ we have*

$$\frac{1}{2x}\sum_{|g|\le x} *_g(a,d) = *(a,d)+O(\frac{1}{\sqrt{x}}).$$

(All results in this paper with the condition $|g|\le x$ remain valid if this condition is replaced with $1<g\le x$ or $-x\le g<1$ and $2x$ by x.) Proposition 1 is a simple consequence of the following result in which 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 (in other words the rational numbers g that satisfy $h=1$ in the notation of Lemma 3).

Theorem 2 (GRH). *Suppose that $g\in G$. Set $D_1=|D(g)/(D(g),d)|$ and $D_2=[2,D(g)]$, where $D(g)$ denotes the discriminant of the number field $\mathbb{Q}(\sqrt{g})$. Then*

$$\Big|\delta_g^o(a,d)-\delta(a,d)\Big| < \frac{2^{\omega(D_1)+2}}{\varphi(D_1)D_1},\quad \Big|\delta_g(a,d)-\delta(a,d)\Big| < \frac{3\cdot 2^{\omega(D_1)+2}}{\varphi(D_1)D_1},$$

and

$$\Big|\rho_g(a,d)-\rho(a,d)\Big| < \frac{2^{\omega(D_2)+2}}{\varphi(D_2)D_2},$$

where $\omega(n)$ denotes the number of distinct prime divisors of n.

Corollary 1 *If $|D(g)|$ tends to infinity with $g\in G$, then $*_g(a,d)$ tends to $*(a,d)$, where $*=\delta,\delta^{(0)}$ or ρ.*

Corollary 1 for $*=\delta_g$ has been already announced (but not proved) as Theorem 2 of [M-Av]. Theorem 2 shows that 'generically' $*_g(a,d)$ is quite close to $*(a,d)$. For a numerical demonstration of this see Tables 1 and 2 of [M-Av]. Much more is true, however:

Theorem 3 (GRH). *Let d be fixed. There are at most $O_d(x\log^{-1/\varphi(k_1(d))}x)$ integers g with $|g|\le x$ such that $*_g(a,d)\ne *(a,d)$ for some integer a, where $*=\delta,\delta^{(0)}$ or $*=\rho$. In particular,*

$$(*_g(0,d),\dots,*_g(d-1,d)) = (*(0,d),\dots,*(d-1,d))$$

for almost all integers g.

This result allows one to introduce various notions of 'genericity' for g. Actually a more precise version of Theorem 3 is provided by Theorem 7 in case $*=\delta$ or $*=\delta^{(0)}$ and by Propositions 6 and 7 in case $*=\rho$. Note that $k_1(d)|4d$.

The final main result is concerned with explicitly evaluating $*_g(a,d)$. For χ a Dirichlet character, let

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

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

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

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

(By G_d we denote the group of Dirichlet characters mod d and by o_χ the order of the Dirichlet character in G_χ.)

Theorem 4 (GRH). *Let a and d be arbitrary natural numbers. Then there exists an integer d_1 such that*

$$*(a,d) = \sum_{\chi \in G_{d_1}} c_\chi A_\chi \text{ with } c_\chi \in \mathbb{Q}(\zeta_{o_\chi}).$$

Furthermore, c_χ can be explicitly computed.
1) *If $* = \delta_g^{(0)}$, then one can take $d_1 = k_2(d)$.*
2) *If $* = \delta_g$, then one can take $d_1 = k_1(d)$.*
3) *If $* = \rho_g$, then one can take $d_1 = d/(a,d)$.*

Unconditional results of this nature for $\delta(a,d)$ and $\rho(a,d)$ are proved in [M-Av] (with $d_1 = k(d)$, respectively $d_1 = d/(a,d)$).

The proofs of Theorems 3 and 4 require more explicit knowledge of the Galois coefficients c_g appearing in (2). Theorem 5 (which requires a good deal of work in order to be proved) allows one to compute $\mathbb{Q}(\zeta_f) \cap K_{v,v}$. Using this the coefficient c_g can be explicitly related to a Kronecker symbol. In all this, unfortunately, the case $g < 0$ turns out to be considerably more complicated than the case $g > 0$ (Proposition 4, however, sometimes brings relief).

2 Preliminaries on algebraic number theory

Let $K : \mathbb{Q}$ 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(mod 4). The following lemma allows one to determine all quadratic subfields of a given cyclotomic field.

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

Consider the cyclotomic extension $\mathbb{Q}(\zeta_f) : \mathbb{Q}$. There are $\varphi(f)$ distinct automorphisms each determined uniquely by $\sigma_a(\zeta_f) = \zeta_f^a$, with $1 \le a \le f$ 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 (for a description of the Kronecker symbol see e.g. §2.1 of [M-II]):

Lemma 2 *Let $\mathbb{Q}(\sqrt{g_1}) \subseteq \mathbb{Q}(\zeta_f)$ be a quadratic field of discriminant $D(g_1)$ and a be an integer with $(a, f) = 1$. We have $\sigma_a|_{\mathbb{Q}(\sqrt{g_1})} = \mathrm{id}$ iff $(\frac{D(g_1)}{a}) = 1$, with $(\frac{\cdot}{\cdot})$ the Kronecker symbol.*

From the theory of profinite groups we recall the notion of a supernatural (or Steinitz) number. A supernatural number is a formal product $\prod_p p^{e_p}$, where each $e_p \in \mathbb{N} \cup \{\infty\}$. The set of supernatural numbers forms a commutative monoid with respect to the obvious product. If a is a supernatural number, then by $\nu_p(a)$ we denote the exponent of p occurring in a. We say that $a|b$, that is that a divides b, if $\nu_p(a) \le \nu_p(b)$ for all primes p. If $a|b$, then $b = ca$, with c a supernatural number. Given supernatural numbers, we define their greatest common divisor by the formula $(a, b) = \prod_p p^{\inf(\nu_p(a),\nu_p(b))}$. To a natural number d we associate the supernatural number d_∞, where $d_\infty = \prod_{p|d} p^\infty$. The '$d$-part' of a natural number n is then given by (n, d_∞).

2.1 Preliminaries on field degrees and intersections

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 $\mathbb{Q}(\sqrt{g})$. An integer D is said to be a fundamental discriminant if $D = D(g_1)$ for some $g_1 \in \mathbb{Q}$. If D is a fundamental discriminant, then $\mathbb{Q}(\sqrt{D})$ has conductor $|D|$ by Lemma 1. The notation $D(g_1)$ along with the notation g_0, h, m and n_r introduced in the next lemma will reappear again and again in the sequel.

Lemma 3 [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 $m = D(g_0)/2$ if $\nu_2(h) = 0$ and $D(g_0) \equiv 4 (\mathrm{mod}\ 8)$ or $\nu_2(h) = 1$ and $D(g_0) \equiv 0 (\mathrm{mod}\ 8)$, and $m = [2^{\nu_2(h)+2}, D(g_0)]$ otherwise. Put*

$$n_r = \begin{cases} m & \textit{if } g < 0 \textit{ and } r \textit{ is odd;} \\ [2^{\nu_2(hr)+1}, D(g_0)] & \textit{otherwise.} \end{cases}$$

We have

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

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

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

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

$$\epsilon(kr,k)=\begin{cases}2 & \text{if } n_r|kr;\\ \frac{1}{2} & \text{if } 2|k \text{ and } 2^{\nu_2(h)+1}\nmid k;\\ 1 & \text{otherwise.}\end{cases}$$

`Remark`. Note that if h is odd, then $n_r=[2^{\nu_2(r)+1},D(g)]$. Note that $n_r=n_{\nu_2(r)}$.

An easy consequence of the latter result is the following lemma.

Lemma 4
1) *Suppose that q is an odd prime dividing d_1 and $q^2\nmid n$. Then $[K_{[qd_1,n]t,nt}:\mathbb{Q}]=q[K_{[d_1,n]t,nt}:\mathbb{Q}]$.*
2) *Suppose that $\nu_2(d_1)\ge\max\{2,\nu_2(D(g_0))\}$ and $4\nmid n$. Then $[K_{[2^\alpha d_1,n]t,nt}:\mathbb{Q}]=2^\alpha[K_{[d_1,n]t,nt}:\mathbb{Q}]$.*

Let $g_1\neq 0$ be a rational number and $n|2m$. Note that the field $\mathbb{Q}(\zeta_m,\zeta_n\sqrt{g_1})$ is either equal to $\mathbb{Q}(\zeta_m)$ or a quadratic extension thereof. The following result records precisely when the extension is not quadratic. In the case $m=n$ this result is Lemma 3 of [GP] (but earlier references undoubtedly exist).

Lemma 5 *Let $g_1\neq 0$ be a rational number and suppose that $n|2m$. Then we have that $[\mathbb{Q}(\zeta_m,\zeta_n\sqrt{g_1}):\mathbb{Q}(\zeta_m)]=\epsilon_1(m,n)$, where*

$$\epsilon_1(m,n)=\begin{cases}1 & \text{if } D(g_1)|m \text{ and } \nu_2(n)\le\nu_2(m);\\ 1 & \text{if } D(g_1)|m \text{ and } 2||n;\\ 1 & \text{if } D(-g_1)|m \text{ and } 4||n;\\ 1 & \text{if } D(2g_1)|m \text{ and } 8||n;\\ 2 & \text{otherwise.}\end{cases}$$

Proof. If $p|D(g_1)$ and p is odd, then p ramifies in $\mathbb{Q}(\zeta_m,\zeta_n\sqrt{g_1})$. This shows that if in addition $p\nmid n$, then $[\mathbb{Q}(\zeta_m,\zeta_n\sqrt{g_1}):\mathbb{Q}(\zeta_m)]=2$ (since then p does not ramify in $\mathbb{Q}(\zeta_m)$). The rest of the argument requires some case distinctions and is left to the interested reader. □

`Example`. The result predicts that $\mathbb{Q}(i,\zeta_8\sqrt{2})=\mathbb{Q}(i)$. Indeed, note that $\zeta_8\sqrt{2}=1+i$.

Lemma 6 *Let $L:\mathbb{Q}$ be abelian with $L\subseteq M$. If*

$$[\mathbb{Q}(\zeta_f)\cap L:\mathbb{Q}]=[\mathbb{Q}(\zeta_f)\cap M:\mathbb{Q}]. \qquad (4)$$

for every integer f, then L is the maximal abelian subfield of M.

Proof. Suppose there is an abelian field L_1 with $L\subsetneq L_1\subset M$. Let $f(L_1)$ be the conductor of L_1. Then

$$[\mathbb{Q}(\zeta_{f(L_1)})\cap M:\mathbb{Q}]\ge[L_1:\mathbb{Q}]>[L:\mathbb{Q}]=[\mathbb{Q}(\zeta_{f(L_1)})\cap L:\mathbb{Q}].$$

This contradicts equation (4) with $f=f(L_1)$. □

With some additional effort one can explicitly describe $\mathbb{Q}(\zeta_f)\cap K_{n,n}$. Clearly this intersection field is abelian and contains $\mathbb{Q}(\zeta_{(f,n)})$. Let us first compute the absolute degree of $K_{[f,n],n}$. We have

$$[K_{[f,n],n}:\mathbb{Q}]=\frac{\varphi(f)[K_{n,n}:\mathbb{Q}]}{[\mathbb{Q}(\zeta_f)\cap K_{n,n}:\mathbb{Q}]}. \tag{5}$$

On noting that $\varphi((f,n))\varphi([f,n])=\varphi(f)\varphi(n)$, it follows from Lemma 3 and (5) that

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

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 $\mathbb{Q}(\zeta_f)\cap K_{n,n}$ is equal to $\mathbb{Q}(\zeta_{(f,n)})$ or a quadratic extension thereof.

Definition 2 *Let D be a fundamental discriminant. Put $b=D/(f,D)$ and let $f_{\rm odd}$ be the largest odd divisor of f. Put*

$$\gamma(D)=\begin{cases}(-1)^{\frac{(f_{\rm odd},D)-1}{2}}(f_{\rm odd},D) & \text{if } \nu_2(f)<\nu_2(D);\\ (-1)^{\frac{b-1}{2}}(f,D) & \text{otherwise.}\end{cases}$$

Put

$$\gamma_0(D)=\begin{cases}\gamma(D) & \text{if } D\nmid n \text{ and } D|[f,n];\\ 1 & \text{otherwise.}\end{cases}$$

Put

$$\gamma_1(D)=\begin{cases}\gamma(D) & \text{if } \nu_2(f)>\nu_2(n) \text{ and } D|[f,n];\\ 1 & \text{otherwise.}\end{cases}$$

Lemma 7 *The numbers $\gamma(D)$, $\gamma_0(D)$, $\gamma_1(D)$, $\frac{D}{\gamma(D)}$, $\frac{D}{\gamma_0(D)}$ and $\frac{D}{\gamma_1(D)}$ are all fundamental discriminants.*

Proof. This requires a few case distinctions and is left to the reader. □

`Remark`. In this notation the dependence on f and n is suppressed. It would be more accurate to write $\gamma_0(D;f,n)$ etcetera. This notation is used in Lemma 12.

Lemma 8 *Let $g_1\neq 0$ be a rational number. Then*

$$[\mathbb{Q}(\zeta_f)\cap\mathbb{Q}(\zeta_n,\sqrt{g_1}):\mathbb{Q}(\zeta_{(f,n)})]=\begin{cases}2 & \text{if } D(g_1)\nmid n \text{ and } D(g_1)|[f,n];\\ 1 & \text{otherwise.}\end{cases}$$

Furthermore,

$$\mathbb{Q}(\zeta_f)\cap\mathbb{Q}(\zeta_n,\sqrt{g_1})=\mathbb{Q}(\zeta_{(f,n)},\sqrt{\gamma_0(D(g_1))}),$$

with $\gamma_0(D(g_1))\neq 1$ iff $D(g_1)\nmid n$ and $D(g_1)|[f,n]$.

Proof. Using Lemma 1 we find that

$$[\mathbb{Q}(\zeta_n,\sqrt{g_1}):\mathbb{Q}]=\varphi(n)\epsilon_2(n),\ \text{where } \epsilon_2(n)=\begin{cases}1 & \text{if } D(g_1)|n;\\ 2 & \text{otherwise.}\end{cases}$$

It then follows (cf. the argument leading up to (6)) that $[\mathbb{Q}(\zeta_f)\cap\mathbb{Q}(\zeta_n,\sqrt{g_1}) : \mathbb{Q}(\zeta_{(f,n)})]=\epsilon_2(n)/\epsilon_2([f,n])$. Thus our field intersection is quadratic over $\mathbb{Q}(\zeta_{(f,n)})$ if $D(g_1)\nmid n$ and $D(g_1)|[f,n]$ and equals $\mathbb{Q}(\zeta_{(f,n)})$ otherwise. In the latter case $\gamma_0(D(g_1))=1$ and we are done. Next assume that $D(g_1)\nmid n$ and $D(g_1)|[f,n]$. Write $\gamma=\gamma_0(D(g_1))$. By Lemma 7 γ is a fundamental discriminant and hence by Lemma 1 $\mathbb{Q}(\sqrt{\gamma})$ is a quadratic field of conductor $|\gamma|$. Since $\gamma|f$, it follows that $\sqrt{\gamma}\in\mathbb{Q}(\zeta_f)$. Likewise, using Lemma 7, it is seen that $\mathbb{Q}(\sqrt{D(g_1)/\gamma})$ is a field of conductor $|D(g_1)/\gamma|$. Note that the assumption that $D(g_1)$ divides $[f,n]$ implies that $\frac{D(g_1)}{(f,D(g_1))}|\frac{n}{(f,n)}|n$ and, in case $\nu_2(f)<\nu_2(D)$, that $\nu_2(n)\ge\nu_2(D(g_1))$. Using this we infer that $\sqrt{D(g_1)/\gamma}\in\mathbb{Q}(\zeta_n)$. Since $\sqrt{D(g_1)}\in\mathbb{Q}(\zeta_n,\sqrt{g_1})$, it follows that $\sqrt{\gamma}\in\mathbb{Q}(\zeta_n,\sqrt{g_1})$. The proof will now be completed once we show that $\sqrt{\gamma}\notin\mathbb{Q}(\zeta_{(f,n)})$. Assume that $\sqrt{\gamma}\in\mathbb{Q}(\zeta_{(f,n)})$. Then one infers, using that γ is a fundamental discriminant and, in case $\nu_2(f)<\nu_2(D)$, that $\nu_2(n)\ge\nu_2(D)$, that $(f,D(g_1))|(f,n)$. This together with $\frac{D(g_1)}{(f,D(g_1))}|\frac{n}{(f,n)}$ then leads to the conclusion that $D(g_1)|n$, contradicting our assumption that $D(g_1)\nmid n$. □

Lemma 9 *Let $g_1\ne 0$ be a rational number. We have*

$$\mathbb{Q}(\zeta_n,\zeta_{2n}\sqrt{g_1})=\begin{cases}\mathbb{Q}(\zeta_n,\sqrt{g_1}) & \text{if } 2\nmid n;\\ \mathbb{Q}(\zeta_n,\sqrt{-g_1}) & \text{if } \nu_2(n)=1;\\ \mathbb{Q}(\zeta_n,\sqrt{2g_1}) & \text{if } \nu_2(n)=2 \text{ and } 8|D(g_1),\end{cases}\tag{7}$$

and in these cases the intersection $I=\mathbb{Q}(\zeta_f)\cap\mathbb{Q}(\zeta_n,\zeta_{2n}\sqrt{g_1})$ can be determined using Lemma 8. Next assume that none of the conditions (7) *are satisfied. Then*

$$[I:\mathbb{Q}(\zeta_{(f,n)})]=\begin{cases}2 & \text{if } D(g_1)|[f,n] \text{ and } \nu_2(f)>\nu_2(n);\\ 1 & \text{otherwise.}\end{cases}$$

Furthermore,

$$I=\begin{cases}\mathbb{Q}(\zeta_{(f,n)},\zeta_{2(f,n)}\sqrt{\gamma(D(g_1))}) & \text{if } D(g_1)|[f,n] \text{ and } \nu_2(f)>\nu_2(n);\\ \mathbb{Q}(\zeta_{(f,n)}) & \text{otherwise.}\end{cases}$$

Proof. Let us consider the case where $4|n$, not both $8|D(g_1)$ and $4||n$, and such that, moreover, $D(g_1)|[f,n]$ and $\nu_2(f)>\nu_2(n)$. As in the proof of Lemma 8 we infer that $\sqrt{\gamma(D(g_1))}\in\mathbb{Q}(\zeta_f)$. Since $\nu_2(f)>\nu_2(n)$, we infer that $\zeta_{2(f,n)}\sqrt{\gamma(D(g_1))}$ is in $\mathbb{Q}(\zeta_f)$. As in the proof of Lemma 8 we infer that $\sqrt{D(g_1)/\gamma(D(g_1))}\in\mathbb{Q}(\zeta_n)$. Since $\zeta_{2(f,n)}\sqrt{D(g_1)}\in\mathbb{Q}(\zeta_n,\zeta_{2n}\sqrt{g_1})$, we infer that $\zeta_{2(f,n)}\sqrt{\gamma(D(g_1))}\in\mathbb{Q}(\zeta_n,\zeta_{2n}\sqrt{g_1})$. It remains to show that $\zeta_{2(f,n)}\sqrt{\gamma(D(g_1))}\notin\mathbb{Q}(\zeta_{(f,n)})$. If the latter element would be contained in $\mathbb{Q}(\zeta_{(f,n)})$, by Lemma 5 we would have $D(2\gamma(D(g_1)))|(f,n)$ and $8||2(f,n)$. Note that these conditions imply that $8|D(2g_1)$ and $8|f$ and so $8|D(2\gamma(D(g_1)))|(f,n)$, contradicting the assumption that $4||(f,n)$. Note that

$$[I:\mathbb{Q}(\zeta_{(f,n)})]=[\mathbb{Q}(\zeta_f)\cap\mathbb{Q}(\zeta_n,\zeta_{2n}\sqrt{g_1}):\mathbb{Q}(\zeta_{(f,n)})]=\frac{\epsilon_1(n,2n)}{\epsilon_1([f,n],2n)}.\tag{8}$$

The conditions imposed ensure that $\epsilon_1(n,n)=1$. Using (8) and Lemma 5 it follows that

$$[I:\mathbb{Q}(\zeta_{(f,n)})]=\begin{cases}2 & \text{if } D(g_1)|[f,n] \text{ and } \nu_2(f)>\nu_2(n);\\ 2 & \text{if } D(2g_1)|[f,n] \text{ and } \nu_2(n)=2;\\ 1 & \text{otherwise.}\end{cases}$$

Let us assume that $D(2g_1)|[f,n]$ and $\nu_2(n)=2$. Since if $\nu_2(n)=2$, then $8\nmid D(g_1)$ (by assumption), it follows that $\nu_2(f)>\nu_2(n)$ and so $D(g_1)|[f,n]$. It follows that

$$[I:\mathbb{Q}(\zeta_{(f,n)})]=\begin{cases}2 & \text{if } D(g_1)|[f,n] \text{ and } \nu_2(f)<\nu_2(n);\\ 1 & \text{otherwise.}\end{cases}$$

This concludes the proof. □

Let $K_{n,n}^{\rm ab}$ denote the maximal abelian subfield of $K_{n,n}$. Note that $\mathbb{Q}(\zeta_f)\cap K_{n,n}=\mathbb{Q}(\zeta_f)\cap K_{n,n}^{\rm ab}$. In the next lemma $K_{n,n}^{\rm ab}$ is determined. Note that for each choice of g precisely one of the seven cases applies.

Lemma 10 *Let g and g_0 be as in Lemma* 3. *Let $K_{n,n}^{\rm ab}$ denote the maximal abelian subfield of $K_{n,n}$. We have*
1) $K_{n,n}^{\rm ab}=\mathbb{Q}(\zeta_n)$ *if* $g>0$ *and* $\nu_2(n)\le\nu_2(h)$;
2) $K_{n,n}^{\rm ab}=\mathbb{Q}(\zeta_n,\sqrt{g_0})$ *if* $g>0$ *and* $\nu_2(n)\ge\nu_2(h)+1$;
3) $K_{n,n}^{\rm ab}=\mathbb{Q}(\zeta_n,\sqrt{g_0})$ *if* $g<0$ *and* $\nu_2(n)\ge\nu_2(h)+2$;
4) $K_{n,n}^{\rm ab}=\mathbb{Q}(\zeta_n,\sqrt{-g_0})$ *if* $g<0,\ \nu_2(n)=1$ *and* $\nu_2(h)=0$;
5) $K_{n,n}^{\rm ab}=\mathbb{Q}(\zeta_n,\sqrt{2g_0})$ *if* $g<0,\ \nu_2(h)=1,\ \nu_2(n)=2$ *and* $8|D(g_0)$;
6) $K_{n,n}^{\rm ab}=\mathbb{Q}(\zeta_{2n})$ *if* $g<0$ *and* $\nu_2(n)\le\nu_2(h)$;
7) $K_{n,n}^{\rm ab}=\mathbb{Q}(\zeta_n,\zeta_{2n}\sqrt{g_0})$ *if* $g<0$ *and* $\nu_2(n)=\nu_2(h)+1$ *and none of the previous cases apply.*

The latter result can be formulated more compactly, but with regards to computing $\mathbb{Q}(\zeta_f)\cap K_{n,n}$ the more extended formulation turns out to be more suitable. A more compact reformulation of Lemma 10 is as follows.

Proposition 2 *If $g>0$, then*

$$K_{n,n}^{\rm ab}=\begin{cases}\mathbb{Q}(\zeta_n) & \text{if } \nu_2(n)\le\nu_2(h);\\ \mathbb{Q}(\zeta_n,\sqrt{g_0}) & \text{if } \nu_2(n)>\nu_2(h).\end{cases}$$

If $g<0$, then

$$K_{n,n}^{\rm ab}=\begin{cases}\mathbb{Q}(\zeta_{2n}) & \text{if } \nu_2(n)\le\nu_2(h);\\ \mathbb{Q}(\zeta_n,\zeta_{2n}\sqrt{g_0}) & \text{if } \nu_2(n)=\nu_2(h)+1;\\ \mathbb{Q}(\zeta_n,\sqrt{g_0}) & \text{if } \nu_2(n)\ge\nu_2(h)+2.\end{cases}$$

Proof of Lemma 10. For each of the seven cases one easily checks that the explicit field indicated, let us call it E, is abelian and is contained in $K_{n,n}^{\rm ab}$. The idea is now to apply Lemma 6 with $L=E$ and $M=K_{n,n}$. By (6) it follows that $[\mathbb{Q}(\zeta_f)\cap K_{n,n}:\mathbb{Q}]=\varphi((f,n))\epsilon([f,n],n)/\epsilon(n,n)$. In cases 1 and 6 the degree $[\mathbb{Q}(\zeta_f)\cap E:\mathbb{Q}]$ is trivially determined. In the cases 2, 3, 4 and 5 it can be determined by invoking Lemma 8. In the remaining case 6 we apply Lemma 9. One computes that in each of the seven cases $[\mathbb{Q}(\zeta_f)\cap E:\mathbb{Q}]=[\mathbb{Q}(\zeta_f)\cap K_{n,n}:\mathbb{Q}]$ for every f and hence the result then follows on invoking Lemma 6.

As an example we deal with case 2. One checks that $\mathbb{Q}(\zeta_n,\sqrt{g_0})\subseteq K_{n,n}^{\rm ab}$. By Lemma 8 it follows that

$$[\mathbb{Q}(\zeta_f)\cap\mathbb{Q}(\zeta_n,\sqrt{g_0}):\mathbb{Q}(\zeta_{(f,n)}]=\begin{cases}2 & \text{if } D(g_0)\nmid n \text{ and } D(g_0)|[f,n];\\ 1 & \text{otherwise.}\end{cases}$$

On the other hand, by (6) and Lemma 3,

$$[\mathbb{Q}(\zeta_f)\cap K_{n,n}^{\mathrm{ab}} : \mathbb{Q}(\zeta_{(f,n)}] = \frac{\epsilon([f,n],n)}{\epsilon(n,n)} = \begin{cases} 2 & \text{if } D(g_0)\nmid n \text{ and } D(g_0)|[f,n]; \\ 1 & \text{otherwise.} \end{cases}$$

The proof of this case then follows on invoking Lemma 6. □

Next we compute the intersection of $\mathbb{Q}(\zeta_f)$ with the fields given in Lemma 10. To this end we require a definition.

Definition 3 *In each of the seven cases as described in* Lemma 10, *we define* $\gamma_g(f,n)$ *as follows.*
1) $\gamma_g(f,n)=1$.
2) $\gamma_g(f,n)=\gamma_0(D(g_0))$.
3) $\gamma_g(f,n)=\gamma_0(D(g_0))$.
4) $\gamma_g(f,n)=\gamma_0(D(-g_0))$.
5) $\gamma_g(f,n)=\gamma_0(D(2g_0))$.
6) $\gamma_g(f,n)=1$.
7) $\gamma_g(f,n)=\gamma_1(D(g_0))$.

Definition 4 *If* $\nu_2(f)>\nu_2(n)\ge 1$ *and either we are in case* 6 *or we are in case* 7 *and* $D(g_0)|[f,n]$, *then we say we are in the exceptional case.*

Note that if h is odd or $g>0$, the exceptional case does not arise.

Now the main result of this section can be formulated:

Theorem 5 *The equality* $\mathbb{Q}(\zeta_f)\cap K_{n,n}=\mathbb{Q}(\zeta_{(f,n)},\sqrt{\gamma_g(f,n)})$ *holds, unless we are in the exceptional case when we have*

$$\mathbb{Q}(\zeta_f)\cap K_{n,n}=\mathbb{Q}(\zeta_{(f,n)},\zeta_{2(f,n)}\sqrt{\gamma_g(f,n)}).$$

Proof. Follows on combining Lemma 10 with Lemma 9 and Lemma 8. □

Corollary 2 *Suppose that either* $g>0$ *or* $g<0$ *and* h *is odd. Then*

$$\mathbb{Q}(\zeta_f)\cap K_{n,n} = \begin{cases} \mathbb{Q}(\zeta_{(f,n)},\sqrt{\gamma_0(D(g))}) & \text{if } \nu_2(n)\ge\nu_2(h)+1; \\ \mathbb{Q}(\zeta_{(f,n)}) & \text{otherwise.} \end{cases}$$

Proof. By Lemma 10 we have

$$K_{n,n}^{\mathrm{ab}} = \begin{cases} \mathbb{Q}(\zeta_n,\sqrt{g}) & \text{if } \nu_2(n)\ge\nu_2(h)+1; \\ \mathbb{Q}(\zeta_n) & \text{otherwise.} \end{cases}$$

Now invoke Lemma 8. □

Lemma 11 *Let* a *and* f *be natural numbers that are coprime. Then the density of primes* p *such that* p *splits completely in* $K_{n,n}$ *and* $p\equiv a(\mathrm{mod}\ f)$ *is zero if* $a\not\equiv 1(\mathrm{mod}\ (f,n))$ *and equals*

$$\frac{1+\epsilon_3(a,f,n)(\frac{\gamma_g(f,n)}{a})}{2[K_{[f,n],n}:\mathbb{Q}]}$$

otherwise, where $(\frac{\cdot}{\cdot})$ *denotes the Kronecker symbol and*

$$\epsilon_3(a,f,n) = \begin{cases} (-1)^{\frac{a-1}{(f,n)}} & \text{in the exceptional case;} \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Using Chebotarev's Density Theorem we infer that the set under consideration has a density and that the density equals $1/[K_{[f,n],n}:\mathbb{Q}]$ if the restriction of σ_a to $\mathbb{Q}(\zeta_f)\cap K_{n,n}$ is the identity and zero otherwise. The latter intersection of fields always contains $\zeta_{(f,n)}$. So if $a\not\equiv 1(\mathrm{mod}\ (f,n))$, then σ_a does not leave $\zeta_{(f,n)}$ fixed and the density is zero. So assume that $a\equiv 1(\mathrm{mod}\ (f,n))$. Using Lemma 2 and the fact that $\gamma_g(f,n)$ is a fundamental discriminant, we infer that $\sigma_a(\sqrt{\gamma_g(f,n)})=(\frac{\gamma_g(f,n)}{a})\sqrt{\gamma_g(f,n)}$. Furthermore, we have $\sigma_a(\zeta_{2(f,n)})=(-1)^{(a-1)/(f,n)}\zeta_{2(f,n)}=\epsilon_3(a,f,n)\zeta_{2(f,n)}$. On invoking Theorem 5 the result then follows. □

`Remark`. If $\alpha\in\mathbb{Q}(\zeta_f)\cap K_{n,n}$ and $\alpha\notin\mathbb{Q}(\zeta_{(f,n)})$, then $\sigma_a(\alpha)=\epsilon_3(a,f,n)(\frac{\gamma_g(f,n)}{a})\alpha$.

Corollary 3 *Let n be squarefree. Put $t_d=(t,d^\infty)$. The density of primes p such that $p\equiv 1+ta(\mathrm{mod}\ dt)$ and p splits completely in $K_{nt,nt}$ equals zero if $(d,n)\nmid a$ or $(1+ta,d)>1$, otherwise it equals*

$$\frac{1+\epsilon_3(1+ta,dt,nt)(\frac{\gamma_g(dt,nt)}{1+ta})}{2[K_{[d,n]t,nt}:\mathbb{Q}]}=\frac{1+\epsilon_3(1+ta,dt_d,nt)(\frac{\gamma_g(dt_d,nt)}{1+ta})}{2[K_{[d,n]t,nt}:\mathbb{Q}]},\tag{9}$$

where

$$\epsilon_3(1+ta,dt_d,nt)=\begin{cases}(-1)^{\frac{a}{(d,n)}} & \textit{in the exceptional case;}\\ 1 & \textit{otherwise.}\end{cases}$$

Proof. This follows from Lemma 11 together with the observation that the two systems of congruences

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

are equivalent. □

`Remark`. The equivalence of the system of congruences shows that $[dt_d,nt]=[dt,nt]=[d,n]t$, an observation that will be needed later (e.g. in the proof of Lemma 12).

The advantage of the formula on the right hand side of (9) is that the numbers $\gamma_g(dt_d,nt)$ that occur are restricted to a finite set of divisors, namely those of $(4d,D(g_0))$, so this is a very restricted set of numbers. The situation is described more precisely by the next result (the easy proof of which is left to the reader).

Lemma 12 *Let D be a fundamental discriminant.*
If $(d,D)=1$, then $\gamma_0(D;dt_d,nt)=1$. Assume that $(d,D)\neq 1$. Set

$$\Delta_1(D)=(-1)^{\frac{(d_{\mathrm{odd}},D)-1}{2}}(d_{\mathrm{odd}},D)\text{ and }\Delta_2(D)=(-1)^{\frac{D/(8d,D)-1}{2}}(8d,D).$$

1) *If $2\nmid d$, then*

$$\gamma_0(D;dt_d,nt)=\begin{cases}\Delta_1(D) & \textit{if } D\nmid nt \textit{ and } D|[d,n]t;\\ 1 & \textit{otherwise,}\end{cases}$$

where $\Delta_1(D)|d$.
2) *If* $\nu_2(d) \geq \nu_2(D)$, *then*

$$\gamma_0(D; dt_d, nt) = \begin{cases} \Delta_2(D) & \text{if } D \nmid nt \text{ and } D|[d,n]t; \\ 1 & \text{otherwise,} \end{cases}$$

where $\Delta_2(D)|d$.
3) *If* $1 \leq \nu_2(d) < \nu_2(D)$, *then*

$$\gamma_0(D; dt_d, nt) = \begin{cases} \Delta_1(D) & \text{if } \nu_2(t) < \nu_2(D/d),\ D \nmid nt \text{ and } D|[d,n]t; \\ \Delta_2(D) & \text{if } \nu_2(t) \geq \nu_2(D/d),\ D \nmid nt \text{ and } D|[d,n]t; \\ 1 & \text{otherwise,} \end{cases}$$

where $\Delta_1(D)|d/2$ *and* $\Delta_2(D)|4d$.

The symbol $(\frac{\gamma_g(f,n)}{a})$ appearing in Lemma 11 has a preference (certainly as $D(g_0)$ becomes large), to be equal to 1. This can be quantified as follows.

Proposition 3 *Let* a *and* f *be natural numbers that are coprime and assume that* $a \equiv 1(\text{mod } (f,n))$. *Then* $(\frac{\gamma_g(f,n)}{a}) \neq 0$. *If* $D(g_0)_{\text{odd}} \nmid [f,n]$, *then* $(\frac{\gamma_g(f,n)}{a}) = 1$.

Proof. Since by definition $\gamma_g(f,n)|f$ and by assumption $(a,f)=1$, the definition of the Kronecker symbol implies that $(\frac{\gamma_g(f,n)}{a}) \neq 0$. If $D(g_0)_{\text{odd}} \nmid [f,n]$, then Definition 3 implies that $\gamma_g(f,n)=1$. On noting that $(\frac{\gamma_g(f,n)}{a}) = (\frac{1}{a}) = 1$, the result follows. $\square$

`Remark`. When h is odd the conclusion of Proposition 3 holds if we make the (weaker) assumption that $D(g) \nmid [f,n]$.

3 A more explicit formula for $\delta_g(a,d)$

After all this preparation we can rewrite (2) in a more explicit form involving the Kronecker symbol.

Theorem 6 (GRH). *Let* $a \geq 1$ *and* $t_d = (t, d^\infty)$. *Then*

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

where

$$c_g(1+ta, dt, nt) = \frac{1}{2}\left(1 + \epsilon_3(1+ta, dt_d, nt)\left(\frac{\gamma_g(dt_d, nt)}{1+ta}\right)\right),$$

with $\gamma_g(\cdot,\cdot)$ *as in Definition* 3, $(\frac{\cdot}{\cdot})$ *the Kronecker symbol and where* $\epsilon_3(1+ta, dt_d, nt)$ *equals* $(-1)^{a/(d,n)}$ *if* $\nu_2(d) > \nu_2(n)$, $\nu_2(nt) \geq 1$ *and* $K^{\text{ab}}_{nt,nt}$ *falls under case* 6 *or* 7 *of Lemma* 10 *and where* $\epsilon_3(1+ta, dt_d, nt) = 1$ *otherwise.*

Proof. Follows from (2), the observation that $c_g(1+ta,dt,nt)/[K_{[d,n]t,nt}:\mathbb{Q}]$ is the density of primes $p\equiv 1+ta(\text{mod } dt)$ that split completely in $K_{nt,nt}$, Corollary 3 and the definition of the exceptional case. □

`Remark`. If $g>0$, d is odd or h is odd the exceptional case does not arise and hence $\epsilon_3(.,.,.)=1$ for the relevant values of t and n.

`Example`. Suppose that h is odd and that, furthermore, d is odd or $8|d$. Then, on GRH,

$$\delta_g(a,d)=\delta_g^{(0)}(a,d)-\sum_{\substack{t=1\\(1+ta,d)=1\\(\frac{\delta}{1+ta})=-1}}^{\infty}\ \sum_{\substack{n=1,\ (d,n)|a\\ D(g)\nmid nt,\ D(g)|[d,n]t\\ \nu_2(nt)\ge 1}}^{\infty}\frac{\mu(n)}{[K_{[d,n]t,nt}:\mathbb{Q}]},\tag{10}$$

where

$$\delta=\begin{cases}\Delta_1(D(g)) & \text{if } d \text{ is odd;}\\ \Delta_2(D(g)) & \text{if } 8|d,\end{cases}$$

where Δ_1 and Δ_2 are as in Lemma 12 and divide d. Alternatively one can write

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

`Example`. If $g>0$ and either d is odd or $8|d$, then, on GRH, (10) holds with the condition $\nu_2(nt)\ge 1$ replaced by $\nu_2(nt)\ge\nu_2(h)+1$ and $D(g)$ by $D(g_0)$.

`Example` (occurrence of exceptional case). Suppose that $8|d$, $g<0$ and $\nu_2(h)\ge 2$. Let t and n be such that $(1+ta,d)=1$ and $(n,d)|a$. Let $\delta=\Delta_2(D(g_0))$. Then

$$2c_g(1+ta,dt,nt)=\begin{cases}1+(\frac{\delta}{1+ta}) & \text{if } \nu_2(nt)\ge\nu_2(h)+2;\\ 1+(-1)^{\frac{a}{(d,n)}}(\frac{\delta}{1+ta}) & \text{if } \nu_2(nt)=\nu_2(h)+1 \text{ and } D(g_0)|[d,n]t;\\ 2 & \text{otherwise.}\end{cases}$$

In case $1\le\nu_2(d)\le 2$ more complicated formulae for $\delta_g(a,d)$ arise. For our purposes it turns out, however, that in order to prove Theorem 3 or part 2 of Theorem 4 these are not needed.

4 Relating $\delta_{-g}(a,d)$ to $\delta_g(a,d)$

In this section $\delta_{-g}(a,d)$ is related to $\delta_g(a,d)$ (where $g>0$). Since the case where g is negative is algebraically rather more complicated, this connection can sometimes be used to simplify proofs.

The basic observation is the following:

Lemma 13 *Let p be odd and $g\ne 0$ be a rational number. Suppose that $\nu_p(g)=0$. Then*

$$\text{ord}_p(-g)=\begin{cases}2\text{ord}_p(g) & \text{if } 2\nmid\text{ord}_p(g);\\ \text{ord}_p(g)/2 & \text{if } \text{ord}_p(g)\equiv 2(\text{mod } 4);\\ \text{ord}_p(g) & \text{if } 4|\text{ord}_p(g).\end{cases}$$

Proof. Left to the reader. □

Using this observation the following result is almost immediate.

Proposition 4 (GRH). *Suppose $g > 0$. There is an integer $1 \le k \le 4$ and integers a_j, d_j for $1 \le j \le k$ such that $\delta_{-g}(a,d) = \sum_{j=1}^{k} \delta_g(a_j, d_j)$, where $d_j | \frac{8d}{(4,d)}$.*

Proof. First suppose that $4|d$. Then, by Lemma 13,

$$\delta_{-g}(a,d) = \begin{cases} \delta_g(2a, 2d) & \text{if } 2 \nmid a; \\ \delta_g(a/2, d/2) & \text{if } a \equiv 2 (\text{mod } 4); \\ \delta_g(a,d) & \text{if } a \equiv 0 (\text{mod } 4). \end{cases} \tag{11}$$

If $2|d$ we write $\delta_{-g}(a,d) = \delta_{-g}(a,2d) + \delta_{-g}(a+d,2d)$ and apply (11) to each of the summands. If $2 \nmid d$, we write

$$\delta_{-g}(a,d) = \delta_{-g}(a,4d) + \delta_{-g}(a+d,4d) + \delta_{-g}(a+2d,4d) + \delta_{-g}(a+3d,4d)$$

and apply (11) to each of the summands. □

5 Proof of Theorems 1 and 2

Proof of Theorem 1. A proof of part 1, based on part 1 of Lemma 4 was given in [M-II]. Similarly part 2 can be proved using part 2 of Lemma 4. The result for $\delta_g^{(0)}$ follows trivially from Lemma 4 and for δ it follows easily from part 1 of Theorem 1 of [M-I]. □

Proof of Theorem 2.
Proof of the inequality for $|\delta_g^{(0)}(a,d) - \delta(a,d)|$. Using Lemma 3 we infer that

$$\delta_g^{(0)}(a,d) = \sum_{\substack{t=1 \\ (1+ta,d)=1}}^{\infty} \sum_{\substack{n=1 \\ (n,d)|a}}^{\infty} \frac{\mu(n)}{\varphi([d,n]t)nt} + E, \tag{12}$$

with

$$|E| \le \sum_{\substack{t=1 \\ (1+ta,d)=1}}^{\infty} \sum_{\substack{n=1 \\ (n,d)|a,\ D(g)|dnt}}^{\infty} \frac{|\mu(n)|}{\varphi([d,n]t)nt}.$$

Let us denote the latter double sum by E_1. Note that

$$\begin{aligned} E_1 &\le \sum_{t=1}^{\infty} \sum_{\substack{n=1 \\ D(g)|dnt}}^{\infty} \frac{|\mu(n)|}{\varphi(nt)nt} = \sum_{D_1|v} \frac{2^{\omega(v)}}{\varphi(v)v} \\ &= \sum_{v_1=1}^{\infty} \frac{2^{\omega(D_1 v_1)}}{\varphi(D_1 v_1) D_1 v_1} \le \frac{2^{\omega(D_1)}}{\varphi(D_1)D_1} \sum_{v=1}^{\infty} \frac{2^{\omega(v)}}{\varphi(v)v} < \frac{2^{\omega(D_1)+2}}{\varphi(D_1)D_1}. \end{aligned} \tag{13}$$

By Theorem 3 of [M-Av] the second double sum in (12) equals $\delta(a,d)$. □

`Remark`. In case $(a,d)=1$, the term $\varphi(D_1)$ in the first inequality of Theorem 2 can be replaced by $\varphi(dD_1)$.

Proof of the inequality for $|\delta_g(a,d)-\delta(a,d)|$. Using Theorem 6 and the remark following Proposition 3 we have $\delta_g(a,d)=\delta_g^{(0)}(a,d)+E_2$, with

$$|E_2|\le \sum_{\substack{t=1\\(1+ta,d)=1}}^{\infty}\ \sum_{\substack{n=1\\(n,d)|a,\ D(g)|[d,n]t}}^{\infty}\frac{|\mu(n)|}{[K_{[d,n]t,nt}:\mathbb{Q}]}.$$

Using Lemma 3 we infer that

$$|E_2|\le 2\sum_{\substack{t=1\\(1+ta,d)=1}}^{\infty}\ \sum_{\substack{n=1\\(n,d)|a,\ D(g)|dnt}}^{\infty}\frac{|\mu(n)|}{\varphi([d,n]t)nt}=2E_1.$$

Using (13), we then infer that $|E_2|<2^{\omega(D_1)+3}/(\varphi(D_1)D_1)$. From the latter estimate, (13) and the inequality for $\delta_g^{(0)}(a,d)$, the result then follows. □

Proof of inequality for $|\rho_g(a,d)-\rho(a,d)|$. For this, see the proof of Proposition 5 of [M-Av]. □

6 The index reconsidered

In this section we compare $\rho_g(a,d)$ with its average value $\rho(a,d)$. We will use the following two lemmas.

Lemma 14 [M-II]. *Let $d\ge 3$. The number of integers $1\le g\le x$ such that $D(g)$ has no prime divisor p with $p\equiv 1(\text{mod } d)$ is $O_d(x\log^{-1/\varphi(d)}x)$. The same assertion holds with $D(g)$ replaced by $D(-g)$.*

The following simple result is also needed.

Lemma 15 *If $p|v$ with $p\equiv 1(\text{mod } d)$ and $p\nmid m$, then*

$$\sum_{\substack{t\equiv a(\text{mod } d)\\ t|v,\ (\frac{v}{t},m)|r}}\mu(\frac{v}{t})=0.$$

Proof. Let $p^e||v$. Put $v_1=v/p^e$. Then

$$\sum_{\substack{t\equiv a(\text{mod } d)\\ t|v,\ (\frac{v}{t},m)=\alpha}}\mu(\frac{v}{t})=\sum_{j=0}^{e}\ \sum_{\substack{t\equiv a(\text{mod } d)\\ t|v_1,\ (\frac{v_1}{t},m)=\alpha}}\mu(p^j\frac{v_1}{t})=\sum_{j=0}^{1}(-1)^j\sum_{\substack{t\equiv a(\text{mod } d)\\ t|v_1,\ (\frac{v_1}{t},m)=\alpha}}\mu(\frac{v_1}{t})=0.$$

Proposition 5 (GRH). *Let $\alpha=(a,d)$ and $d_1=d/\alpha$. Suppose that $g\in G$ and $D(g)$ has a prime divisor p with $p\equiv 1(\text{mod } d_1)$ and $p\nmid\alpha$, then $\rho_g(a,d)=\rho(a,d)$.*

Proof. On GRH we have (see [M-I])

$$\rho_g(a,d)=\sum_{t\equiv a(\bmod\ d)}\sum_{v=1}^{\infty}\frac{\mu(v)}{[K_{vt,vt}:\mathbb{Q}]}=\sum_{w=1}^{\infty}\frac{\sum_{t|w,\ t\equiv a(\bmod\ d)}\mu(\frac{w}{t})}{[K_{w,w}:\mathbb{Q}]}.$$

By [M-Av] we have

$$\rho(a,d)=\sum_{w=1}^{\infty}\frac{\sum_{t|w,\ t\equiv a(\bmod\ d)}\mu(\frac{w}{t})}{w\varphi(w)}.$$

Let n_1 be as in Lemma 3 (note that $n_1=[2,D(g)]$). The assumption that $g\in G$ ensures, by Lemma 3, that

$$\begin{aligned}\rho_g(a,d) &= \rho(a,d)+\sum_{n_1|w}\frac{\sum_{t|w,\ t\equiv a(\bmod\ d)}\mu(\frac{w}{t})}{w\varphi(w)}.\\ &= \rho(a,d)+\sum_{\frac{n_1}{(n_1,\alpha)}|w}\frac{\sum_{t|w,\ t\equiv a/\alpha(\bmod\ d_1)}\mu(\frac{w}{t})}{w\alpha\varphi(w\alpha)}.\end{aligned}$$

If $p|D(g)$, $p\equiv 1(\bmod\ d_1)$ and $p\nmid\alpha$, then $p|\frac{n_1}{(n_1,\alpha)}$ and so p divides every w occurring in the latter sum and hence, by Lemma 15, this sum will equal zero. □

Proposition 6 (GRH). *Let $\alpha=(a,d)$ and $d_1=d/\alpha$. For almost all integers g we have $\rho_g(a,d)=\rho(a,d)$. More precisely, if $d_1\le 2$, then there are at most $O_d(\sqrt{x})$ integers g with $|g|\le x$ such that $\rho_g(a,d)\ne\rho_g(a,d)$. If $d_1\ge 3$, then there are at most $O_d(x\log^{-1/\varphi(d_1)}x)$ integers g with $|g|\le x$ such that, moreover, $\rho_g(a,d)\ne\rho(a,d)$.*

Proof. In case $d_1\le 2$, then $\rho_g(a,d)=\rho(a,d)$ for those g for which $g\in G$ and $D(g)$ is not in a certain finite set by the previous proposition. The set of remaining g is of size $O_d(\sqrt{x})$. (Note that there are at most $O(\sqrt{x})$ integers $|g|\le x$ that are not in G and that, for a fixed integer g_1, there at most $O(\sqrt{x})$ integers g_2 satisfying $D(g_2)=D(g_1)$.) If $d_1\ge 3$ we invoke Lemma 14 with $d=d_1$. □

In case $d|2(a,d)$, that is $d_1\le 2$, the latter result can be improved. Then $\rho(a,d)$ is a rational number and, more precisely, we have:

Lemma 16 [M-Av]. *Let $d\ge 1$. Then*

$$\rho(0,d)=\frac{1}{d\varphi(d)}\text{ and }\rho(d,2d)=\begin{cases}\rho(0,2d) & \text{if } d \text{ is odd;}\\ 3\rho(0,2d) & \text{if } d \text{ is even.}\end{cases}$$

In this case we can both improve the error term and drop the GRH assumption in Proposition 6.

Proposition 7 *We have at most $O_d(\sqrt{x})$ integers g with $|g|\le x$ such that $\rho_g(0,d)\ne\rho(0,d)$. Similarly we have at most $O_d(\sqrt{x})$ integers g with $|g|\le x$ such that $\rho_g(d,2d)\ne\rho(d,2d)$.*

Proof. It is not difficult to show that $\rho_g(0,d)=1/[K_{d,d}:\mathbb{Q}]$ and hence $\rho_g(d,2d)=1/[K_{d,d}:\mathbb{Q}]-1/[K_{2d,2d}:\mathbb{Q}]$. Using Lemma 3, we infer that there are at most finitely many squarefree integers g for which $\rho_g(0,d)\neq 1/d\varphi(d)=\rho(0,d)$ (where the equality is a consequence of Proposition 16) and that, similarly, there are at most finitely many squarefree integers g for which $\rho_g(0,d)\neq 1/d\varphi(d)-1/2d\varphi(2d)=\rho(0,2d)$ (where the equality is a consequence of Proposition 16). From this the result easily follows. □

Theorem 1 only seems to have an analog for $\rho_g(a,d)$ in case $d|a$:

Proposition 8 *If q is an odd prime dividing d_1, then $\rho_g(0,qd_1)=\rho_g(0,d_1)/q^2$ (on GRH) and $\rho(0,qd_1)=\rho(0,d_1)/q^2$.*

Proof. The first equality is an immediate consequence of (1) and $[K_{vqd_1,vqd_1}:\mathbb{Q}]=q^2[K_{vd_1,vd_1}:\mathbb{Q}]$ which holds by Lemma 3 for arbitrary v. The second equality is a consequence of Lemma 16. □

7 Proof of Theorem 3

The idea of the proof of Theorem 3 is to show that if $g\in G$ and $D(g)$ contains a prime divisor p with $p\equiv 1(\text{mod } k_1(d))$, $p\mid d$, then $*_g(a,d)=*(a,d)$. Lemma 14 then allows us to finish the proof. Thus, in outline, the proof is similar to that of Proposition 6 in the previous section. Note that in case $*=\rho$ we are done by Proposition 6.

Lemma 17 *Let $d\geq 2$. Suppose that $g\in G$ and that $D(g)$ has a prime divisor p with $p\equiv 1(\text{mod } d/(a,d))$ and $p\nmid d$, then $\delta_g^{(0)}(a,d)=\delta(a,d)$.*

Proof. By the definition of $\delta_g^{(0)}(a,d)$ and Lemma 3, we find that

$$\delta_g^{(0)}(a,d)=\sum_{\substack{t=1\\(1+ta,d)=1}}^{\infty}\ \sum_{\substack{n=1\\(n,d)|a}}^{\infty}\frac{\mu(n)}{\varphi([d,n]t)nt}+\sum_{\substack{t=1\\(1+ta,d)=1}}^{\infty}\ \sum_{\substack{n=1,\ (n,d)|a\\ n_{d/(d,n)}|[d,n]t}}^{\infty}\frac{\mu(n)}{\varphi([d,n]t)nt}.$$

In the first double sum we recognize $\delta(a,d)$. Let us denote the second double sum by E_3. By the remark following Lemma 3 we have $n_{d/(d,n)}=[2^{\nu_2(d/(d,n))+1},D(g)]$. Note that $n_{d/(d,n)}|[d,n]t$ iff $2|nt$ and $D(g)|[d,n]t$. Following the argument of Proposition 7 of [M-Av] and dragging along the conditions $2|nt$ and $D(g)|[d,n]t$ we obtain

$$E_3=\sum_{\alpha|(a,d)}\frac{\mu(\alpha)}{\alpha}\sum_{\substack{t=1\\(1+ta,d)=1}}^{\infty}\ \sum_{\substack{m=1,\ (m,d)=1\\ D(g)|dmt,\ 2|\alpha mt}}^{\infty}\frac{\mu(m)}{\varphi(dmt)mt}.$$

Making the substitution $mt=v$ we obtain

$$E_3=\sum_{\alpha|(a,d)}\frac{\mu(\alpha)}{\alpha}\sum_{\substack{v=1\\ D(g)|dv,\ 2|\alpha v}}^{\infty}\frac{\sum_{t|v,\ (1+ta,d)=1,\ (\frac{v}{t},d)=1}\mu(\frac{v}{t})}{\varphi(dv)v}.$$

If $p|D(g)$, $p\equiv 1(\text{mod } d/(a,d))$ and $p\nmid d$, then p divides every v occurring in the latter sum and hence, by Lemma 15, we deduce that $E_3=0$ (note that the set of integers t satisfying $(1+ta,d)=1$ is an union of arithmetic progressions of modulus $d/(a,d))$. □

`Remark`. This lemma when combined with Theorem 1 shows, on GRH, that if $g\in G$, $D(g)$ has a prime divisor p with $p\equiv 1(\bmod\ k_2(d))$ and $p\nmid d$, then $\delta_g^{(0)}(a,d)=\delta(a,d)$.

The next few results are concerned with when the equality $\delta_g(a,d)=\delta_g^{(0)}(a,d)$ holds.

Proposition 9 (GRH). *Suppose that d is odd and $(d,D(g_0))=1$. Then $\delta_g(a,d)=\delta_g^{(0)}(a,d)$.*

Proof. The condtions $(d,D(g_0))=1$ and d is odd ensure that $\gamma_g(dt_d,nt)=1$, respectively $\epsilon_3(1+ta,dt_d,nt)=1$ for all n and t (cf. the remark following Theorem 6). Now apply Theorem 6. □

Lemma 18 (GRH) *Suppose that $g\in G$ and that $D(g)$ has a prime divisor p with $p\equiv 1(\bmod\ k_1(d))$ and $p\nmid d$, then $\delta_g(a,d)=\delta_g^{(0)}(a,d)$.*

Proof. Let us first consider the case where d is odd or $8|d$. It follows from Theorem 1 that if $\delta_g(a,k_1(d))=\delta_g^{(0)}(a,k_1(d))$, then $\delta_g(a,d)=\delta_g^{(0)}(a,d)$ and thus, w.l.o.g., we may assume that $k_1(d)=d$. By (10) we have

$$\delta_g(a,d)=\delta_g^{(0)}(a,d)-\sum_{\substack{(1+ta,d)=1\\ (\frac{\delta}{1+ta})=-1}}\ \sum_{\substack{D(g)\nmid nt,\ D(g)|[d,n]t\\ \nu_2(nt)\ge\nu_2(h)+1\\ (d,n)|a}}\frac{\mu(n)}{[K_{[d,n]t,nt}:\mathbb{Q}]},$$

for some $\delta|d$. Since δ is a fundamental discriminant dividing d it follows from the reciprocity law for the Kronecker symbol that the sum over t is a sum over a certain set of arithmetic progressions modulo d. Let us consider the inner sum where t runs over one such arithmetic progression, say $t\ge 1$ and $t\equiv b(\bmod\ d)$. Setting $(d,n)=\alpha$ and $nt=v$ we obtain for the inner sum:

$$\sum_{\alpha|(a,d)}\ \sum_{\substack{D(g)\nmid v,D(g)|\frac{d}{\alpha}v\\ \nu_2(v)\ge\nu_2(h)+1}}\frac{\sum_{t\equiv b(\bmod\ d),\ (\frac{v}{t},d)=\alpha}\mu(v/t)}{[K_{\frac{d}{\alpha}v,v}:\mathbb{Q}]}.$$

Now the assumption on $D(g)$ implies, by Lemma 15, that for all v occurring in the sum the inner sum is zero. Hence we infer that $\delta_g(a,d)=\delta_g^{(0)}(a,d)$.

In case $d\equiv 4(\bmod\ 8)$ we note that $\delta_g(a,d)=\delta_g(a,2d)+\delta_g(a+d,2d)$ and $\delta_g^{(0)}(a,d)=\delta_g^{(0)}(a,2d)+\delta_g^{(0)}(a+d,2d)$. Hence it suffices to show that $\delta_g(a,2d)=\delta_g^{(0)}(a,2d)$ and $\delta_g(a+d,2d)=\delta_g^{(0)}(a+d,2d)$. Since $8|2d$ and $k_1(2d)=k_1(d)$ we are reduced to the previous case. The remaining case where $2||d$ can be dealt with similarly. □

Theorem 7 (GRH). *For almost all integers g we have $*_g(a,d)=*(a,d)$, with $*$ is δ or $\delta^{(0)}$. More precisely, there are at most $O_d(x\log^{-1/\varphi(k_2(d))}x)$ integers g with $|g|\le x$ such that $\delta_g^{(0)}(a,d)\ne\delta(a,d)$. There are at most $O_d(x\log^{-1/\varphi(k_1(d))}x)$ integers g with $|g|\le x$ such that $\delta_g(a,d)\ne\delta(a,d)$.*

Proof. This follows from the remark following Lemma 17, Lemma 18 and Lemma 14 (cf. the proof of Proposition 6). $\square$

Remark. For various choices of a and d, the terms $\varphi(k_2(d))$ and $\varphi(k_1(d))$ can be sometimes replaced by smaller numbers, resulting in a smaller error term.

Proof of Theorem 3. Combine Theorem 7 and Proposition 6. $\square$

8 The proof of Theorem 4

For any Dirichlet character χ, we let h_χ denote the Dirichlet convolution of χ and μ. For properties of h_χ the reader is referred to [M-I].

Lemma 19 *Let α, β, d, d_1 and r be arbitrary positive integers with $(\alpha,\beta)=1$. Write $v=v_1v_d$ with $v_1=v/(v,d^\infty)$ and $v_d=(v,d^\infty)$. Then*

$$\sum_{\substack{t=1\\ t\equiv\alpha(\mathrm{mod}\ \beta)}}^{\infty}\sum_{\substack{n=1\\ (n,d)=1}}^{\infty}\frac{\mu(n)}{[K_{d_1rnt,rnt}:\mathbb{Q}]}=\frac{1}{\varphi(\beta)}\sum_{\chi\in G_\beta}\overline{\chi(\alpha)}\sum_{v=1}^{\infty}\frac{\chi(v_d)h_\chi(v_1)}{[K_{d_1rv,rv}:\mathbb{Q}]}.$$

Proof. We have

$$\begin{aligned}
\varphi(\beta)\sum_{\substack{t=1\\ t\equiv\alpha(\mathrm{mod}\ \beta)}}^{\infty}\sum_{\substack{n=1\\ (n,d)=1}}^{\infty}\frac{\mu(n)}{[K_{d_1rnt,rnt}:\mathbb{Q}]} &= \sum_{v=1}^{\infty}\frac{\sum_{t\equiv\alpha(\mathrm{mod}\ \beta),\ t|v,\ (v/t,d)=1}\mu(v/t)}{[K_{d_1vr,vr}:\mathbb{Q}]}\\
&= \sum_{\chi\in G_\beta}\overline{\chi(\alpha)}\sum_{v=1}^{\infty}\frac{\sum_{t|v,\ (v/t,d)=1}\chi(t)\mu(v/t)}{[K_{d_1rv,rv}:\mathbb{Q}]}\\
&= \sum_{\chi\in G_\beta}\overline{\chi(\alpha)}\sum_{\delta|d^\infty}\chi(\delta)\sum_{\substack{v=1\\ (v,d)=1}}^{\infty}\frac{h_\chi(v)}{[K_{d_1\delta rv,\delta rv}:\mathbb{Q}]}\\
&= \sum_{\chi\in G_\beta}\overline{\chi(\alpha)}\sum_{v=1}^{\infty}\frac{\chi(v_d)h_\chi(v_1)}{[K_{d_1rv,rv}:\mathbb{Q}]}.
\end{aligned}$$

This concludes the proof. $\square$

Note that the inner three sums in the next result are finite sums. The complicated nature of the result suggests that the arithmetic function $h_\chi(v)$ might not be the proper one to work with. However, in the analysis of $d=3,4$ [M-I] and d is prime [M-II], this function turned out to be of crucial importance.

Theorem 8 *Let a and $d\geq 1$ be arbitrary integers. Then*

$$\delta_g^{(0)}(a,d)=\sum_{\substack{0<t_1\leq d\\ (1+t_1a,d)=1}}\sum_{\chi\in G_{\frac{d}{(t_1,d)}}}\frac{\overline{\chi(\frac{t_1}{(t_1,d)})}}{\varphi(\frac{d}{(t_1,d)})}\sum_{\alpha|(a,d)}\mu(\alpha)\sum_{v=1}^{\infty}\frac{\chi(v_d)h_\chi(v_1)}{[K_{d(t_1,d)v,d(t_1,d)\alpha v}:\mathbb{Q}]}.$$

Proof. Note that

$$\begin{aligned}\sum_{\substack{n=1\\(n,d)|a}}^{\infty}\frac{\mu(n)}{[K_{[d,n]t,nt}:\mathbb{Q}]} &= \sum_{\alpha|(a,d)}\sum_{\substack{n=1\\(n,d)=\alpha}}^{\infty}\frac{\mu(n)}{[K_{dnt/(d,n),nt}:\mathbb{Q}]}\\ &= \sum_{\alpha|(a,d)}\mu(\alpha)\sum_{\substack{n=1\\(n,d)=1}}^{\infty}\frac{\mu(n)}{[K_{dnt,\alpha nt}:\mathbb{Q}]},\end{aligned}$$

cf. the proof of Part 2 of Theorem 1 [M-Av]. On invoking Lemma 19 the proof is then easily completed. □

Lemma 20 *We have $\delta_g^{(0)}(a,d)=\sum_{\chi\in G_d}c_\chi A_\chi$, where $c_\chi\in\mathbb{Q}(\zeta_{o_\chi})$ can be explicitly computed.*

The proof of this result can be easily inferred from the next lemma in combination with Theorem 8 and the observation that if a Dirichlet character χ mod d is the lift of a Dirichlet character χ' mod d_1, then $A_\chi/A_{\chi'}$ is rational.

Lemma 21 *Let v_1 and v_d be as in Lemma* 19. *We have*

$$\sum_{v=1}^{\infty}\frac{\chi(v_d)h_\chi(v_1)}{[K_{d_1rv,rv}:\mathbb{Q}]}=c_\chi A_\chi,$$

where $c_\chi\in\mathbb{Q}(\zeta_{o_\chi})$ can be explicitly computed.

Proof. Using Lemmas 10 and 11 of [M-I] it is easily inferred that

$$\sum_{(r,v)=1}\frac{h_\chi(v)}{[K_{sv,v}:\mathbb{Q}]}=c'_\chi A_\chi,$$

where c'_χ can be effectively computed. The proof of the present lemma is a variation of this. □

Proof of Theorem 4.
1) Follows from Lemma 20 and Theorem 1.
2) (Sketch). The same trick as in the proof of Lemma 18 can be applied to reduce to the case where d is odd or $8|d$. In these cases comparatively easy explicit formulae for $\delta_g(a,d)$ can be written down. Each of them can be expressed in terms of a function very closely related to $h_\chi(v)$, this being possible due to the fact that the t arising in these formulae run over an union of arithmetic progressions modulo a divisor of $4d$. We then get a finite combination of sums not unlike those in Lemma 21 that, like the sums in Lemma 21 can be expressed in terms of A_χ. In case $8|d$ it suffices by (11) and Theorem 1 to only consider the case $g>0$. As the amount of work involved is quite considerable and no new ideas are involved, I suppress the details here.
3) This is Theorem 5 of [M-I]. □

9 Equidistribution results

Let $N_g(a_1,d_1;a_2,d_2)(x)$ denote the number of primes $p\le x$ with $p\equiv a_1(\mathrm{mod}\ d_1)$ such that $\nu_p(g)=0$ and the order of g modulo p is congruent to $a_2(\mathrm{mod}\ d_2)$. Although $N_g(a,d)(x)$ does not seem to have equidistribution properties, results in this direction can be proved for $N_g(a_1,d_1;a_2,d_2)(x)$. In [M-II] it is established that, on GRH, $N_g(a_1,d_1;a_2,d_2)$ has a density $\delta_g(a_1,d_1;a_2,d_2)$.

Recall that $k(d)$ denotes the squarefree kernel of d. The result below generalizes results in [M-I] and [M-II].

Theorem 9 (GRH). *Suppose that* $(a,d)=(b,d)=1$.
1) *If d is odd, then* $\rho_g(1,k(d);a,d)=\rho_g(1,k(d);b,d)$.
2) *If d is even, then* $\rho_g(1,2k(d);a,d)=\rho_g(1,2k(d);b,d)$.

Proof. A variation of Theorem 6 yields that

$$\rho_g(1,k(d);a,d)=\sum_{k(d)|t}\sum_{\substack{n=1\\(n,d)=1}}^{\infty}\frac{\mu(n)\epsilon_4(a,n,t)}{[K_{[d,n]t,nt}:\mathbb{Q}]},\tag{14}$$

where $\epsilon_4(a,n,t)=c_g(1+ta,dt,nt)=(1+\epsilon_3(1+ta,dt_d,nt)(\frac{\gamma_g(dt_d,nt)}{1+ta}))/2\in\{0,1\}$.
1) The assumption that d be odd, implies that dt_d is odd and hence the exceptional case never arises and we have $\epsilon_3(1+ta,dt_d,nt)=1$ for the values of n and t we sum over. Using that all quadratic subfields of $\mathbb{Q}(\zeta_{dt_d})$ are contained in $\mathbb{Q}(\zeta_{k(d)})$ and since $k(d)|t$, it follows that $\sigma_{1+ta}(\zeta_{k(d)})=\zeta_{k(d)}$ and so certainly $\sigma_{1+ta}(\sqrt{\gamma_g(dt_d,nt)})=\sqrt{\gamma_g(dt_d,nt)}$ and hence $(\gamma_g(dt_d,nt)/1+ta)=1$ (alternatively one can use quadratic reciprocity to infer this). It follows that $\epsilon_4(a,n,t)=1$ for all the values of n and t we sum over. Similarly we have $\epsilon_4(b,n,t)=1$ and it thus follows that

$$\rho_g(1,k(d);a,d)=\rho_g(1,k(d);b,d)=\sum_{k(d)|t}\sum_{\substack{n=1\\(n,d)=1}}^{\infty}\frac{\mu(n)}{[K_{[d,n]t,nt}:\mathbb{Q}]}.$$

2) In this case the analog of (14) holds, but with the condition $k(d)|t$ replaced by $2k(d)|t$. Now the exceptional case may arise. In that case we have $\epsilon_3(1+ta,dt_d,nt)=(-1)^{ta/t_d}=-1$ and, similarly, $\epsilon_3(1+tb,dt_d,nt)=-1$. Using that all quadratic subfields of $\mathbb{Q}(\zeta_{dt_d})$ are contained in $\mathbb{Q}(\zeta_{4k(d)})$ and since $4k(d)|t(a-b)$ (since $2k(d)|t$ and $a-b$ is even), it follows that $\sigma_{1+ta}(\zeta_{4k(d)})=\sigma_{1+tb}(\zeta_{4k(d)})$ and so certainly $\sigma_{1+ta}(\sqrt{\gamma_g(dt_d,nt)})$ is equal to $\sigma_{1+tb}(\sqrt{\gamma_g(dt_d,nt)})$ and hence $(\gamma_g(dt_d,nt)/1+ta)=(\gamma_g(dt_d,nt)/1+tb)$. It follows that $\epsilon_4(a,n,t)=\epsilon_4(b,n,t)$ for all the values of n and t we sum over in (14) and hence $\rho_g(1,2k(d);a,d)=\rho_g(1,2k(d);b,d)$. □

Acknowledgement. This is the final paper concluding a rather extensive project. I like to thank Dr. Paul Tegelaar for his friendship, continuous support, interest, computer assistance and proofreading. The project was begun whilst the author was at the University of Amsterdam, he likes to thank Prof. Eric Opdam for the opportunity to work for several years in his PIONIER-group (funded by NWO).

References

[CM] K. Chinen and L. Murata, On a distribution property of the residual order of $a$mod p), I, II *J. Number Theory* **105** (2004), 60–81, 82-100.

[GP] A.J. Granville and P.A.B. Pleasants, Aurefeuillian factorization revisited, preprint submitted to Mathematics of Computation.

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

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

[M-Fi] P. Moree, Convoluted convolved Fibonacci numbers, *J. Integer Seq.* **7** (2004), Article 04.2.2, 16 pp. (electronic)

[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-I] P. Moree, On the distribution of the order and index of $g(\text{mod } p)$ over residue classes I, arXiv:math.NT/0211259, *J. Number Theory*, to appear.

[M-II] P. Moree, On the distribution of the order and index of $g(\text{mod } p)$ over residue classes II, arXiv:math.NT/0404339, submitted.

[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, On Hooley's theorem with weights, Number theory, II (Rome, 1995), *Rend. Sem. Mat. Univ. Politec. Torino* **53** (1995), 375–388.

[Wa] S.S. Wagstaff, jr., Pseudoprimes and a generalization of Artin's conjecture, *Acta Arith.* **41** (1982), 141–150.

[Wi1] K. Wiertelak, On the density of some sets of primes, IV, *Acta Arith.* **43** (1984), 177–190.

[Wi2] K. Wiertelak, On the density of some sets of primes p, for which $n|\text{ord}_p(a)$, *Funct. Approx. Comment. Math.* **28** (2000), 237–241.