Primes in arithmetic progressions having a prescribed primitive root

Pieter Moree

Abstract

Let $g \in \mathbb{Z}$ be not -1 or a square. Let $\mathcal{P}_g$ denote the set of primes p such that g is a primitive root mod p. Let $f \geq 1$ and $1 \leq a \leq f$, $(a, f) = 1$. Under the Generalized Riemann Hypothesis (GRH) it can be shown that the set of primes $p \in \mathcal{P}_g$ with $p \equiv a(\text{mod } f)$, has a natural density. In this note this density is explicitly evaluated.

1 Introduction

Let $g \in \mathbb{Z}$ be not -1 or a square. Let $\mathcal{P}_g$ denote the set of primes p such that g is a primitve root mod p. It was conjectured by Emil Artin in 1927 that $\mathcal{P}_g$ is infinite. There is no integer g for which this has been proved, however, Heath-Brown [1] in a classical paper established a result which implies, for example, that there are at most two primes q for which $\mathcal{P}_q$ is finite. In 1967 Hooley [2] established Artin's conjecture under the assumption of the Generalized Riemann Hypothesis (GRH). Moreover, he showed that under that assumption the set $\mathcal{P}_g$ has a natural density, which he evaluated (his result is Theorem 2 below with $a = 1$ and $f = 1$). It turns out that this density is a rational number times the Artin constant A, with

$$A = \prod_p \left(1 - \frac{1}{p(p-1)}\right) \approx .37395581.$$

In connection with his study of Euclidian number fields, Lenstra [3] considered the distribution over arithmetic progressions of the primes in $\mathcal{P}_g$. Let $\mathcal{P}_{a,f,g}$ denote the set of primes such that g is a primitive root mod p and $p \equiv a(\text{mod } f)$. From Lenstra's work it follows that, under GRH, $\mathcal{P}_{a,f,g}$ has a natural density.

Theorem 1 [3]. *Put $\zeta_m = e^{2\pi i/m}$. Let $f \geq 1$ and $1 \leq a \leq f$, $(a, f) = 1$. Let σ_a be the automorphism of $\mathbb{Q}(\zeta_f)$ determined by $\sigma_a(\zeta_f) = \zeta_f^a$. Let $c_a(n)$ be 1 if the restriction of σ_a to the field $\mathbb{Q}(\zeta_f) \cap \mathbb{Q}(\zeta_n, g^{1/n})$ is the identity and $c_a(n) = 0$ otherwise. Put*

$$\delta(a, f, g) = \sum_{n=1}^{\infty} \frac{\mu(n)c_a(n)}{[\mathbb{Q}(\zeta_f, \zeta_n, g^{1/n}) : \mathbb{Q}]}.$$

Then, assuming GRH, we have

$$\pi_g(x;f,a)=\delta(a,f,g)\frac{x}{\log x}+O\left(\frac{x\log\log x}{\log^2 x}\right),$$

where $\pi_g(x;f,a)$ *denotes the number of primes* $p\le x$ *that are in* $\mathcal{P}_{a,f,g}$.

In the light of the apparent arithmetical complexity of Lenstra's formula, the following relatively simple expression for $\delta(a,f,g)$ may come as a bit of a surprise.

Theorem 2 *Let* $g\in\mathbb{Z}$ *be not* -1 *or a square. Let* $h\ge 1$ *be the largest integer such that* g *is an* h*th power. Let* Δ *denote the discriminant of the quadratic field* $\mathbb{Q}(\sqrt{g})$. *Let* $f\ge 1$ *and* $1\le a\le f,\ (a,f)=1$. *Let* $b=\Delta/(f,\Delta)$. *Put*

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

if $(a-1,f,h)=1$ *and* $A(a,f,h)=0$ *otherwise. Then*

$$\delta(a,f,g)=\frac{A(a,f,h)}{\varphi(f)}\left(1+(\frac{\Delta}{a})(\frac{a}{|b|})\frac{\mu(2|b|)}{\prod_{p|b,\ p|h}(p-2)\prod_{p|b,\ p\nmid h}(p^2-p-1)}\right).$$

Here (Δ/a) *denotes the Kronecker symbol and* $(a/|b|)$ *the Jacobi symbol.*

In case b is even, the Jacobi symbol (a/b) is not defined, then however $\mu(2b)=0$ and the term involving $\mu(2b)$ is taken to be zero. Write $g=g_1g_2^2$, with g_1 squarefree. Then $\Delta=g_1$ if $g_1\equiv 1(\mathrm{mod}\ 4)$ and $\Delta=4g_1$ otherwise. We see that b is odd if and only if $g_1\equiv 1(\mathrm{mod}\ 4)$ or $g_1\equiv 2(\mathrm{mod}\ 4)$ and $8|f$ or $g_1\equiv 3(\mathrm{mod}\ 4)$ and $4|f$. Theorem 2 can be reformulated, using properties of the Kronecker symbol (see Section 2), in terms of g_1.

Theorem 3 *Let* a,f,g,h *and* $A(a,f,h)$ *be as in Theorem 2. Let* $\tilde{g}_1$ *denote the odd part of* g_1. *Let* $\beta=g_1/(g_1,f)$. *We have*

$$\delta(a,f.g)=\frac{A(a,f,h)}{\varphi(f)}\left(1-(\frac{a}{(f,g_1)})\frac{(-1)^{\frac{\tilde{g}_1-1}{2}\frac{a-1}{2}}\mu(|\beta|)}{\prod_{p|\beta,\ p|h}(p-2)\prod_{p|\beta,\ p\nmid h}(p^2-p-1)}\right)$$

in case $g_1\equiv 1(\mathrm{mod}\ 4)$ *or* $g_1\equiv 2(\mathrm{mod}\ 4)$ *and* $8|f$ *or* $g_1\equiv 3(\mathrm{mod}\ 4)$ *and* $4|f$ *and*

$$\delta(a,f,g)=\frac{A(a,f,h)}{\varphi(f)},$$

otherwise. Here $(./.)$ *denotes the Jacobi symbol with the stipulation that* $(a/2)=(-1)^{(a^2-1)/8}$.

From Theorem 2 various known results can be rather easily deduced. That will be the subject of Section 5. The remaining sections are devoted to proving Theorem 2.

The author thanks F. Lemmermeyer and P. Stevenhagen for some helpful remarks.

2 Some facts from algebraic number theory

Although Theorem 1 suggests differently, the problem of evaluating $\delta(a,f,g)$ really only involves cyclotomic fields, quadratic subfields and their composita. In this section some facts concerning these fields relevant for the proof of Theorem 2 are discussed. We start by recalling some properties of the Kronecker symbol, a rarely covered topic in books on number theory.

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

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

with Jacobi symbols in the right.

The following lemma allows one to determine all quadratic subfields of a given cyclotomic field (for a proof see e.g. [9, p. 163]).

Lemma 1 *Let $\mathbb{Q}(\sqrt{d})$ be a quadratic field of determinant Δ_d. Then the smallest cyclotomic field containing $\mathbb{Q}(\sqrt{d})$ is $\mathbb{Q}(\zeta_{|\Delta_d|})$.*

Consider the cyclotomic field $\mathbb{Q}(\zeta_f)$. There are $\varphi(f)$ distinct automorphisms given by $\sigma_a(\zeta_f) = \zeta_f^a$, with $1 \leq a \leq f$ 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 determinant Δ_d. We have $\sigma_a|_{\mathbb{Q}(\sqrt{d})} =$id if and only if $(\Delta_d/a) = 1$, where $(./.)$ denotes the Kronecker symbol.*

Proof. Notice that, by Lemma 1, we can restrict to the case where $f = |\Delta_d|$. Define χ by $\chi(a) = \sigma_a(\sqrt{d})/\sqrt{d}$, $1 \leq a \leq |\Delta_d|$, $(a, \Delta_d) = 1$. Then χ is the uniqe non-trivial character of the character group of $\mathbb{Q}(\sqrt{d})$. As is well-known (see e.g. [7, p. 437]) the primitive character induced by this is (Δ_d/a). Using Lemma 1, we see that χ is a primitive character mod $|\Delta_d|$. Thus $\chi(a) = (\Delta_d/a)$. Now $\sigma_a|_{\mathbb{Q}(\sqrt{d})} =$id if and only if $\chi(a) = (\Delta_d/a) = 1$. $\square$

Remark. It is also possible to prove Lemma 2 using quadratic reciprocity and properties of Gauss sums.

The next result can be proved by a trivial generalization of an argument given by Hooley [2, pp. 213-214].

Lemma 3 *Let $g \in G$ and let h be the largest positive integer such that g is a pure hth power. Suppose that $k|r$ and k is squarefree. Put $k_1 = k/(k,h)$ and $n(k,r) = [\mathbb{Q}(\zeta_r, g^{1/k}) : \mathbb{Q}]$. Then* *i) if k is odd, $n(k,r)=k_1\varphi(r)$;*

ii) if k is even and $\Delta\nmid r$, $n(k,r)=k_1\varphi(r)$;

iii) if k is even and $\Delta|r$, $n(k,r)=k_1\varphi(r)/2$.

The next lemma together with Lemma 2 allows one to compute $c_a(n)$.

Lemma 4 *Let $g\in\mathbb{Z}$ be not -1 or a square. Let Δ denote the discriminant of $\mathbb{Q}(\sqrt{g})$. Let $n\ge 1$ be squarefree and $f\ge 1$ be arbitrary. Put $b=\Delta/(f,\Delta)$. Then*

$$\mathbb{Q}(\zeta_f)\cap\mathbb{Q}(\zeta_n,g^{1/n})=\mathbb{Q}(\zeta_{(f,n)},\sqrt{(-1)^{(b-1)/2}(f,\Delta)})$$

if n is even, $\Delta\nmid n$ and $\Delta|\mathrm{lcm}(f,n)$ and

$$\mathbb{Q}(\zeta_f)\cap\mathbb{Q}(\zeta_n,g^{1/n})=\mathbb{Q}(\zeta_{(f,n)})$$

otherwise.

Proof. On noting that $\varphi((f,n))\varphi(\mathrm{lcm}(f,n))=\varphi(f)\varphi(n)$, it easily follows, using Lemma 3, that

$$[\mathbb{Q}(\zeta_f)\cap\mathbb{Q}(\zeta_n,g^{1/n}):\mathbb{Q}(\zeta_{(f,n)})]=2 \tag{2}$$

if n is even, $\Delta\nmid n$ and $\Delta|\mathrm{lcm}(f,n)$ and $\mathbb{Q}(\zeta_f)\cap\mathbb{Q}(\zeta_n,g^{1/n})=\mathbb{Q}(\zeta_{(f,n)})$ otherwise. Thus we may assume that n is even, $\Delta\nmid n$ and $\Delta|\mathrm{lcm}(f,n)$. Notice that this implies that b is odd. Put $\gamma=(-1)^{(b-1)/2}(f,\Delta)$. We now distinguish cases according to the residue mod 4 of the odd part of Δ, respectively the odd part of (f,Δ). In each case we check, using Lemma 1, that $\sqrt{\gamma}\not\in\mathbb{Q}(\zeta_{(f,n)})$, $\sqrt{\gamma}\in\mathbb{Q}(\zeta_f)$ and $\sqrt{\Delta/\gamma}\in\mathbb{Q}(\zeta_n)$. These inclusion relations together with (2) yield the result.

3 Euler products

In this section we prove some results that will help us to write down the Euler product of the sums encountered in the proof of the main result (Theorem 2).

Proposition 1 *Let $f,h\ge 1$ be integers. Then the function $w:\mathbb{N}\to\mathbb{N}$ defined by*

$$w(k)=\frac{k\varphi(\mathrm{lcm}(k,f))}{(k,h)\varphi(f)}$$

is multiplicative. Furthermore,

i) if $p\nmid h$ and $p\nmid f$, then $w(p)=p(p-1)$

ii) if $p\nmid h$ and $p|f$, then $w(p)=p$

iii) if $p|h$ and $p\nmid f$, then $w(p)=p-1$

iv) if $p|h$ and $p|f$, then $w(p)=1$

v) if h is odd, then $w(2)=2$.

This will help us to prove the following lemma.

Lemma 5 *Let $f, h \geq 1$ be integers with $1 \leq a \leq f$, $(a,f)=1$ and h odd. Let Δ be a discriminant of a quadratic number field. Let $b = \Delta/(f,\Delta)$. Put*

$$S(b) = \sum_{\substack{n=1,\ \Delta|\mathrm{lcm}(n,f) \\ a\equiv 1 (\mathrm{mod}\ (f,n))}}^{\infty} \frac{\mu(n)}{w(n)}.$$

Let $S_2(b)$ denote the same sum as $S(b)$ but with the restriction that $2|n$. Then $S(b)=0$ if b is even and

$$S(b) = \frac{\mu(b)A(a,f,h)}{\prod_{p|b}(w(p)-1)}$$

otherwise. Furthermore, $S_2(b) = -S(b)$.

Proof. If b is even, then the summation in $S(b)$ runs over non squarefree n only and hence $S(b)=0$. Next assume that b is odd. We have

$$\begin{aligned} S(b) &= \sum_{\substack{n=1,\ b|n/(f,n) \\ a\equiv 1 (\mathrm{mod}\ (f,n))}}^{\infty} \frac{\mu(n)}{w(n)} = \sum_{d|(a-1,f)} \sum_{\substack{n=1,\ (f,n)=d \\ b|n/d}}^{\infty} \frac{\mu(n)}{w(n)} \\ &= \sum_{d|(a-1,f)} \frac{\mu(d)}{w(d)} \sum_{\substack{n=1,\ (f,n)=1 \\ b|n}}^{\infty} \frac{\mu(n)}{w(n)} = \frac{\mu(|b|)}{w(|b|)} \sum_{d|(a-1,f)} \frac{\mu(d)}{w(d)} \sum_{\substack{n=1,\ (f,nb)=1 \\ (b,n)=1}}^{\infty} \frac{\mu(n)}{w(n)}. \end{aligned}$$

Now by assumption Δ is a discriminant and b is odd. This implies that $(f,b)=1$ and b is squarefree. Thus

$$\begin{aligned} S(b) &= \frac{\mu(|b|)}{w(|b|)} \prod_{p|(a-1,f)} (1-\frac{1}{w(p)}) \prod_{p\nmid fb} (1-\frac{1}{w(p)}) \\ &= \frac{\mu(|b|)}{w(|b|)} \prod_{p|(a-1,f)} (1-\frac{1}{w(p)}) \prod_{p\nmid f} (1-\frac{1}{w(p)}) \prod_{p|b} (1-\frac{1}{w(p)})^{-1} \\ &= \frac{\mu(|b|)A(a,f,h)}{\prod_{p|b}(w(p)-1)}, \end{aligned}$$

where we used that $w(p) > 1$ for $p|b$ and

$$\prod_{p|(a-1,f)} (1-\frac{1}{w(p)}) \prod_{p\nmid f} (1-\frac{1}{w(p)}) = A(a,f,h),$$

an identity immediately obtained on invoking Proposition 1.

The latter part of the assertion follows easily on using that $w(2)=2$. □

4 Proof of the main result

Proof of Theorem 2.
Let γ be as in the proof of Lemma 4. Suppose that b is odd. Note that the discriminant of $\mathbb{Q}(\sqrt{\gamma})$ equals γ. On using (1), it is seen that the Kronecker symbol (γ/a) equals $(\Delta/a)(a/|b|)$.

i) The case b is odd and $(\Delta/a)(a/|b|) = 1$. Using Lemma 4, Lemma 2 and the observation above, we find that $c_a(n) = 1$ in case $a \equiv 1(\text{mod } (f, n))$ and $c_a(n) = 0$ otherwise. This together with Theorem 1 and Lemma 3 implies that

$$\begin{aligned} \varphi(f)\delta(a, f, g) &= \sum_{\substack{n=1 \\ 2\nmid n}}^{\infty} \frac{\mu(n)}{w(n)} + \sum_{\substack{n=1,\ 2|n \\ \Delta\nmid \mathrm{lcm}(n,f)}}^{\infty} \frac{\mu(n)}{w(n)} + 2 \sum_{\substack{n=1,\ 2|n \\ \Delta|\mathrm{lcm}(n,f)}}^{\infty} \frac{\mu(n)}{w(n)}. \\ &= \sum_{n=1}^{\infty} \frac{\mu(n)}{w(n)} + \sum_{\substack{n=1,\ 2|n \\ \Delta|\mathrm{lcm}(n,f)}}^{\infty} \frac{\mu(n)}{w(n)} = \mathrm{I}_1 + S_2(b), \end{aligned} \tag{3}$$

where furthermore in each sum we restrict to those integers n such that $a \equiv 1(\text{mod } (f, n))$. Now, on using Proposition 1,

$$\begin{aligned} \mathrm{I}_1 &= \sum_{d|(a-1,f)} \sum_{(f,n)=d} \frac{\mu(n)}{w(n)} = \sum_{d|(a-1,f)} \frac{\mu(d)}{w(d)} \sum_{(f,n)=1} \frac{\mu(n)}{w(n)} \\ &= \prod_{p|(a-1,f)} (1 - \frac{1}{w(p)}) \prod_{p\nmid f} (1 - \frac{1}{w(p)}) = A(a, f, h). \end{aligned}$$

The result follows from (3) on invoking Lemma 5 and Proposition 1.

ii) The case b is odd and $(\Delta/a)(a/|b|) = -1$. Using Lemma 4, Lemma 2, the observation in the beginning of this proof and (3), we find

$$\varphi(f)\delta(a, f, g) = \mathrm{I}_1 + S_2(b) - 2 \sum_{\substack{2|n,\ \Delta\nmid n \\ \Delta|\mathrm{lcm}(f,n) \\ a\equiv 1(\text{mod } (f,n))}} \frac{\mu(n)}{w(n)}.$$

Now

$$\sum_{\substack{2|n,\ \Delta|\mathrm{lcm}(f,n) \\ a\equiv 1(\text{mod } (f,n))}} \frac{\mu(n)}{w(n)} = \sum_{\substack{2|n,\ \Delta\nmid n \\ \Delta|\mathrm{lcm}(f,n) \\ a\equiv 1(\text{mod } (f,n))}} \frac{\mu(n)}{w(n)} + \sum_{\substack{2|n,\ \Delta|n \\ a\equiv 1(\text{mod } (f,n))}} \frac{\mu(n)}{w(n)}.$$

In case $\Delta \equiv 0(\text{mod } 4)$, the latter sum is obviously zero. In case $\Delta \equiv 1(\text{mod } 4)$, a necessary condition for the latter sum to be non-zero is that $a \equiv 1(\text{mod } (f, 2\Delta))$. For such a, we have however, $(\Delta/a)(a/b) = (a/(f, \Delta)) = 1$. It thus follows that $\varphi(f)\delta(a, f, g) = \mathrm{I}_1 - S_2(b)$.

iii) The case b is even. As in the case where b is odd, we either have that $\varphi(f)\delta(a, f, g) = \mathrm{I}_1 + S_2(b)$ or $\varphi(f)\delta(a, f, g) = \mathrm{I}_1 - S_2(b)$. By Lemma 5 it then follows that $\varphi(f)\delta(a, f, g) = \mathrm{I}_1$. $\square$

5 Applications

Setting $a = 1$ and $f = 1$ in Theorem 2 we obtain Hooley's theorem [2]. Setting $a = 1$ we obtain Theorem 4 of [5]. Notice that of all the progressions mod f, the progression $1(\text{mod } f)$ is the easiest to deal with, since trivially $c_1(n) = 1$ for every n.

Rodier [8], in connection with a coding theoretical problem, conjectured that the density of the primes in $\mathcal{P}_2$ such that $p \equiv -1, 3$ or $19(\text{mod } 28)$ is $A/4$. From Theorem 2 it follows however that, under GRH, this density is $21A/82$ (cf. [4]).

Lenstra [3, Theorem 8.3] gave a sketch of a proof of the following result.

Theorem 4 *Let $g \in \mathbb{Z}$ be not -1 or a square and h be the largest integer such that g is an hth power. Then $\delta(a, f, g) = 0$ if and only if one of the following holds*

i) $(a - 1, f, h) > 1$;

ii) $\Delta | f$ *and* $(\frac{\Delta}{a}) = 1$ *(Kronecker symbol);*

iii) $\Delta | 3f$, $3 | \Delta$, $3 | h$ *and* $(\frac{-\Delta/3}{a}) = -1$.

This result very easily follows from Theorem 2. We leave it to the reader to show that if $\delta(a, f, g) = 0$, then actually $\mathcal{P}_g$ is finite.

If S is any set of integers, denote by $S(x)$ the number of integers in S not exceeding x. For given integers a and f, denote by $S(x; f, a)$ the number of integers in S not exceeding x that are congruent to a modulo f. We say that S is weakly uniformly distributed mod f (or WUD mod f for short) if $S(x) \to \infty$ $(x \to \infty)$ and for every a coprime to f,

$$S(x; f, a) \sim \frac{S(x)}{\varphi(d)},$$

where $\varphi(d)$ denotes Euler's totient. The progressions $a(\text{mod } f)$ such that the latter asymptotic equivalence holds and $S(x) \to \infty$ $(x \to \infty)$ are said to get their fair share of primes from S. Thus S is weakly uniformly distributed mod f if and only if all the progressions mod f get their fair share of primes from S. Narkiewicz [6] has written a nice survey on the state of knowledge regarding the (weak) uniform distribution of many important arithmetical sequences. Let D_g denote the set of natural numbers f such that $\mathcal{P}_g$ is weakly uniformly distributed modulo f.

Theorem 5 (GRH). *Let $g \in \mathbb{Z}$ be not -1 or a square and let h the largest integer such that g is a pure hth power. Write $g = g_1 g_2^2$ with g_1 squarefree. Assume that not both $g_1 = 21$ and $(h, 21) = 7$, then D_g, the set of natural numbers f such that the set of primes p such that g is a primitive root mod p is weakly uniformly distributed mod d, equals*

i) $\{2^n : n \geq 0\}$ *if* $g_1 \equiv 1(\text{mod } 4)$;

ii) $\{1, 2, 4\}$ *if* $g_1 \equiv 2(\text{mod } 4)$;

iii) $\{1,2\}$ *if* $g_1 \equiv 3(\text{mod } 4)$.

In the remaining case $g_1 = 21$ *and* $(h, 21) = 7$, *we have* $D_g = \{2^n 3^m : n,\ m \geq 0\}$.

Using only a formula for $\delta(1, f, g)$ and Theorem 1 in some special cases, this result was first deduced in [5]. Here a shorter proof, using the full force of Theorem 3, is given.

Proof of Theorem 5. Put $S_f := \{A(a, f, h) \mid 1 \leq a \leq f,\ (a, f) = 1\}$. Put

$$\chi_{g,f}(a) = (-1)^{\frac{\tilde{g}_1 - 1}{2}\frac{a-1}{2}}(\frac{a}{(f, g_1)}).$$

Let us first consider the case where $f = 2^m$ for some $m \geq 0$. In case $g_1 \equiv 1(\text{mod } 4)$, $\chi_{g,2^m}$ equals the identity, in case $g_1 \equiv 2(\text{mod } 4)$ and $m \geq 3$, $\chi_{g,2^m}$ is not equal to the identity and similarly for $g_1 \equiv 3(\text{mod } 4)$ and $m \geq 2$. Notice that $|S_{2^m}| = 1$. It follows that if $g_1 \equiv 1(\text{mod } 4)$ and $m \geq 0$, then $\mathcal{P}_g$ is WUD mod 2^m. Similarly if $g_1 \equiv 2(\text{mod } 4)$ and $m \leq 2$, or $g_1 \equiv 3(\text{mod } 4)$ and $m \leq 1$. For the other pairs $(g, 2^m)$, the image of $\delta(., f, g)$ has cardinality two and so $\mathcal{P}_g$ is not WUD mod 2^m.

It remains to deal with the case where f is odd. First let us consider the case where $f = q$ with q an odd prime. In case β is even,

$$\varphi(f)\delta(1, f, g) = A(1, f, h) \neq A(2, f, h) = \delta(2, f, g)\varphi(f)$$

and we do not have equidistribution. Next assume that β is odd. If $q = 3$, then a short calculation shows that a necessary and sufficient condition for equidistribution to occur, is that $3|g_1$, $(3, h) = 1$, $\mu(|\beta|) = -1$, $g_1 \equiv 1(\text{mod } 4)$ and the equation $\prod_{p|\beta,\ p|h}(p-2)\prod_{p|\beta,\ p\nmid h}(p^2 - p - 1) = 5$ has a solution with β is odd. Now notice that g is solution to this if and only if $g_1 = 21$ and $(h, 21) = 7$. Call such a g exceptional. If $q \geq 5$, then $A(2, f, g) = A(3, f, g) = \cdots = A(q-1, f, g)$ and there exist $2 \leq a_1 < a_2 \leq q - 1$ with $(a_1/q) = -(a_2/q)$. Then $\delta(a_1, f, g) \neq \delta(a_2, f, g)$. From this it immediately follows that for odd f and g not exceptional, equidistribution does not occur, for if $\mathcal{P}_g$ is WUD mod f, then $\mathcal{P}_g$ must also be WUD mod δ for every divisor δ of f. It remains to show that when g is exceptional we have that $\mathcal{P}_g$ is WUD mod $2^m 3^n$, with $m \geq 0$ and $n \geq 1$ arbitrary. This follows easily from Theorem 2 and the calculation done in the case $f = 3$. $\square$

References

[1] D.R. Heath-Brown, Artin's conjecture for primitive roots, *Quart. J. Math. Oxford* **37** (1986), 27-38.

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

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

[4] P. Moree, On a conjecture of Rodier on primitive roots, *Abh. Math. Sem. Univ. Hamburg* **67** (1997), 165-171.

[5] P. Moree, Uniform distribution of primes having a rational prescribed primitive root, MPI-preprint 23, 1998.

[6] W. Narkiewicz, *Uniform distribution of sequences of integers in residue classes,* Lecture Notes in Math. 1087, Springer, 1984.

[7] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer, 2nd edition, 1989.

[8] F. Rodier, Estimation asymptotique de la distance minimale du dual des codes BCH et polynômes de Dickson, *Discrete Math.* **149** (1996), 205-221.

[9] E. Weiss, *Algebraic number theory*, New York University Press, New York, 1963.

Max-Planck-Institut für Mathematik, Gottfried-Claren-Straße 26, 53225 Bonn, Germany.
(e-mail: moree@mpim-bonn.mpg.de)