Functiones et Approximatio
XXXIX.1 (2008), 133–144

ON PRIMES IN ARITHMETIC PROGRESSION HAVING A PRESCRIBED PRIMITIVE ROOT. II

Pieter Moree

To Prof. Władysław Narkiewicz
on the occasion of his 70th birthday

Abstract: Let a and f be coprime positive integers. Let g be an integer. Under the Generalized Riemann Hypothesis (GRH) it follows by a result of H.W. Lenstra that the set of primes p such that $p \equiv a (\mathrm{mod}\ f)$ and g is a primitive root modulo p has a natural density. In this note this density is explicitly evaluated with an Euler product as result. This extends a classical result of Hooley (1967) on Artin's primitive root conjecture. Various application are given, for example the integers g and f such that the set of primes p such that g is a primitive root modulo p is equidistributed modulo f is determined (on GRM).
Keywords: Artin's primitive root conjecture, arithmetic progression, natural density

1. Introduction

Let $g \in \mathbb{Z}\backslash\{0\}$. 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 in case g is in $\mathcal{G}$, the set of integers not equal to -1 or a square. Clearly, if g is not in $\mathcal{G}$, then $\mathcal{P}_g$ is finite. There is no integer g for which *Artin's primitive root conjecture* (as it is usually called) has been proved. However, Heath-Brown [6] in a classical paper, basing himself on a breakthrough paper of Gupta and Murty [5], 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 [7] 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 1.2 below with $a = 1$ and $f = 1$). It turns out that this density is a rational number (depending on g) times the Artin constant A, with

$$A = \prod_p \left(1 - \frac{1}{p(p-1)}\right) = 0.37395581361920228805472805 4346\cdots$$

(Here and in the rest of the paper the notation p is used to indicate primes.)

Mathematics Subject Classification: Primary 11N69, Secondary 11N13, 11N36, 11N56, 11R45

In connection with his study of Euclidian number fields, Lenstra [8] considered the distribution over arithmetic progressions of the primes in $\mathcal{P}_g$. Let $\mathcal{P}_{a,f,g}$ denote the set of primes p such that g is a primitive root mod p and $p \equiv a (\mathrm{mod}\ f)$. From Lenstra's work it follows that, under GRH, $\mathcal{P}_{a,f,g}$ has a natural density.

Theorem 1.1. [8]. *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

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

where $\pi_g(x; f, a)$ denotes the number of primes $p \leq x$ 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 1.2. *Let $g \in \mathcal{G}$. Let $h \geq 1$ be the largest integer such that g is an hth power. Let Δ denote the discriminant of the quadratic field $\mathbb{Q}(\sqrt{g})$. Let $f \geq 1$ and $1 \leq a \leq f,\ (a,f) = 1$. Let $b = \Delta/(f,\Delta)$. Put*

$$\gamma = \begin{cases} (-1)^{\frac{b-1}{2}}(f,\Delta) & \text{if } b \text{ is odd;} \\ 1 & \text{otherwise .} \end{cases}$$

Put

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

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

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

Here $(\frac{\cdot}{\cdot})$ denotes the Kronecker symbol.

On writing $g = g_1 g_2^2$, with g_1 squarefree and the g_i integers, we see that $\Delta = g_1$ if $g_1 \equiv 1 (\mathrm{mod}\ 4)$ and $\Delta = 4g_1$ otherwise. Note 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 1.2 can be easily reformulated in terms of g_1.

Theorem 1.3. *Let a, f, g, h, γ and $A(a,f,h)$ be as in Theorem* 1.2. *Let*

$$\beta = \frac{g_1}{(g_1, f)} \text{ and } \gamma_1 = \begin{cases} (-1)^{\frac{\beta-1}{2}}(f, g_1) & \text{if } \beta \text{ is odd;} \\ 1 & \text{otherwise.} \end{cases}$$

We have

$$\delta(a,f.g)=\frac{A(a,f,h)}{\varphi(f)}\left(1-(\frac{\gamma_1}{a})\frac{\mu(|\beta|)}{\prod_{p|\beta,\ p|h}(p-2)\prod_{p|\beta,\ p\nmid h}(p^2-p-1)}\right)$$

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.

From Theorem 1.2 various known results can be rather easily deduced. That is the subject of Section 5. The remaining sections are devoted to proving Theorem 1.2.

Remark. The results in this paper were first proved in 1998 in preprint MPIM1998-57 [12]. Not much later Lenstra and Stevenhagen found a method which allows one to give a more conceptual and elegant proof of Theorem 1.2. This method allows one to directly express the density of a large class of Artin type density problems in product form, whereas the usual approach leads to a sum for the density which has to be brought in product form. For a sketch of this method see Stevenhagen [19]. It was planned to withhold the publication of the present note and rather make Theorem 1.2 part of a joint paper with Lenstra and Stevenhagen, delineating their method. Recently, however, using the theory of 'entangled radicals', cf. Lenstra [9], the Lenstra and Stevenhagen approach is being further extended and refined by de Smit and Palenstijn [3], to be published first as part of Palenstijn's PhD thesis (Leiden University, 2009). Since the method presented in this note requires a rather more modest input from algebraic number theory than the latter work in progress [3] and is quite different, I now decided to publish (an updated and polished version of) MPIM1998-57.

The proof of the main result of part I of this series, Theorem 4 of [14], depends crucially on Theorem 1.2 (see part 7 of §5 for a brief description of Theorem 4 of [14] and its proof).

2. Some facts from algebraic number theory

Although Theorem 1.1 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 1.2 are discussed. We start by recalling some properties of the Kronecker symbol, a rarely covered topic in books on number theory (but see e.g. Cohen [2, pp. 36-39]).

The Kronecker symbol $(\frac{a}{b})$ is the extension of the Jacobi symbol to $(\mathbb{Z}\backslash\{0\})^2$ obtained by setting $(\frac{a}{-1})=\mathrm{sign}(a)$ and $(\frac{a}{2})=(\frac{2}{a})$ for a odd ($(\frac{a}{2})=0$ for a even),

and extending by multiplicativity. All symbols of the form $(\frac{\cdot}{\cdot})$ in this paper will be Kronecker symbols. For two nonzero integers m and n write $m = 2^{\nu_2(m)}m_1$ and $n = 2^{\nu_2(n)}n_1$, with m_1 and n_1 odd. Then

$$\Big(\frac{n}{m}\Big) = (-1)^{((m_1-1)(n_1-1)+(\mathrm{sign}(m)-1)(\mathrm{sign}(n)-1))/4}\Big(\frac{m}{n}\Big).$$

This is the law of quadratic reciprocity formulated in terms of the Kronecker symbol. Furthermore, if D is a discriminant then (see Cohen [2, Theorem 2.2.9])

$$\Big(\frac{D}{a+kD}\Big) = \Big(\frac{D}{a}\Big). \tag{2.1}$$

The following lemma allows one to determine all quadratic subfields of a given cyclotomic field (for a proof see e.g. [20, p. 163]).

Lemma 2.1. *Let $\mathbb{Q}(\sqrt{d})$ be a quadratic field of discriminant 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 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.

Lemma 2.2. *Let $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_f)$ be a quadratic field of discriminant Δ_d. We have $\sigma_a|_{\mathbb{Q}(\sqrt{d})} = id$ if and only if $(\frac{\Delta_d}{a}) = 1$.*

Proof. Notice that, by Lemma 2.1, we can restrict to the case where $f = |\Delta_d|$. Define χ by $\chi(a) = \sigma_a(\sqrt{d})/\sqrt{d}$, $1 \le a \le |\Delta_d|$, $(a, \Delta_d) = 1$. Then χ is the unique non-trivial character of the character group of $\mathbb{Q}(\sqrt{d})$. As is well-known (see e.g. [17, p. 437]) the primitive character induced by this is $(\frac{\Delta_d}{a})$. Using Lemma 2.1, we see that χ is a primitive character mod $|\Delta_d|$. Thus $\chi(a) = (\frac{\Delta_d}{a})$. Now $\sigma_a|_{\mathbb{Q}(\sqrt{d})} = \mathrm{id}$ if and only if $\chi(a) = (\frac{\Delta_d}{a}) = 1$. ∎

Remark. It is also possible to prove Lemma 2.2 using quadratic reciprocity and properties of Gauss sums.

The next result can be proved by a trivial generalization of an argument given by Hooley [7, pp. 213-214].

Lemma 2.3. *Let $g \in \mathcal{G}$ and let h be the largest positive integer such that g is an hth power. Let Δ be the discriminant of the quadratic field $\mathbb{Q}(\sqrt{g})$. 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 $\Delta | r$, $n(k, r) = k_1\varphi(r)/2$.

Remark. Without the condition that k be squarefree, the latter lemma becomes much more complicated to state, see e.g. Moree [15, Lemma 1]. Indeed, in the general case, different definitions of h and Δ appear to be the natural ones: one writes $g = \pm g_0^h$ with $g_0 > 0$ and h as large as possible and denotes with Δ the discriminant of $\mathbb{Q}(\sqrt{g_0})$. Partly because of these different definitions it is not so straightforward to check that the general lemma implies Lemma 2.3. This is left as an exercise for the interested reader.

The next lemma together with Lemma 2.2 allows one to compute $c_a(n)$.

Lemma 2.4. *Let $g \in \mathcal{G}$. Let Δ denote the discriminant of $\mathbb{Q}(\sqrt{g})$. Let $n \geq 1$ be squarefree and $f \geq 1$ be arbitrary. Put $b = \Delta/(f,\Delta)$. Put*

$$\gamma = \begin{cases} (-1)^{\frac{b-1}{2}}(f,\Delta) & \text{if } b \text{ is odd;} \\ 1 & \text{otherwise.} \end{cases}$$

Then

$$\mathbb{Q}(\zeta_f) \cap \mathbb{Q}(\zeta_n, g^{1/n}) = \begin{cases} \mathbb{Q}(\zeta_{(f,n)}, \sqrt{\gamma}) & \text{if } n \text{ is even }, \Delta \nmid n \text{ and } \Delta | \mathrm{lcm}(f,n); \\ \mathbb{Q}(\zeta_{(f,n)}) & \text{otherwise.} \end{cases}$$

Proof. On noting that $\varphi((f,n))\varphi(\mathrm{lcm}(f,n)) = \varphi(f)\varphi(n)$, it easily follows, using Lemma 2.3, that

$$[\mathbb{Q}(\zeta_f) \cap \mathbb{Q}(\zeta_n, g^{1/n}) : \mathbb{Q}(\zeta_{(f,n)})] = 2 \tag{2.2}$$

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. It is easy to check that γ is a fundamental discriminant. Since clearly $\gamma | f$ it follows by Lemma 2.1 that $\sqrt{\gamma} \in \mathbb{Q}(\zeta_f)$. Note that $\Delta | \mathrm{lcm}(f,n)$ implies that $\frac{\Delta}{(f,\Delta)} | \frac{n}{(f,n)} | n$. From this it follows that $(f,\Delta) | (f,n)$ would imply $\Delta | n$, contradicting the assumption $\Delta \nmid n$. This contradiction shows that $\sqrt{\gamma} \notin \mathbb{Q}(\zeta_{(f,n)})$. Note that Δ/γ is a fundamental discriminant. Since $b | n$ it follows by Lemma 2.1 that $\sqrt{\Delta/\gamma} \in \mathbb{Q}(\zeta_n)$ and thus, since n is even, $\sqrt{\gamma} \in \mathbb{Q}(\zeta_n, g^{1/n})$. In summary we have that $\sqrt{\gamma} \notin \mathbb{Q}(\zeta_{(f,n)})$, $\sqrt{\gamma} \in \mathbb{Q}(\zeta_f)$ and $\sqrt{\gamma} \in \mathbb{Q}(\zeta_n, g^{1/n})$. These inclusion relations together with (2.2) 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 Theorem 1.2.

Proposition 3.1. *Let $f, h \geq 1$ 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 $w(2) = 2$.

Proof. For every multiplicative function g and arbitrary integers $a, b \geq 1$, we obviously have $g(a)g(b) = g((a,b))g(\mathrm{lcm}(a,b))$. Thus, it is enough to show that $\varphi((k,f))$ is a multiplicative function in k, which is obvious. The remaining part of the result follows on direct calculation. ■

The multiplicativity of w plays an important role in the proof of the following lemma.

Lemma 3.1. *Let $a, f, h \geq 1$ 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

$$S(b) = -\frac{\mu(2|b|)A(a,f,h)}{\prod_{p|b}(w(p)-1)}.$$

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

$$\begin{aligned} S(b) &= \frac{\mu(|b|)}{w(|b|)} \prod_{p|(a-1,f)} (1-\frac{1}{w(p)}) \prod_{p\nmid fb} (1-\frac{1}{w(p)}) \\ &= \frac{\mu(|b|)}{w(|b|)} \prod_{p|(a-1,f)} (1-\frac{1}{w(p)}) \prod_{p\nmid f} (1-\frac{1}{w(p)}) \prod_{p|b} (1-\frac{1}{w(p)})^{-1} \\ &= \frac{\mu(|b|)A(a,f,h)}{\prod_{p|b}(w(p)-1)} = -\frac{\mu(2|b|)A(a,f,h)}{\prod_{p|b}(w(p)-1)}, \end{aligned}$$

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 3.1.

On using that $w(2) = 2$ along with the fact that both μ and w are multiplicative, we find that

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

First assume that f is even. Then a is odd and hence, for n odd, $a \equiv 1 (\mathrm{mod}\ (f,2n))$ if and only if $a \equiv 1 (\mathrm{mod}\ (f,n))$. It follows that

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

One easily checks that the latter formula also holds if f is odd. On noting that

$$S_2(b) + \sum_{\substack{2\nmid n,\ \Delta|\mathrm{lcm}(n,f) \\ a\equiv 1 (\mathrm{mod}\ (f,n))}} \frac{\mu(n)}{w(n)} = S(b),$$

we infer that $S_2(b) = -S(b)$. ∎

4. Proof of Theorem 1.2

i) The case b is odd and $(\frac{\gamma}{a}) = 1$; Using Lemma 2.4, Lemma 2.2 and the observation above, we find that $c_a(n) = 1$ in case $a \equiv 1 (\mathrm{mod}\ (f,n))$ and $c_a(n) = 0$ otherwise. This together with Theorem 1.1 and Lemma 2.3 implies that

$$\begin{aligned} \varphi(f)\delta(a,f,g) &= \sum_{\substack{n=1 \\ 2\nmid n}}^{\infty} \frac{\mu(n)}{w(n)} + \sum_{\substack{n=1,\ 2|n \\ \Delta\nmid \mathrm{lcm}(n,f)}}^{\infty} \frac{\mu(n)}{w(n)} + 2 \sum_{\substack{n=1,\ 2|n \\ \Delta|\mathrm{lcm}(n,f)}}^{\infty} \frac{\mu(n)}{w(n)}. \\ &= \sum_{n=1}^{\infty} \frac{\mu(n)}{w(n)} + \sum_{\substack{n=1,\ 2|n \\ \Delta|\mathrm{lcm}(n,f)}}^{\infty} \frac{\mu(n)}{w(n)} = \mathrm{I}_1 + S_2(b), \end{aligned} \tag{4.1}$$

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

ii) The case b is odd and $(\frac{\gamma}{a}) = -1$; Using Lemma 2.4, Lemma 2.2, the observation in the beginning of this proof and (4.1), we find

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

Now

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

In case $\Delta \equiv 0 (\mathrm{mod}\ 4)$, the latter sum is obviously zero. In case $\Delta \equiv 1 (\mathrm{mod}\ 4)$, a necessary condition for the latter sum to be non-zero is that $a \equiv 1 (\mathrm{mod}\ (f, 2\Delta))$. By (2.1) it then follows that $(\frac{\gamma}{a}) = (\frac{\gamma}{1}) = 1$, this contradiction shows that the latter sum is always zero. It thus follows that $\varphi(f)\delta(a,f,g) = \mathrm{I}_1 - S_2(b)$.

iii) The case b is even; In this case we cannot have that n is squarefree, $2|n$, $\Delta \nmid n$ and $\Delta|\mathrm{lcm}(f,n)$ (for this would imply that b is odd) and as in case i) we find that $c_a(n) = 1$ in case $a \equiv 1 (\mathrm{mod}\ (f,n))$ and $c_a(n) = 0$ otherwise. As in case i) we then find that $\varphi(f)\delta(a,f,g) = I_1 + S_2(b)$.

Note that in all three cases we have $\varphi(f)\delta(a,f,g) = I_1 + (\frac{\gamma}{a})S_2(b)$. Now, on using Proposition 3.1,

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

On invoking Lemma 3.1 it follows that

$$\varphi(f)\delta(a,f,g) = I_1 + (\frac{\gamma}{a})S_2(b) = A(a,f,h)\Big(1 + (\frac{\gamma}{a})\frac{\mu(2|b|)}{\prod_{p|b}(w(p)-1)}\Big).$$

On working out the product using Proposition 3.1, the proof is then completed. ■

5. Applications

1. *Hooley's theorem.* Setting $a = 1$ and $f = 1$ in Theorem 1.3 we obtain Hooley's theorem [7].

2. $a = 1$. Setting $a = 1$ in Theorem 1.2 we obtain Theorem 4 of [13]. Notice that of all the progressions mod f, the progression $1(\mathrm{mod}\ f)$ is the easiest to deal with, since trivially $c_1(n) = 1$ for every n.

3. *Rodier's conjecture.* Rodier [18], 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 $19(\mathrm{mod}\ 28)$ is $A/4$. From Theorem 1.2 it follows however that, under GRH, this density is $21A/82$ (cf. [10]): for each progression $a_i(\mathrm{mod}\ 28)$ under consideration we find that $\delta(a_i, 28, 2) = A(a_i, 28, 1)/\varphi(28) = 21A/246$.

4. *Zero density.* Lenstra [8, Theorem 8.3] gave a sketch of a proof of the following result.

Theorem 5.1. *Let $g \in \mathcal{G}$. 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* $(\frac{\Delta}{a}) = 1$;
iii) $\Delta | 3f$, $3 | \Delta$, $3 | h$ *and* $(\frac{-\Delta/3}{a}) = -1$.

This result very easily follows from Theorem 1.2. We leave it to the reader to show that if $\delta(a, f, g) = 0$, then actually $\mathcal{P}_{a,f,g}$ is finite. In each of these cases, there are obstructions not going beyond quadratic reciprocity. So, assuming GRH, loosely speaking $\delta(a, f, g) = 0$ if and only if there is an elementary obstruction, or obstruction coming from quadratic reciprocity.

5. *Equidistribution.* 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,

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

The progressions $a(\mathrm{mod}\ f)$ 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 [16] has written a nice survey concerning the (weak) uniform distribution of many important arithmetical sequences. Let $\mathcal{D}_g$ denote the set of natural numbers f such that $\mathcal{P}_g$ is weakly uniformly distributed modulo f.

Theorem 5.2. (GRH). *Let $g \in \mathcal{G}$ and let h the largest integer such that g is an hth power. Write $g = g_1 g_2^2$ with g_1 squarefree. If $g_1 = 21$ and $(h, 21) = 7$, then $\mathcal{D}_g = \{2^m 3^n : n,\ m \geq 0\}$. In the remaining cases we have*

$$D_g = \begin{cases} \{2^n : n \geq 0\} & \text{if } g_1 \equiv 1(\mathrm{mod}\ 4); \\ \{1, 2, 4\} & \text{if } g_1 \equiv 2(\mathrm{mod}\ 4); \\ \{1, 2\} & \text{if } g_1 \equiv 3(\mathrm{mod}\ 4). \end{cases}$$

Using only a formula for $\delta(1,f,g)$ and Theorem 1.1 in some special cases, this result was first deduced in [13]. Here a shorter proof, using the full force of Theorem 1.3, is given.

Proof of Thoerem 5.2. Put $S_f := \{A(a,f,h) \mid 1 \le a \le f,\ (a,f)=1\}$. Let γ be as in Theorem 1.2. Let us first consider the case where $f = 2^m$ for some $m \ge 0$. Notice that $|S_{2^m}| = 1$. By Theorem 1.3 we now infer that $\mathcal{P}_g$ is WUD mod 2^m if $g_1 \equiv 2 (\mathrm{mod}\ 4)$ and $m \le 2$, or $g_1 \equiv 3 (\mathrm{mod}\ 4)$ and $m \le 1$. In the remaining case we have

$$\Big(\frac{\gamma_1}{a}\Big) = \begin{cases} \big(\frac{1}{a}\big) & \text{if } g_1 \equiv 1 (\mathrm{mod}\ 4); \\ \big(\frac{-1}{a}\big) & \text{if } g_1 \equiv 3 (\mathrm{mod}\ 4); \\ \Big(\frac{(-1)^{\frac{g_1-2}{4}}2}{a}\Big) & \text{if } g_1 \equiv 2 (\mathrm{mod}\ 4), \end{cases}$$

and $\mathcal{P}_g$ is WUD 2^m if and only if $(\frac{\gamma_1}{a})$ is trivial character, that is if and only if $g_1 \equiv 1 (\mathrm{mod}\ 4)$.

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

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

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 $3|g_1,\ (3,h) = 1,\ \mu(|\beta|) = -1,\ g_1 \equiv 1 (\mathrm{mod}\ 4)$ 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 $q \ge 5$, then there exists $2 \le a_1 \le q-1$ such that $(\frac{\gamma_1}{a_1}) = 1$ and so, by Theorem 1.2, $\delta(1,f,g) \ne \delta(a_1,f,g)$. From this it immediately follows that in case f has an odd prime divisor and g is 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^m3^n, with $m \ge 0$ and $n \ge 1$ arbitrary. This follows easily from Theorem 1.2 and the calculation done in the case $f = 3$. ∎

6. *Optimal normal basis.* Let q be an odd given prime power and m a natural number. One can wonder whether there exists an extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_{q^m}$ such that $\mathbb{F}_{q^n}$ has an optimal normal basis over $\mathbb{F}_q$. A number theoretic question that arises in this context, see [1], is whether there is a prime p such that $p \equiv 1 (\mathrm{mod}\ m)$ and q is a primitive root modulo p and if yes to provide a small upper bound for the smallest such prime. The latter part of the question seems very difficult, but the results obtained in this paper allow one to shed some light on the first part of the question [4].

7. *Asymptotically exact heuristics.* On invoking Hooley's theorem [7] it can be shown, see [11], [14], that, under GRH, we have

$$\pi_g(x;2,1) = 2 \sum_{\substack{2<p\le x,\ (g/p)=-1 \\ (p-1,h)=1}} \frac{\varphi(p-1)}{p-1} + O_g\Big(\frac{x\log\log x}{\log^2 x}\Big),$$

were the sum is not so difficult to evaluate (with (g/p) the Legendre symbol, $g \in \mathcal{P}_g$ and h the largest integer such that g is an hth power). One would then expect that

$$\pi_g(x; f, a) = 2 \sum_{\substack{2<p\le x,\ (g/p)=-1 \\ p\equiv a \pmod f,\ (p-1,h)=1}} \frac{\varphi(p-1)}{p-1} + O_{f,g}\Big(\frac{x \log\log x}{\log^2 x}\Big). \tag{5.1}$$

Unconditionally the sum appearing here can be evaluated with error $O(x \log^{-c} x)$ with $c > 0$ arbitrary, see [14, Theorem 1]. It turns out that the main term equals $\delta(a, f, g)\mathrm{Li}(x)$, with $\delta(a, f, g)$ as given in Theorem 3. From this the truth of (5.1), on GRH, then follows. This is the main result (Theorem 4) of [14].

Acknowledgement. The author thanks F. Lemmermeyer and P. Stevenhagen for some helpful remarks and B. de Smit for updating him on [3].

References

[1] M. Christopoulou, T. Garefalakis, D. Panario and D. Thomson, The trace of an optimal normal element and low complexity normal bases, *Des. Codes Cryptogr.*, to appear (already published online).
[2] H. Cohen, *Number theory. Volume I: Tools and Diophantine equations*, Graduate Texts in Mathematics **239**, New York, NY, 2007.
[3] B. de Smit and W.J. Palenstijn, in preparation.
[4] T. Garefalakis, P. Moree and D. Panario, in preparation.
[5] R. Gupta and M. Ram Murty, A remark on Artin's conjecture, *Invent. Math.* **78** (1984), 127–130
[6] D.R. Heath-Brown, Artin's conjecture for primitive roots, *Quart. J. Math. Oxford* **37** (1986), 27-38.
[7] C. Hooley, Artin's conjecture for primitive roots, *J. Reine Angew. Math.* **225** (1967), 209-220.
[8] H.W. Lenstra, jr., On Artin's conjecture and Euclid's algorithm in global fields, *Invent. Math.* **42** (1977), 201-224.
[9] H.W. Lenstra, jr., Entangled radicals, Colloquium Lectures, AMS 112th Annual Meeting, San Antonio, January 12-15, 2006.
[10] P. Moree, On a conjecture of Rodier on primitive roots, *Abh. Math. Sem. Univ. Hamburg* **67** (1997), 165-171.
[11] ———, On some sums connected with primitive roots, MPIM-preprint, MPIM1998-42, available from http://www.mpim-bonn.mpg.de/Research/MPIM+Preprint+Series/
[12] ———, Primes in arithmetic progressions having a prescribed primitive root, MPIM-preprint, MPIM1998-57, available from http://www.mpim-bonn.mpg.de/Research/MPIM+Preprint+Series/
[13] ———, Uniform distribution of primes having a prescribed primitive root, *Acta Arith.* **89** (1999), 9–21.

[14] ———, On primes in arithmetic progression having a prescribed primitive root, *J. Number Theory* **78** (1999), 85–98.
[15] ———, On the distribution of the order and index of $g(\mathrm{mod}\ p)$ over residue classes. I, *J. Number Theory* **114** (2005), 238–271.
[16] W. Narkiewicz, *Uniform distribution of sequences of integers in residue classes,* Lecture Notes in Math. **1087**, Springer, Berlin, 1984.
[17] ———, *Elementary and analytic theory of algebraic numbers*, Springer, Berlin, 2nd edition, 1989.
[18] F. Rodier, Estimation asymptotique de la distance minimale du dual des codes BCH et polynômes de Dickson, *Discrete Math.* **149** (1996), 205-221.
[19] P. Stevenhagen, The correction factor in Artin's primitive root conjecture, *J. Théor. Nombres Bordeaux* **15** (2003), 383–391.
[20] E. Weiss, *Algebraic number theory*, New York University Press, New York, 1963.

Address: Max-Planck-Institut für Mathematik, Vivatsgasse 7, 53111 Bonn, Germany.
E-mail: moree@mpim-bonn.mpg.de
Received: 20 July 2007; **revised:** 4 September 2008