Uniform distribution of primes having a prescribed primitive root

Pieter Moree

January 21, 1997

Abstract

Suppose that $g \in \mathbb{Z}$ is not an hth power with $h \geq 2$. Let $\mathcal{P}_g$ denote the set of primes p such that g is a primitive root mod p and D_g the set of natural numbers $d \geq 1$ such that $\mathcal{P}_g$ is weakly uniformly distributed mod d. Assuming GRH, that is the Generalized Riemann Hypothesis, D_g is computed. En route, for arbitrary $f \geq 1$ the density of primes p such that $p \equiv 1(\text{mod } f)$ and g is a primitive root mod p is computed (on GRH).

1 Introduction

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

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

where $\varphi(d)$ denotes Euler's totient. In [6] the (weak) uniform distribution of many important arithmetical sequences is considered. In this note the weak uniform distribution of a class of sequences, apparently not considered in this light before, will be investigated. Let G be the set of integers g such that $g \neq -1$ and g is not a square. Let $\mathcal{P}_g$ denote the set of primes p such that g is a primitive root modulo p and let D_g denote the set of natural numbers d such that $\mathcal{P}_g$ is weakly uniformly distributed modulo d. Clearly a necessary condition for $\mathcal{P}_g$ to be infinite is that $g \in G$. That this is also a sufficient condition was conjectured by Emil Artin in 1927 and is called Artin's primitive root conjecture. There is no value of g for which $\mathcal{P}_g$ is known to be infinite. Presently the best unconditional result on Artin's conjecture is due to Heath-Brown [1], who strengthened a result of Gupta and Ram Murty. Heath-Brown's result implies that there are at most two primes for which Artin's conjecture fails. Assuming GRH, Hooley [2] proved in 1967 a quantitative version of Artin's conjecture. In this note we will make use of the following straightforward generalization of Hooley's result. As usual let ν respectively ζ_n denote the Möbius function respectively a primitive root of unity of order n.

Theorem 1 [5] *Let M be Galois and $g \neq \pm 1$ an integer. Suppose the Riemann Hypothesis holds for the fields $M_k := M(\zeta_k, g^{1/k})$ for every squarefree k. Then $N_M(g;x)$, the number of primes p not exceeding x that split completely in M and such that g is a primitive root mod p, satisfies*

$$N_M(g;x) = \left(\sum_{k=1}^{\infty} \frac{\mu(k)}{[M_k : \mathbb{Q}]}\right) \frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x}\right). \tag{1}$$

Define

$$\delta(M,g) := \sum_{k=1}^{\infty} \frac{\mu(k)}{[M_k : \mathbb{Q}]}.$$

Hooley computed $\delta(\mathbb{Q},g)$ for $g \in G$. It turns out that $\delta(\mathbb{Q},g) \neq 0$ for such g and thus Artin's conjecture holds true, on GRH. In particular $\delta(\mathbb{Q},g)$ is a rational number times

$$A = \prod_p \left(1 - \frac{1}{p(p-1)}\right) \quad (\approx .3739558),$$

the so called Artin constant. For example taking $g = 2$ and $M = \mathbb{Q}$ yields $\mathcal{P}_2(x) \sim Ax/\log x$. In this note we will compute $\delta(M,g)$ in case M is a cyclotomic field (Theorem 3). From Theorem 3 it is not dif and only ificult to deduce Theorem 2 with equality in i) replaced by inclusion (cf. the proof of Theorem 2). To obtain equality in i) we use the work of H. W. Lenstra [3].

In [8] Rodier, in connection with a coding theoretical result involving Dickson polynomials, made the conjecture that

$$\mathcal{P}_2(x;3,28) + \mathcal{P}_2(x;19,28) + \mathcal{P}_2(x;27,28) \sim \frac{A}{4}\frac{x}{\log x}. \tag{2}$$

Note that weak uniform distribution mod 28 of $\mathcal{P}_2$ would imply Rodier's conjecture. In [5] it was shown that $D_2 = \{1,2,4\}$, and thus $\mathcal{P}_2$ is not WUD mod 28. Moreover, it was shown that the true constant, on GRH, in (2) is 21A/82. Another coding theoretical application of primitive roots in arithmetic progressions occurs in the theory of perfect arithmetic codes [4].

In this note D_g will be computed in case g is not an hth power with $h \geq 2$. The same method can be applied for all $g \in G$, however at the cost of unwieldy technical complications. Throughout we use g_1 to denote the squarefree part of g, that is $g = g_1 g_2^2$, with g_1 squarefree. We put $h_1 = 2g_1$ if $g_1 \equiv 1 (\mathrm{mod}\ 4)$, otherwise we put $h_1 = 4g_1$.

Theorem 2 (GRH). *Let $g \in \mathbb{Z}$ not be an hth power, with $h \geq 2$. Then*

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

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

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

2 The density of primes $p \equiv 1 (\text{mod } f)$ having a prescribed primitive root

In this section Theorem 3 will be proved. This result gives, under GRH, for arbitrary $f \geq 1$ the density of primes p such that $p \equiv 1(\text{mod } f)$ and moreover a prescribed integer g is primitive root mod p. Theorem 1 relates this density to the degrees of the Kummerian fields $[M(\zeta_k, g^{1/k}) : \mathbb{Q}]$ with M cyclotomic. These degrees are computed in Lemma 2, making use of the following well-known fact from cyclotomy (see e.g. [9, p. 163]).

Lemma 1 *Let $0 \neq a \in \mathbb{Z}$. Write $a = a_1 a_2^2$, with a_1 squarefree. Then the smallest cyclotomic field containing $\mathbb{Q}(\sqrt{a})$ is $\mathbb{Q}(\zeta_{|a_1|})$ in case $a_1 \equiv 1(\text{mod } 4)$ and $\mathbb{Q}(\zeta_{4|a_1|})$ otherwise.*

Lemma 2 *Let g not be an hth power with $h \geq 2$. Suppose that $k|r$. Put $n(k, r) = [\mathbb{Q}(g^{1/k}, \zeta_r) : \mathbb{Q}]$. Then*

i) if k is odd, $n(k, r) = k\varphi(r)$;

ii) if k is even and $h_1 \nmid r$, $n(k, r) = k\varphi(r)$;

iii) if k is even and $h_1 | r$, $n(k, r) = k\varphi(r)/2$.

Proof. The conditions on g ensure that $[\mathbb{Q}(g^{1/k}) : \mathbb{Q}] = k$. Every subfield of a cyclotomic field is normal. The maximal normal subfield of $\mathbb{Q}(g^{1/k})$ is $\mathbb{Q}$ if k is odd and $\mathbb{Q}(\sqrt{g})$ if k is even. Thus if k is odd, $\mathbb{Q}(\zeta_r)$ and $\mathbb{Q}(g^{1/k})$ are linearly disjoint and hence

$$n(k, r) = [\mathbb{Q}(g^{1/k}) : \mathbb{Q}][\mathbb{Q}(\zeta_r) : \mathbb{Q}] = k\varphi(r).$$

If k is even, then $\sqrt{g} \in \mathbb{Q}(\zeta_r)$ if and only if $h_1 | r$, by Lemma 1. Then using that

$$n(k, r) = \frac{[\mathbb{Q}(g^{1/k}) : \mathbb{Q}][\mathbb{Q}(\zeta_r) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_r) \cap \mathbb{Q}(g^{1/k}) : \mathbb{Q}]} = \frac{k\varphi(r)}{[\mathbb{Q}(\zeta_r) \cap \mathbb{Q}(g^{1/k}) : \mathbb{Q}]},$$

the proof is completed. □

Proposition 1 *Let $f \geq 1$ be an integer. Then the function $h : \mathbb{N} \to \mathbb{N}$ defined by $h(k) = k\varphi(\text{lcm}(k, f))/\varphi(f)$ is multiplicative.*

Proof. We have to show that for arbitrary coprime natural numbers k and s,

$$\varphi(\text{lcm}(k, f))\varphi(\text{lcm}(s, f)) = \varphi(f)\varphi(\text{lcm}(ks, f)). \tag{2}$$

Due to the multiplicativity of Euler's totient the left hand side and the right hand side of (2) can be written as $\prod_{p|ksf} h_1(p)$ and $\prod_{p|ksf} h_2(p)$ respectively. Now suppose that $p|ksf$, $p^\alpha || k$, $\alpha \geq 1$. Then $p \nmid s$. Let $p^\beta || f$. Now $h_1(p) = \varphi(p^{\max(\alpha,\beta)})\varphi(p^\beta)$ and $h_2(p) = \varphi(p^\beta)\varphi(p^{\max(\alpha,\beta)})$. The case where $p|s$ and $p \nmid k$ is dealt with similarly. Thus (2) holds. □

Corollary 1 *For k odd, $h(2k)=h(2)h(k)=2h(k)$.*

Theorem 3 *Let $g\in\mathbb{Z}$ be not an hth power with $h\ge 2$. Let $f\ge 1$ be an arbitrary integer. Let Δ denote the discriminant of $\mathbb{Q}(\sqrt{g})$. Put $b=\Delta/(\Delta,f)$. For $k\ge 1$, put $h(k)=k\varphi(\mathrm{lcm}(k,f))/\varphi(f)$. Suppose the Riemann Hypothesis holds for the field $\mathbb{Q}(\zeta_f,g^{1/k},\zeta_k)$ for every squarefree k. Then $N_{\mathbb{Q}(\zeta_f)}(g;x)$, the number of primes p not exceeding x that split completely in $\mathbb{Q}(\zeta_f)$ and such that g is a primitive root mod p, satisfies*

$$N_{\mathbb{Q}(\zeta_f)}(g;x)=\delta(\mathbb{Q}(\zeta_f),g)\frac{x}{\log x}+O\left(\frac{x\log\log x}{\log^2 x}\right),$$

where

$$\begin{aligned}\delta(\mathbb{Q}(\zeta_f),g)&=\frac{1}{\varphi(f)}\prod_p(1-\frac{1}{h(p)})\left(1-\frac{\mu(|b|)}{\prod_{p|b}(h(p)-1)}\right)\\&=\frac{A}{\varphi(f)}\prod_{p|f}\left(1-\frac{p-2}{p^2-p-1}\right)\left(1-\frac{\mu(|b|)}{\prod_{p|b}(p^2-p-1)}\right)\end{aligned}\qquad(3)$$

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 $4|f$. Otherwise

$$\delta(\mathbb{Q}(\zeta_f),g)=\frac{1}{\varphi(f)}\prod_p(1-\frac{1}{h(p)})=\frac{A}{\varphi(f)}\prod_{p|f}\left(1-\frac{p-2}{p^2-p-1}\right).\qquad(4)$$

Proof. For notational convenience put $\delta=\delta(\mathbb{Q}(\zeta_f),g)$. Using Theorem 1 the proof of Theorem 3 reduces to rewriting

$$\delta=\sum_{k=1}^{\infty}\frac{\mu(k)}{[\mathbb{Q}(g^{1/k},\zeta_{\mathrm{lcm}(k,f)}):\mathbb{Q}]}$$

as a product. Using Lemma 2 and Corollary 1, it follows that

$$\begin{aligned}\varphi(f)\delta&=\sum_{k\ \mathrm{odd}}\frac{\mu(k)}{h(k)}+\sum_{\substack{k=1\\ h_1\nmid \mathrm{lcm}(2k,f)}}^{\infty}\frac{\mu(2k)}{h(2k)}+2\sum_{\substack{k=1\\ h_1|\mathrm{lcm}(2k,f)}}^{\infty}\frac{\mu(2k)}{h(2k)}.\\&=\frac{1}{2}\sum_{k\ \mathrm{odd}}\frac{\mu(k)}{h(k)}+\sum_{\substack{k=1\\ h_1|\mathrm{lcm}(2k,f)}}^{\infty}\frac{\mu(2k)}{h(2k)}=\mathrm{I}_1+\mathrm{I}_2.\end{aligned}$$

The arithmetic function h is multiplicative by Proposition 1, moreover $h(2)=2$ and thus

$$\mathrm{I}_1=\frac{1}{2}\sum_{k\ \mathrm{odd}}\frac{\mu(k)}{h(k)}=\frac{1}{2}\prod_{p\nmid 2}(1-\frac{1}{h(p)})=\prod_p(1-\frac{1}{h(p)}).$$

Suppose that $g_1\equiv 1(\mathrm{mod}\ 4)$. Thus $h_1=2g_1$ and since moreover h_1 is squarefree it follows that

$$\mathrm{I}_2=\sum_{\substack{k=1\\ g_1|kf}}^{\infty}\frac{\mu(2k)}{h(2k)}=\sum_{\substack{k=1\\ b|k}}^{\infty}\frac{\mu(2k)}{h(2k)}=\frac{\mu(2|b|)}{h(2|b|)}\sum_{\substack{k=1\\ (k,2b)=1}}^{\infty}\frac{\mu(k)}{h(k)}=-\frac{1}{2}\frac{\mu(|b|)}{h(|b|)}\prod_{p\nmid 2b}(1-\frac{1}{h(p)}),\qquad(5)$$

where in the derivation of the second equality it is used that $g_1/(g_1, f) = \Delta/(\Delta, f) = b$. The fourth identity follows on using that b is odd, $\mu(2) = -1$ and Corollary 1. Adding the product expansions so found for I_1 and I_2, one then obtains the first identity in (3). Notice that $\prod_{p|b}(h(p)-1) = \prod_{p|b,\ p|f}(p-1)\prod_{p|b,\ p\nmid f}(p^2-p-1)$. Since Δ is squarefree, $(b, f) = 1$ and thus $\prod_{p|b}(h(p)-1) = \prod_{p|b}(p^2-p-1)$. Using this, we arrive at the second identity in (3).

Next assume that $g_1 \equiv 3(\mathrm{mod}\ 4)$. Then $h_1 = 4g_1$. Since the only terms contributing to I_2 are those with k odd, for k is odd the condition $h_1|\mathrm{lcm}(2k, f)$ can only be satisfied if $4|f$. If $4 \nmid f$, then $\delta = \mathrm{I}_1/(2\varphi(f))$ and we obtain (4). If $4|f$, then the condition $h_1|\mathrm{lcm}(2k, f)$ can be replaced by $g_1|k(f/4)$ without altering the sum I_2. Analyzing I_2 as before, we find the same product, but with b replaced by $g_1/(g_1, f/4) = 4g_1/(4g_1, f) = \Delta/(\Delta, f)$. Notice that again b is odd and squarefree. So the fourth identity in (5) and the second in (3), follow as before.

Finally consider the case where $g_1 \equiv 2(\mathrm{mod}\ 4)$. Then if $8 \nmid f$, the sum I_2 is seen to be zero and in that case δ is given by (4). If $8|f$, the condition $h_1|\mathrm{lcm}(2k, f)$ can be replaced by $g_1|k(f/4)$ without altering the sum I_2. Now proceed as in the case where $g_1 \equiv 3(\mathrm{mod}\ 4)$. Notice that again b is odd and squarefree. So the fourth identity in (5) and the second in (3), follow as before. □

From Theorem 3 it is easily deduced that $\delta(\mathbb{Q}(\zeta_f), g) = 0$ if and only if $\Delta|f$, that is, by Lemma 1. if and only if $\sqrt{g} \in \mathbb{Q}(\zeta_f)$. This is a particular case of the following result.

Theorem 4 (GRH). *Let $g \in \mathbb{Z}$ be not an hth power with $h \geq 2$. Let M be an abelian number field. Then*

$$\delta(M, g) = 0 \iff \sqrt{g} \in M.$$

Moreover, if $N_M(g; x) \to \infty$ as $x \to \infty$, then $\delta(M, g) \neq 0$.

Proof. Since for odd q, $\mathbb{Q}(g^{1/q})$ is not normal, $\mathbb{Q}(\zeta_q, g^{1/q}) \not\subseteq M$. Using this and [3, Corollary 4.8], it then follows that $\delta(M, g) = 0$ if and only if $\sqrt{g} \in M$. The latter part of the assertion follows from [3, Theorem 4.6]. □

As an example let us consider the set $\mathcal{L}$ of primes ℓ such that there are infinitely many primes p satisfying $p \equiv \pm 1(\mathrm{mod}\ \ell)$ with ℓ a primitive root mod p. Thus we have to put $M = \mathbb{Q}(\zeta_\ell + \zeta_\ell^{-1})$ and $g = \ell$ in Theorem 4. Since $\sqrt{\ell} \in \mathbb{R}$ and M is the maximal real subfield of $\mathbb{Q}(\zeta_\ell)$, we have that $\sqrt{\ell} \in M$ if and only if $\sqrt{\ell} \in \mathbb{Q}(\zeta_\ell)$. Thus, using Lemma 1, we see that on GRH, $\mathcal{L} = \{\ell : \ell \equiv 3(\mathrm{mod}\ 4)\}$. Unconditionally it can be shown [7, Theorem 3.2] that $\mathcal{L}$ equals $\{\ell : \ell \equiv 3(\mathrm{mod}\ 4)\}$ with at most two primes excluded. The fact that $\mathcal{L}$ is infinite is used in Reznikov's proof of a weaker version of a conjecture of Lubotzky and Shalev on three-manifolds [7].

3 Proof of the main result

In this section we will prove Theorem 2. First we carry out some preparations.

Lemma 3 *Let $g \in \mathbb{Z}$. If k is squarefree and $g_1 \equiv 1 (\mathrm{mod}\ 4)$ then, for $n \geq 0$, $\mathbb{Q}(g^{1/k}, \zeta_k) \cap \mathbb{Q}(\zeta_{2^n}) = \mathbb{Q}$.*

Proof. The intersection of the two fields under consideration must be abelian and so is contained in $\mathbb{Q}(\sqrt{g}, \zeta_k)$. Since the prime divisors of $d(L_1 \cdot L_2)$ all divide $d(L_1)d(L_2)$, we see that $d_{\mathbb{Q}(\sqrt{g},\zeta_k)}$ is odd, on noting that $d_{\mathbb{Q}(\sqrt{g})} = g_1$, $d_{\mathbb{Q}(\zeta_k)} = d_{\mathbb{Q}(\zeta_{k/2})}$ for $k \equiv 2 (\mathrm{mod}\ 4)$ and that $d_{\mathbb{Q}(\zeta_k)}$ is not divisible by primes not dividing k. Thus 2 is not ramified in $\mathbb{Q}(\sqrt{g}, \zeta_k)$. On the other hand, the field $\mathbb{Q}(\zeta_{2^n})$ is at most ramified in 2. Thus $\mathbb{Q}(g^{1/k}, \zeta_k) \cap \mathbb{Q}(\zeta_{2^n}) \subseteq \mathbb{Q}(\sqrt{g}, \zeta_k) \cap \mathbb{Q}(\zeta_{2^n})$, where the latter field intersection is not ramified in any prime and hence, by a well-known theorem from Minkowski, equals $\mathbb{Q}$. $\square$

Lemma 4 (GRH). *Let $g \in \mathbb{Z}$ be not an hth power with $h \geq 2$. Let ℓ be an odd prime. Then $\delta(\mathbb{Q}(\zeta_l), g) \neq \delta(\mathbb{Q}, g)/\varphi(l)$.*

Corollary 2 *Let g and ℓ be as in Lemma 4. Then $\mathcal{P}_g$ is not WUD mod ℓ.*

Proof. We prove the result by contradiction. So assume that $\delta(\mathbb{Q}(\zeta_l), g) = \delta(\mathbb{Q}, g)/\varphi(l)$.

First assume that $g_1 \equiv 1 (\mathrm{mod}\ 4)$. Then, by Theorem 3 and $\Delta = g_1$, the equality $\delta(\mathbb{Q}(\zeta_l), g) = \delta(\mathbb{Q}, g)/\varphi(l)$ is equivalent with

$$\left(1 - \frac{\mu(|g_1|)}{\prod_{p|g_1}(p^2 - p - 1)}\right) = \left(1 - \frac{\ell - 2}{\ell^2 - \ell - 1}\right)\left(1 - \frac{\mu(|b|)}{\prod_{p|b}(p^2 - p - 1)}\right). \tag{6}$$

Now if $\ell \nmid g_1$, then $b = g_1$ and $1 - (\ell - 2)/(\ell^2 - \ell - 1) = 1$, a contradiction. If $\ell | g_1$, then $b = g_1/\ell$ and thus (6) becomes

$$\left(1 - \frac{\mu(|g_1|)}{\prod_{p|g_1}(p^2 - p - 1)}\right) = \left(1 - \frac{\ell - 2}{\ell^2 - \ell - 1}\right)\left(1 + \frac{\mu(|g_1|)(\ell^2 - \ell - 1)}{\prod_{p|g_1}(p^2 - p - 1)}\right).$$

Notice that $\mu(|g_1|) = 1$. We find

$$\prod_{p|g_1}(p^2 - p - 1) = \frac{(\ell^2 - \ell - 1)(\ell^2 - 2\ell + 2)}{\ell - 2}. \tag{7}$$

Since $((\ell^2 - \ell - 1)(\ell^2 - 2\ell + 2), \ell - 2)$ divides 2 and the left hand side of (7) is an integer, it follows that $\ell = 3$ and hence $\prod_{p|g_1}(p^2 - p - 1) = 25$. Contradiction.

Next assume $g_1 \not\equiv 1 (\mathrm{mod}\ 4)$. Then $\delta(\mathbb{Q}(\zeta_l), g) = \delta(\mathbb{Q}, g)/\varphi(l)$ implies, by Theorem 3, that $1 - (\ell - 2)/(\ell^2 - \ell - 1) = 1$. A contradiction. $\square$

Proof of Theorem 2. Assume that g satisfies the assumptions of Theorem 2 and, moreover, assume GRH. Then by Theorem 3 with $f = 1$ it follows that $\{1, 2\} \in D_g$. If $d \in D_g$, then for all divisors δ of d we must have $\delta \in D_g$. This observation together with Corollary 2 shows that $D_g \subseteq \{2^n : n \geq 0\}$. Suppose that $g_1 \equiv 3(\text{mod } 4)$, then by Theorem 3 it follows that $\mathcal{P}_g$ is not WUD mod 4. Thus in this case $D_g = \{1, 2\}$. If $g_1 \not\equiv 3(\text{mod } 4)$, then it is easy to see, by Theorem 3 again, that $4 \in D_g$. If $g_1 \equiv 2(\text{mod } 4)$ then, by Theorem 3 again, it follows that $\mathcal{P}_g$ is not WUD mod 8. Thus in this case $D_g = \{1, 2, 4\}$. Finally assume that $g_1 \equiv 1(\text{mod } 4)$. As we have seen $D_g \subseteq \{2^n : n \geq 0\}$. Theorem 3 shows that $\delta(\mathbb{Q}(\zeta_{2^n}), g) = \delta(\mathbb{Q}, g)/\varphi(2^n)$. This is consistent with weak uniform distribution mod 2^n. In fact, using a result of H. W. Lenstra [3], we will show that $\mathcal{P}_g$ is WUD mod 2^n for every $n \geq 3$. This then completes the proof.

Suppose that a is odd. The set of primes p such that $p \equiv a(\text{mod } 2^n)$ and g is a primitive root mod p is, with at most finite exceptions, equal to the set $M = M(\mathbb{Q}, \mathbb{Q}(\zeta_{2^n}), \sigma_a, < g >, 1)$. (We use Lenstra's notation.) Here σ_a denotes the automorphism of $\text{Gal}(\mathbb{Q}(\zeta_{2^n})/\mathbb{Q})$ determined by $\sigma_a(\zeta_{2^n}) = \zeta_{2^n}^a$. Under GRH, the prime density, δ_a, of the set M is, by [3, (3.15)], equal to

$$\delta_a = \sum_{k=1}^{\infty} \frac{\mu(k) c_a(k)}{[\mathbb{Q}(\zeta_{2^n}, g^{1/k}, \zeta_k) : \mathbb{Q}]},$$

where

$$c_a(k) := \#\{\{\sigma_a\} \cap \text{Gal}(\mathbb{Q}(\zeta_{2^n})/\mathbb{Q}(\zeta_{2^k}, g^{1/k}) \cap \mathbb{Q})\}.$$

Using Lemma 3, it follows that $c_a(k) = \#\{\{\sigma_a\} \cap \text{Gal}(\mathbb{Q}(\zeta_{2^n})/\mathbb{Q})\} = 1$, in case $g_1 \equiv 1(\text{mod } 4)$, for every squarefree k. Thus $\delta_a = \delta_1$. This and $\delta_1 = \delta(\mathbb{Q}(\zeta_{2^n}), g) > 0$, which follows by Theorem 3 (or alternatively Theorem 4), yields that $\mathcal{P}_g$ is WUD mod 2^n. $\square$

Remark. It is instructive to try to apply the latter part of the argument for $g_1 \not\equiv 1(\text{mod } 4)$ as well. Then we already know that $\mathcal{P}_g$ is not WUD mod 2^n for n large enough. Thus $c_a(k) \neq 1$ for some a and squarefree k, that is Lemma 3 must be false in this case. Indeed, if $g_1 \equiv 3(\text{mod } 4)$, then $\mathbb{Q}(g^{1/(2|g_1|)}, \zeta_{2|g_1|}) \cap \mathbb{Q}(\zeta_{2^n}) \supseteq \mathbb{Q}(i)$ for $n \geq 2$. If $g_1 \equiv 2(\text{mod } 4)$ then, for $n \geq 3$, $\mathbb{Q}(g^{1/|g_1|}, \zeta_{|g_1|}) \cap \mathbb{Q}(\zeta_{2^n})$ contains $\mathbb{Q}(\sqrt{2})$, respectively $\mathbb{Q}(\sqrt{-2})$ if $g_1/2 \equiv 1(\text{mod } 4)$, respectively $g_1/2 \equiv 3(\text{mod } 4)$.

The author thanks K. Belabas and T. Kleinjung for some helpful conversations.

References

[1] R. Heath-Brown, A remark on Artin's conjecture, *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] H. W. Lenstra, jr., Perfect arithmetic codes, Séminaire Delange-Pisot-Poitou, 19e année 1978/79, Théorie des nombres, Fasc. 1, Exp. No. 15, 14pp.

[5] P. Moree, On a conjecture of Rodier on primitive roots, MPI-preprint 117, Bonn, 1996.

[6] W. Narkiewicz, *Uniform distribution of sequences of integers in residue classes,* LNIM 1087, Springer, Berlin.

[7] A. Reznikov and P. Moree, Three-manifold subgroup growth, homology of coverings and simplicial volume, MPI-preprint 171, Bonn, 1996.

[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.

Pieter Moree
Max-Planck-Institut für Mathematik
Gottfried-Claren Str. 26
53225 Bonn
Germany
E-mail: moree@mpim-bonn.mpg.de