Uniform distribution of primes having a prescribed rational primitive root

Pieter Moree

Abstract

Suppose that $g \in \mathbb{Q}^*$ satisfies $g \neq -1$ and $g \notin \mathbb{Q}^2$. 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 $p \equiv 1 (\mathrm{mod}\ f)$ and g is a primitive root mod p is computed (on GRH). Also a related problem is considered.

[This is a rewritten an extended version of an earlier preprint, MPI-97-5, the main result is now extended to rational primitive roots and a related problem is considered.]

1 Introduction

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 d, denote by $S(x; a, d)$ the number of integers 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. The progressions $a(\mathrm{mod}\ d)$ 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 d if and only if all the progressions mod d get their fair share of primes from S. W. Narkiewicz [6] has written a nice survey on the state of knowledge regarding the (weak) uniform distribution of many important arithmetical sequences. 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 non-zero rational numbers g such that $g \neq -1$ and

1991 Mathematics Subject Classificiation. 11R45, 11A07, 11N69.

g is not a square of a rational number. 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 R. Heath-Brown [1]. Heath-Brown's result implies that there are at most two primes for which Artin's conjecture fails. Assuming GRH, C. 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 μ, respectively ζ_n denote the Möbius function, respectively a primitive root of unity of order n.

Theorem 1 [3] *Let M be Galois and $g \in G$. Suppose the Riemann Hypothesis holds for the fields $M(\zeta_k, g^{1/k})$ 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*

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

For $g \neq -1, 0, 1$ define

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

(Since $[M(\zeta_k, g^{1/k}) : \mathbb{Q}] \gg k\varphi(k)$, the series is seen to converge, even absolutely, and hence $\delta(M,g)$ is well-defined.) Hooley computed $\delta(\mathbb{Q}, g)$ for $g \in G \cap \mathbb{Z}$. 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 paper $\delta(M,g)$ in case M is cyclotomic (Theorem 4) will be computed. From Theorem 4 it is not difficult to deduce Theorem 2 with in the cases where it is asserted that D_g equals an infinite set, the assertion becomes that D_g is contained in this infinite set. To prove the equalities, the work of H. Lenstra [3] is used.

In [8] F. 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, on GRH, $D_2 = \{1, 2, 4\}$, and thus $\mathcal{P}_2$ is not weakly uniformly distributed 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 for $g \in G$. Notice that we can uniquely write $g = g_1 g_2^2$, with g_1 a squarefree integer and $g_2 \in \mathbb{Q}_{>0}$. We put $\gamma = 2g_1$ if $g_1 \equiv 1(\text{mod } 4)$, and $\gamma = 4g_1$ otherwise.

Theorem 2 (GRH). *Let $g \in G$, and h the largest integer such that g is a pure hth power. Assume that not both $g_1 = 21$ and $(h, 21) = 7$, then D_g, the set of natural numbers d 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 $D_g = \{2^n 3^m : n,\ m \geq 0\}$.

For simplicity we call g *exceptional* if $g_1 = 21$ and $(h, 21) = 7$ and *ordinary* otherwise. The following variant of Theorem 2 sheds some light on i), ii) and iii) of Theorem 2:

Theorem 3 (GRH). *Let g and h be as in Theorem 2 such that, moreover, g is not exceptional. Then $\mathcal{P}_g$ is weakly uniformly distributed modulo d if and only if for every squarefree $k \geq 1$, $\mathbb{Q}(\zeta_k, g^{1/k}) \cap \mathbb{Q}(\zeta_d) = \mathbb{Q}$.*

Lemma 6 shows that the condition in Theorem 3 that g be not exceptional cannot be dropped.

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

In this section Theorem 4 will be proved. This result gives, on 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 fields $M(\zeta_k, g^{1/k})$ with M cyclotomic (namely $M = \mathbb{Q}(\zeta_f)$). These degrees are computed in Lemma 2, making use of the following well-known fact from cyclotomy (see e.g. [10, p. 163]).

Lemma 1 *Let $0 \neq a \in \mathbb{Q}$. Write $a = a_1 a_2^2$, with a_1 a squarefree integer and $a_2 \in \mathbb{Q}$. 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.*

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

Lemma 2 *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 $\gamma \nmid r$, $n(k,r) = k_1\varphi(r)$;

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

Proposition 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.

Proof. For every multiplicative function g and arbitrary integers $a, b \geq 1$, we obviously have $g(a)g(b) = g(\gcd(a,b))g(\mathrm{lcm}(a,b))$. Hence, to finish the proof it is enough to show that $\varphi((k,f))$ is a multiplicative function of k, which is obvious. $\square$

Theorem 4 *Let $g \in G$ and h be the largest integer such that g is a pure hth power. Let $f \geq 1$ be an arbitrary integer. Let Δ denote the discriminant of $\mathbb{Q}(\sqrt{g})$. Put $b = \Delta/(\Delta, f)$. Let $w(k)$ be as in Proposition 1. Put*

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

If $(f,h) > 1$, then $\delta(\mathbb{Q}(\zeta_f), g) = 0$. Next assume that $(f,h) = 1$. Then

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

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

$$\delta(\mathbb{Q}(\zeta_f), g) = \frac{1}{\varphi(f)}\prod_p (1 - \frac{1}{w(p)}) = \frac{A(f,h)}{\varphi(f)}. \tag{4}$$

Let $N_{\mathbb{Q}(\zeta_f)}(g;x)$ denote 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. Suppose the Riemann Hypothesis holds for the field $\mathbb{Q}(\zeta_f, \zeta_k, g^{1/k})$ for every squarefree k. Then

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

Remark. The assertion of Theorem 4 in case $(f,h)>1$ can be trivially improved. Then the order mod p of g, for those primes p for which it exists, is bounded above by $(p-1)/q_1$, where q_1 is the smallest prime dividing (f,h). So $N_{\mathbb{Q}(\zeta_f)}(g;x)$ is bounded above and this holds unconditionally.

Proof of Theorem 4. For notational convenience put $\delta=\delta(\mathbb{Q}(\zeta_f),g)$. We have to evaluate

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

Using Lemma 2 it follows that

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

The arithmetic function w is multiplicative by Proposition 1 thus, by Euler's identity, $\mathrm{I}_1=\prod_p(1-1/w(p))$. Suppose that $g_1\equiv 1(\mathrm{mod}\ 4)$. Then $\gamma=2g_1$ and since moreover γ is squarefree it follows that

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

where in the derivation of the second equality it is used that $g_1/(g_1,f)=\Delta/(\Delta,f)=b$.

First consider the case that $(f,h)=1$. Then $w(p)>1$ for every prime p, and, moreover, $\prod_p(1-1/w(p))=A(f,h)>0$. Adding the product expansions that were found for I_1 and I_2 results in the first equality in (3) on using that $w(p)>1$. Notice that

$$\prod_{p|b}(w(p)-1)=\prod_{p|b,\ p|f}(p-1)\prod_{p|b,\ p\nmid f,\ p|h}(p-2)\prod_{p|b,\ p\nmid f,\ p\nmid h}(p^2-p-1).$$

Since g_1 is squarefree, $(b,f)=1$ and thus

$$\prod_{p|b}(w(p)-1)=\prod_{p|b,\ p|h}(p-2)\prod_{p|b,\ p\nmid h}(p^2-p-1).$$

Using this, we arrive at the second equality in (3).

Next assume that $g_1\equiv 3(\mathrm{mod}\ 4)$. Then $\gamma=4g_1$. For k is odd the condition $\gamma|\mathrm{lcm}(2k,f)$ can only be satisfied if $4|f$. Thus $I_2=0$ if $4\nmid f$ and hence $\delta=I_1/\varphi(f)$ and thus (4) is satisfied in this case. If $4|f$, the condition $\gamma|\mathrm{lcm}(2k,f)$ 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 $g_1/(g_1,f/4)=4g_1/(4g_1,f)=\Delta/(\Delta,f)$. Again b is odd and the fourth equality in (5) follows as before. Notice that again $(b,f)=1$. So the second equality in (3) follows as before.

Now consider the case where $g_1 \equiv 2 \pmod 4$. 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 $\gamma|\mathrm{lcm}(2k, f)$ can be replaced by $g_1|k(f/4)$ without altering the sum I_2. Now proceed as in the case where $g_1 \equiv 3 \pmod 4$. Again b is odd and the fourth equality in (5) follows as before. Notice that again $(b, f) = 1$. So the second equality in (3) follows as before.

Finally assume that $(f, h) > 1$. Since $g \in G$, h is odd. Since $(b, f) = 1$ and h is odd, there is an odd prime p_1 such that $p_1|h$, $p_1|f$ and $p_1 \nmid 2b$. Since $w(p_1) = 1$, it follows that $I_1 = I_2 = 0$ and thus $\delta(\mathbb{Q}(\zeta_f), g) = 0$.

The proof is completed on invoking Theorem 1. □

Let $g \in G$ and h be the largest integer such that g is a pure hth power. From [3, Theorem 8.3] it follows that, under GRH, $\delta(\mathbb{Q}(\zeta_f), g) = 0$ if and only if either $(f, h) > 1$ or $\Delta|f$. Notice that this is an easy consequence of Theorem 4. Assume GRH and, moreover, $(f, h) = 1$. Then the above fact can be reformulated, with the help of Lemma 1, as $\delta(\mathbb{Q}(\zeta_f), g) = 0$ if and only if $\sqrt{g} \in \mathbb{Q}(\zeta_f)$. This is a particular case of the following result:

Theorem 5 (GRH). *Let $g \in G$ and h be the largest integer such that g is a pure hth power. Let M be an abelian number field of conductor f. Suppose that $(f, h) = 1$. Then $\delta(M, g) = 0$ if and only if $\sqrt{g} \in M$. Moreover, if $N_M(g; x) \to \infty$ as $x \to \infty$, then $\delta(M, g) > 0$.*

We will deduce Theorem 5 from a result of Lenstra [3, Theorem 4.6], which in this context simplifies to:

Theorem 6 *Let $g \in G$ and $M : \mathbb{Q}$ be Galois. Let $\pi = \prod_{\ell|h,\ \ell \text{ prime}} \ell$, where h is the largest integer such that g is an hth power. Then if $\mathcal{P}_g$ is infinite, there exists $\sigma \in \mathrm{Gal}(M(\zeta_\pi)/\mathbb{Q})$ with $(\sigma|_M) = \mathrm{id}_M$ and, for every prime ℓ such that $\mathbb{Q}(\zeta_\ell, g^{1/\ell}) \subseteq M(\zeta_\pi)$, $(\sigma|_{\mathbb{Q}(\zeta_\ell, g^{1/\ell})}) \neq \mathrm{id}_{\mathbb{Q}(\zeta_\ell, g^{1/\ell})}$. Conversely, if such a σ exists and GRH is true, then $\mathcal{P}_g$ is infinite and $\delta(M, g) > 0$.*

Proof of Theorem 5. We first prove the if and only if part of the assertion.
'$\Leftarrow$'. If $\sqrt{g} \in M$, then there does not exist a σ such that $(\sigma|_M) = \mathrm{id}_M$ and $(\sigma|_{\mathbb{Q}(\zeta_2, \sqrt{g})}) \neq \mathrm{id}_{\mathbb{Q}(\zeta_2, \sqrt{g})}$, thus, by Theorem 6, $\delta(M, g) = 0$.
'$\Rightarrow$'. If $\ell \nmid h$ and ℓ is odd, then $\mathbb{Q}(g^{1/\ell})$ is not normal and hence $\mathbb{Q}(\zeta_\ell, g^{1/\ell}) \not\subseteq M(\zeta_\pi)$. If $\ell|h$, then $\mathbb{Q}(\zeta_\ell, g^{1/\ell}) = \mathbb{Q}(\zeta_\ell) \subseteq M(\zeta_\pi)$. Thus the ℓ such that $\mathbb{Q}(\zeta_\ell, g^{1/\ell}) \subseteq M(\zeta_\pi)$, are precisely the prime divisors of π and possibly 2. We are done if we show that if $\sqrt{g} \notin M$, there exists σ satisfying the requirements of Theorem 6. The existence of σ is a consequence of the Galois correspondence. The extension $M(\zeta_h) : M$ is Galois. If an extension σ as required in Theorem 5 would not exist, then either $M(\zeta_\ell)$ for some prime $\ell|\pi$ or $M(\sqrt{g})$ would be contained in the fixed field of $\mathrm{Gal}(M(\zeta_h)/M)$. Since $\ell \nmid f$, $M(\zeta_\ell) \neq M$. Furthermore, $M(\sqrt{g}) \neq M$. Thus $M(\zeta_\pi) : M$ is not Galois. Contradiction.

The assertion regarding $N_M(g; x)$ now easily follows using the latter part of Theorem 6. □

As an example let us consider the set $\mathcal{L}$ of odd primes ℓ such that there are infinitely many primes p satisfying $p \equiv \pm 1 (\bmod \ell)$ 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 5. 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, $\mathcal{L} = \{\ell : \ell \equiv 3 (\bmod 4)\}$. Unconditionally it can be shown [7, Theorem 3.2] that $\mathcal{L}$ equals $\{\ell : \ell \equiv 3 (\bmod 4)\}$ with at most two primes excluded. The fact that $\mathcal{L}$ is non-empty is used in A. 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 Theorem 2 will be proved. First we carry out some preparations. Throughout we denote by h the largest integer such that g is a pure hth power.

The next two lemmas are well-known. Lemma 3 follows for example from [9, Theorem 13.2.1]. For the convenience of the reader a direct proof is given. For Lemma 4, I was not able to find a reference.

Lemma 3 *Let M be a number field and $\kappa \in M$. If $[M(\zeta_k, \kappa^{1/k}) : M] = k\varphi(k)$, then $M(\zeta_k) : M$ is the maximal abelian subextension of $M(\zeta_k, \kappa^{1/k}) : M$.*

Proof. Let
$$\mathcal{M}_k = \left\{ \begin{pmatrix} 1 & 0 \\ r & s \end{pmatrix} \ : \ r \in \mathbb{Z}/k\mathbb{Z}, \ s \in (\mathbb{Z}/k\mathbb{Z})^* \right\}.$$
Notice that $\mathcal{M}_k'$, the commutator subgroup of $\mathcal{M}_k$, equals $\left\{ \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} \ : \ r \in \mathbb{Z}/k\mathbb{Z} \right\}$. It is enough to show that if the condition of the lemma is satisfied, then $\mathrm{Gal}(M(\zeta_k, \kappa^{1/k}) : M) \cong \mathcal{M}_k$. For then the Galois group of the maximal abelian subextension of $M(\zeta_k, \kappa^{1/k}) : M$ is isomorphic to $\mathcal{M}_k/\mathcal{M}_k' \cong (\mathbb{Z}/k\mathbb{Z})^*$. Since the maximal abelian subextension of $M(\zeta_k, \kappa^{1/k}) : M$ contains $M(\zeta_k) : M$ and the condition of the lemma implies that the latter has Galois group $(\mathbb{Z}/k\mathbb{Z})^*$, we are done.

Let α be a root of $x^k - \kappa$. For any $\sigma \in \mathrm{Gal}(M(\zeta_k, \kappa^{1/k}) : M)$, there exists $\ell(\sigma) \in (\mathbb{Z}/k\mathbb{Z})$ and $m(\sigma) \in (\mathbb{Z}/k\mathbb{Z})^*$, such that $\sigma(\alpha) = \zeta_k^{\ell(\sigma)}\alpha$ and $\sigma(\zeta_k) = \zeta_k^{m(\sigma)}$. Now define a map $\psi \mapsto \begin{pmatrix} 1 & 0 \\ \ell(\sigma) & m(\sigma) \end{pmatrix}$. One checks that it is a monomorphism of $\mathrm{Gal}(M(\zeta_k, \kappa^{1/k}) : M)$ into $\mathcal{M}_k$. Since $|\mathcal{M}_k| = k\varphi(k)$ and, by assumption, $|\mathrm{Gal}(M(\zeta_k, \kappa^{1/k}) : M)| = k\varphi(k)$, ψ is actually an isomorphism. □

Lemma 4 *Let $g \in G$ and k be squarefree. Then the maximal abelian subextension of $\mathbb{Q}(\zeta_k, g^{1/k})$ is $\mathbb{Q}(\zeta_k)$ if k is odd and $\mathbb{Q}(\zeta_k, \sqrt{g})$ otherwise.*

Proof. Write $g = \gamma_1^h, \ \gamma_1 \in \mathbb{Q}$.
i) k is odd. By Lemma 2 and Lemma 3, $\mathbb{Q}(\zeta_k)$ is the maximal abelian subextension of $\mathbb{Q}(\zeta_k, \gamma_1^{1/k})$. Since $\mathbb{Q}(\zeta_k) \subseteq \mathbb{Q}(\zeta_k, g^{1/k}) \subseteq \mathbb{Q}(\zeta_k, \gamma_1^{1/k})$, we are done in this case.
ii) k is even and $\sqrt{\gamma_1} \notin \mathbb{Q}(\zeta_k)$. Taking $M = \mathbb{Q}(\sqrt{\gamma_1})$ and $k = \gamma_1$ in Lemma 3, we find,

on using Lemma 2, that the maximal abelian subextension of $\mathbb{Q}(\zeta_k,\sqrt{\gamma_1}) = \mathbb{Q}(\zeta_k,\sqrt{g})$. Since $\mathbb{Q}(\zeta_k,\sqrt{g}):\mathbb{Q}$ is abelian and

$$\mathbb{Q}(\zeta_k,\sqrt{g}) \subseteq \mathbb{Q}(\zeta_k,g^{1/k}) \subseteq \mathbb{Q}(\zeta_k,\gamma_1^{1/k}),$$

we are done in this case.
iii) k is even and $\sqrt{\gamma_1}\in\mathbb{Q}(\zeta_k)$. Using Lemma 2 it follows that $\mathbb{Q}(\zeta_k,g^{1/k}) = \mathbb{Q}(\zeta_{k/2},g^{2/k})$. Since by assumption $4\nmid k$, we are thus reduced to case i). □

Lemma 5 *Let $g\in G$. If $g_1\equiv 1(\mathrm{mod}\ 4)$ and k is squarefree then, for $n\ge 0$, $\mathbb{Q}(\zeta_k,g^{1/k})\cap\mathbb{Q}(\zeta_{2^n})=\mathbb{Q}$.*

Proof. The intersection of the two fields under consideration must be abelian and is contained in $\mathbb{Q}(\zeta_k,\sqrt{g})$ by Lemma 4. Let d_K denote the discriminant over $\mathbb{Q}$ of the number field K. Since the prime divisors of $d_{L_1\cdot L_2}$ all divide $d_{L_1}d_{L_2}$, we see that $d_{\mathbb{Q}(\zeta_k,\sqrt{g})}$ 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 at $\mathbb{Q}(\zeta_k,\sqrt{g})$. On the other hand, the field $\mathbb{Q}(\zeta_{2^n})$ is at most ramified at 2. Thus $\mathbb{Q}(\zeta_k,g^{1/k})\cap\mathbb{Q}(\zeta_{2^n})\subseteq\mathbb{Q}(\zeta_k,\sqrt{g})\cap\mathbb{Q}(\zeta_{2^n})$, where the latter field intersection is not ramified at any prime and hence, by a well-known theorem due to Minkowski, equals $\mathbb{Q}$. □

An integer is called y-smooth if all its prime divisors are $\le y$.

Lemma 6 *Let d be 3-smooth, but not 2-smooth. Let $g\in G$ be such that $g_1=21$ and $(h,21)=7$. Let $k\ge 1$ be squarefree. Then $\mathbb{Q}(\zeta_k,g^{1/k})\cap\mathbb{Q}(\zeta_d)=\mathbb{Q}(\sqrt{-3})$ if $3|k$ or $14|k$ and $\mathbb{Q}$ otherwise. Put $v(k)=[\mathbb{Q}(\zeta_k,g^{1/k},\zeta_d):\mathbb{Q}]$ and $k_1=k/(k,h)$. If $42|k$, then $v(k)=\varphi(d)\varphi(k)k_1/4$, if $3\nmid k$ and $14\nmid k$, then $v(k)=\varphi(d)\varphi(k)k_1$ and $v(k)=\varphi(d)\varphi(k)k_1/2$ otherwise.*

Proof. When k is even we have

$$\mathbb{Q}(\zeta_k,g^{1/k})\cap\mathbb{Q}(\zeta_d)\subseteq\mathbb{Q}(\zeta_k,\sqrt{21})\cap\mathbb{Q}(\zeta_d)\subseteq\mathbb{Q}(\zeta_k,\sqrt{21})\cap\mathbb{Q}(\zeta_{3^\alpha})\subseteq\mathbb{Q}(\zeta_3),$$

where $3^\alpha||d$. The first inclusion follows on using Lemma 4, the second on using that $\mathbb{Q}(\zeta_k,\sqrt{g})$ is not ramified at 2 (cf. the proof of the previous lemma) and the third on noticing that $\sqrt{21}\notin\mathbb{Q}(\zeta_{3^\alpha})$ and $(k,3^\alpha)|3$. The above inclusions also hold for the case k is odd, but then $\sqrt{21}$ can be left out. In that case it is clear that $\mathbb{Q}(\zeta_k,g^{1/k})\cap\mathbb{Q}(\zeta_d)=\mathbb{Q}(\zeta_3)$ if and only if $3|k$. Now the intersection part of the assertion follows if we show that, for squarefree k, $\sqrt{-3}\in\mathbb{Q}(\zeta_{2k},\sqrt{21})$ if and only if $3|k$ or $7|k$. The $\Leftarrow$ direction of this assertion is obvious. Now assume that $3\nmid k$ and $7\nmid k$ and assume that $\sqrt{-3}\in\mathbb{Q}(\zeta_{2k},\sqrt{21})$. Then $\mathbb{Q}(\sqrt{21})$ is linearly disjoint from $\mathbb{Q}(\zeta_{2k})$ and the compositum has Galois group isomorphic to $(\mathbb{Z}/2k\mathbb{Z})^*\times\mathbb{Z}/2\mathbb{Z}$. Let $\omega(k)$ denote the number of distinct prime divisors of k. Then $\mathbb{Q}(\zeta_{2k},\sqrt{21})$ contains $2^{\omega(k)+1}-1$ distinct quadratic subfields. On the other hand, denoting the odd prime divisors of k by $p_1,\cdots,p_{\omega(k)}$ and $p^*:=(-1/p)p$, we can construct $2^{\omega(k)+2}-1$ distinct quadratic subfields, on using that $\sqrt{-3}, \sqrt{-7}, \sqrt{p_1^*}, \cdots, \sqrt{p_{\omega(k)}^*} \in \mathbb{Q}(\zeta_{2k}, \sqrt{21})$. Contradiction.

The rest of the assertion now follows easily. We have $[\mathbb{Q}(\zeta_k, g^{1/k}) : \mathbb{Q}] = \varphi(k)k_1/2$ if $42|k$ and $[\mathbb{Q}(\zeta_k, g^{1/k}) : \mathbb{Q}] = \varphi(k)k_1$ otherwise. Now use that

$$v(k) = \frac{[\mathbb{Q}(\zeta_k, g^{1/k}) : \mathbb{Q}][\mathbb{Q}(\zeta_d) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_k, g^{1/k}) \cap \mathbb{Q}(\zeta_d) : \mathbb{Q}]},$$

together with the first part of the assertion. Alternatively one can use Lemma 2 to establish the assertions on $v(k)$ made in Lemma 6. □

Lemma 7 *Let $g \in G$. Let ℓ be an odd prime not dividing h. Then $\delta(\mathbb{Q}(\zeta_\ell), g) \neq \delta(\mathbb{Q}, g)/\varphi(\ell)$, except when g is exceptional and $\ell = 3$.*

Proof. Using Theorem 4 we see that $\delta(\mathbb{Q}(\zeta_3), g) = \delta(\mathbb{Q}, g)/2$ in case g is exceptional. The remainder of the assertion we prove by contradiction. So assume that $\delta(\mathbb{Q}(\zeta_\ell), g) = \delta(\mathbb{Q}, g)/\varphi(\ell)$ and that we are not in the case where g is exceptional and $\ell = 3$. Put $P(\alpha, \beta) = \prod_{p|\alpha,\ p|\beta}(p-2)\prod_{p|\alpha,\ p\nmid\beta}(p^2-p-1)$.

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

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

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

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

Notice that $\mu(|g_1|) = 1$. We find $P(g_1, h) = (\ell^2 - \ell - 1)(\ell^2 - 2\ell + 2)/(\ell - 2)$. Since $((\ell^2-\ell-1)(\ell^2-2\ell+2), \ell-2)$ divides 2 and $P(g_1, h)$ must be an integer, it follows that $\ell = 3$ and hence $P(g_1, h) = 25$. Thus g is exceptional and $\ell = 3$, which contradicts our assumption.

Next assume $g_1 \not\equiv 1 (\mathrm{mod}\ 4)$. Then $\delta(\mathbb{Q}(\zeta_\ell), g) = \delta(\mathbb{Q}, g)/\varphi(\ell)$ implies, by Theorem 4, $A(\ell, h) = A(1, h)$ and hence $1 - (\ell-2)/(\ell^2-\ell-1) = 1$. A contradiction. □

Lemma 7 has the following easy consequence for the weak uniform distribution of $\mathcal{P}_g$.

Lemma 8 (GRH). *Let $g \in G$ and ℓ be an odd prime. Then $\mathcal{P}_g$ is not weakly uniformly distributed mod ℓ, except when g is exceptional and $\ell = 3$.*

Proof. Left to the reader. □

Proof of Theorem 2. Assume that g satisfies the assumptions of Theorem 2 and, moreover, assume GRH. Then by Theorem 4 with $f = 1$ it follows that $\{1, 2\} \subseteq D_g$. If $d \in D_g$, then for all divisors δ of d we must have $\delta \in D_g$. First consider the case where g is ordinary. Then this observation together with Lemma 8 shows that $D_g \subseteq \{2^n : n \geq 0\}$. Suppose that $g_1 \equiv 3 (\mathrm{mod}\ 4)$, then by Theorem 4 it follows that $\mathcal{P}_g$ is not weakly uniformly distributed mod 4. Thus in this case $D_g = \{1, 2\}$. If $g_1 \not\equiv 3 (\mathrm{mod}\ 4)$, then it is easy to see, by Theorem 4 again, that $4 \in D_g$. If $g_1 \equiv 2 (\mathrm{mod}\ 4)$ then, by Theorem 4 again, it follows that $\mathcal{P}_g$ is not weakly uniformly distributed mod 8. Thus in this case $D_g = \{1, 2, 4\}$. Finally assume that $g_1 \equiv 1 (\mathrm{mod}\ 4)$. As we have seen $D_g \subseteq \{2^n : n \geq 0\}$. Theorem 4 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 Lenstra [3], we will show that $\mathcal{P}_g$ is weakly uniformly distributed mod 2^n for every $n \geq 3$. This then completes the proof in the case where g is ordinary.

Suppose that a is odd. The set of primes p such that $p \equiv a \pmod{2^n}$ 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 $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^n})/\mathbb{Q})$ 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, (2.15)], equal to

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

where $c_a(k) = 1$ if σ_a fixes $\mathbb{Q}(\zeta_k, g^{1/k}) \cap \mathbb{Q}(\zeta_{2^n})$ pointwise and $c_a(k) = 0$ otherwise. In case $g_1 \equiv 1 (\mathrm{mod}\ 4)$, by Lemma 5 the latter intersection of fields equals $\mathbb{Q}$ (at least when k is squarefree) and hence $c_a(k) = 1$ 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 4 (or alternatively Theorem 5), yields that $\mathcal{P}_g$ is weakly uniformly distributed mod 2^n.

It remains to deal with the case where g is exceptional. By Corollary 8, a necessary condition for $\mathcal{P}_g$ to be weakly uniformly distributed mod d, is that d is 3-smooth. The proof of the theorem will be completed once we show that this necessary condition is also sufficient. The analysis of the case $g_1 \equiv 1 (\mathrm{mod}\ 4)$ applies in the exceptional case as well and we find that for every 2-smooth integer d, $\mathcal{P}_g$ is weakly uniformly distributed mod d. Next assume that d is 3-smooth, but not 2-smooth. Let a be an integer such that $(a, 6) = 1$. Let σ_a denote the automorphism of $\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ determined by $\sigma_a(\zeta_d) = \zeta_d^a$. Then $\delta_a = \sum_k \mu(k)\tilde{c}_a(k)/v(k)$, where $\tilde{c}_a(k) = 1$ if σ_a fixes $M_{k,d} := \mathbb{Q}(\zeta_k, g^{1/k}) \cap \mathbb{Q}(\zeta_d)$ pointwise and $\tilde{c}_a(k) = 0$ otherwise. (Recall that $v(k) = [\mathbb{Q}(\zeta_k, g^{1/k}, \zeta_d) : \mathbb{Q}]$.) By Lemma 6, there are, in case k is squarefree, only two possibilities for $M_{k,d}$; either $\mathbb{Q}(\sqrt{-3})$ or $\mathbb{Q}$. Thus either $\delta_a = \sum_k \mu(k)/v(k)$, or $\delta_a = \sum_k \mu(k)/v(k) - \sum_{3|k \text{ or } 14|k} \mu(k)/v(k)$ (depending on whether σ_a fixes $\mathbb{Q}(\sqrt{-3})$ or not). Since, by Theorem 5 for example, $\delta_1 > 0$, it remains to show that

$$J := \sum_{\substack{k=1 \\ 3|k \text{ or } 14|k}}^{\infty} \frac{\mu(k)}{v(k)} = 0.$$

Now

$$J = \sum_{\substack{3|k \\ 14\nmid k}} \frac{\mu(k)}{v(k)} + \sum_{\substack{3\nmid k \\ 3|k}} \frac{\mu(k)}{v(k)} + \sum_{42|k} \frac{\mu(k)}{v(k)} = J_1 + J_2 + J_3,$$

say. Using Lemma 6 we find

$$J_1 = -\frac{1}{18\varphi(d)} \prod_{p \neq 2,3,7} \left(1 - \frac{1}{p(p-1)}\right) \prod_{\substack{p|h \\ p \neq 7}} \left(1 - \frac{1}{p-1}\right),$$

$J_2 = -3J_1$ and $J_3 = 2J_1$. Hence $J = 0$. $\square$

Remark 1. In the exceptional case the only integers that can be shown to be in D_g by appealing to Theorem 4 only, are $1, 2, 3, 4, 6$ and 12.

Remark 2. It is instructive to try to apply the argument that showed that $\mathcal{P}_g$ is weakly uniformly distributed modulo 2-smooth numbers in case $g_1 \equiv 1 (\text{mod } 4)$ to the remaining g_1. Then we already know that $\mathcal{P}_g$ is not weakly uniformly distributed mod 2^n for n large enough. Thus $c_a(k) \neq 1$ for some a and squarefree k, that is Lemma 5 must be false in this case. Indeed, if $g_1 \equiv 3 (\text{mod } 4)$, then $\mathbb{Q}(\zeta_{2|g_1|}, g^{1/(2|g_1|)}) \cap \mathbb{Q}(\zeta_{2^n}) \supseteq \mathbb{Q}(i)$ for $n \geq 2$. If $g_1 \equiv 2 (\text{mod } 4)$ then, for $n \geq 3$, $\mathbb{Q}(\zeta_{|g_1|}, g^{1/|g_1|}) \cap \mathbb{Q}(\zeta_{2^n})$ 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 next lemma together with Theorem 2 immediately implies Theorem 3.

Lemma 9 *Let $d \geq 1$ and $g \in G$. We have $\mathbb{Q}(\zeta_k, g^{1/k}) \cap \mathbb{Q}(\zeta_d) = \mathbb{Q}$ for every squarefree k if and only if* i), ii) *or* iii) *of Theorem 2 is satisfied.*

Proof. '$\Rightarrow$'. Suppose d contains an odd prime factor, p. Then $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\zeta_p, g^{1/p}) \cap \mathbb{Q}(\zeta_d)$ thus $d = 2^n$, for some $n \geq 0$. Suppose that $g_1 \equiv 2 (\text{mod } 4)$, we have to show that $n \leq 2$. So assume that $n \geq 3$. Then $\mathbb{Q}(\zeta_{|g_1|}, g^{1/|g_1|}) \cap \mathbb{Q}(\zeta_{2^n})$ contains $\mathbb{Q}(\sqrt{2})$, respectively $\mathbb{Q}(\sqrt{-2})$ if $g_1/2 \equiv 1 (\text{mod } 4)$, respectively $g_1/2 \equiv 3 (\text{mod } 4)$. Finally suppose that $g_1 \equiv 3 (\text{mod } 4)$. We have to show that $n \leq 1$. So assume that $n \geq 2$. Notice that then $\mathbb{Q}(i) \subseteq \mathbb{Q}(\zeta_{2|g_1|}, g^{1/2|g_1|}) \cap \mathbb{Q}(\zeta_{2^n})$.
'$\Leftarrow$'. If $g_1 \equiv 1 (\text{mod } 4)$, then this follows by Lemma 5. The other cases, except $g_1 \equiv 2 (\text{mod } 4)$ and $d = 4$ are trivial. It remains to show that $i \notin \mathbb{Q}(\zeta_k, g^{1/k})$ for k squarefree and $g_1 \equiv 2 (\text{mod } 4)$. A way of showing that $i \notin \mathbb{Q}(\zeta_k, g^{1/k})$ is to show that $[\mathbb{Q}(\zeta_{\text{lcm}(4,k)}, g^{1/k}) : \mathbb{Q}] = 2[\mathbb{Q}(\zeta_k, g^{1/k}) : \mathbb{Q}]$. This now follows by computing these degrees using Lemma 2. $\square$

4 A related open problem

Throughout this section g is assumed to be in G. A question similar to that of determining D_g, is to determine all d and g such that $\delta(\mathbb{Q}(\zeta_d), g) = \delta(\mathbb{Q}, g)/\varphi(d)$. Some obvious solutions are given by Theorem 2. In order to exclude these solutions from further consideration, I introduce the concept of special pairs. To this end let us define, for a coprime to d,

$$\delta(a, d, g) = \sum_{k=1}^{\infty} \frac{\mu(k) c_a(k)}{[\mathbb{Q}(\zeta_k, g^{1/k}, \zeta_d) : \mathbb{Q}]},$$

where $c_a(k) = 1$ if σ_a fixes $\mathbb{Q}(\zeta_k, g^{1/k}) \cap \mathbb{Q}(\zeta_d)$ pointwise and $c_a(k) = 0$ otherwise. (Here σ_a denotes the automorphism of $\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ determined by $\sigma_a(\zeta_d) = \zeta_d^a$.) Notice that $\delta(1,d,g) = \delta(\mathbb{Q}(\zeta_d), g)$. We say that a pair $[g,d]$ is *special* if $\delta(1,d,g) = \delta(1,1,g)/\varphi(d)$, and there exists a such that $\delta(a,d,g) \neq \delta(1,1,g)/\varphi(d)$. If for some g, there is no d such that $[g,d]$ is special, then g is said to be a *good generator*. Similarly, if for some d there is no g such that $[g,d]$ is special, then d is said to be a *good modulus*. Notice that, under GRH, a generator g is good if, for arbitrary d, the progession $1(\bmod\ d)$ gets its fair share of primes from $\mathcal{P}_g$ if and only if $\mathcal{P}_g$ is weakly uniformly distributed mod d. On using Theorem 4 it is easily deduced that if $g_1 \not\equiv 1(\bmod\ 4)$, then g is a good generator. So from now on assume that $g_1 \equiv 1(\bmod\ 4)$. Recall that $P(\alpha,\beta) = \prod_{p|\alpha,\ p|\beta}(p-2)\prod_{p|\alpha,\ p\nmid\beta}(p^2-p-1)$. Notice that $P(\alpha,\beta)$ is odd when β is odd. From Theorem 4 and the proof of Theorem 2 it now follows that $[g,d]$ is special if it satisfies

$$\left(1 - \frac{\mu(|g_1|)}{P(g_1,h)}\right) = \kappa(d)\left(1 - \frac{\mu(|b|)}{P(b,h)}\right) \tag{7}$$

and d is not listed in Theorem 2. In (7) the function κ is defined by

$$\kappa(d) := \prod_{p|d}\left(1 - \frac{p-2}{p^2-p-1}\right) = \prod_{p|d}\frac{(p-1)^2}{p^2-p-1}.$$

Notice that $\kappa : \mathbb{N} \to \mathbb{Q}$ is a multiplicative function satisfying $0 < \kappa(d) \le 1$. Also note that $(x-2)/(x^2-x-1)$ is monotonously decreasing for $x > 3$ and that $\kappa(d) = 1$ implies that d is 2-smooth. Let $\tilde{I}$ denote the image of the odd integers under κ. Clearly $\tilde{I}$ equals $\kappa(\mathbb{N})$ with 1 removed. Recall that $b = g_1/(g_1,d)$.

First we will fix g and study the set of moduli d for which (7) is satisfied. Since we are only interested in exceptional pairs and every 2-smooth number d is a good modulus, we may assume that d contains an odd prime factor, and hence $\kappa(d) < 1$. By comparing the size of the left and right hand side of (7), it is seen that $\mu(|b|) = -1$. Thus $(g_1,d) \neq |g_1|$. On the other hand, if $(g_1,d) = 1$ then d must be 2-smooth. Thus it follows that $[g,d]$ is not special if g_1 is a prime.

Taking $\mu(|b|) = -1$ and rewriting (7) a little bit shows that if

$$Q(g,\tilde{\delta}) \notin \tilde{I} \text{ for all } \tilde{\delta}|g_1 \text{ with } 1 < \tilde{\delta} < |g_1| \text{ and } \mu(|g_1/\tilde{\delta}|) = -1, \tag{8}$$

where, for $\tilde{\delta}|g_1$,

$$Q(g,\tilde{\delta}) := \frac{P(g_1,h) - \mu(|g_1|)}{P(\tilde{\delta},h)(P(g_1/\tilde{\delta},h)+1)},$$

then g is a good generator.

From (8) and the next lemma it follows that given g, there are at most finitely many squarefree moduli d such that $[g,d]$ is special and that they can be effectively determined.

Lemma 10 *For every $q \in \mathbb{Q}$, there are at most finitely many squarefree values of d such that $\kappa(d) = q$. Moreover, they can be effectively determined.*

Proof. Notice that there is at most one prime p such that $\kappa(p) = q$ and that p can be effectively determined. We proceed by induction. Assume that we know there are at most finitely many effectively determinable squarefree d with $\omega(d) \le s$ such that $\kappa(d) = q$ for every fixed $q \in \mathbb{Q}$, then we will show that there are at most finitely many effectively determinable d with $\omega(d) \le s+1$ such that $\kappa(d) = q$ for every fixed $q \in \mathbb{Q}$. To this end consider the equation $\kappa(p_1 p_2 \cdots p_{s+1}) = q$ with $p_1 < p_2 < p_2 < \ldots < p_{s+1}$. Since the lemma is clearly true when $q \ge 1$, assume that $q < 1$. Let $\tilde{p}$ be the largest prime such that $\kappa(\tilde{p})^{s+1} \le q$. Then $p_1 \le \tilde{p}$, for otherwise $\kappa(p_1 \cdots p_{s+1}) \ge \kappa(p_1)^{s+1} > q$. Now for each $p_1 \le \tilde{p}$, the equation $\kappa(p_2 \cdots p_{s+1}) = q/\kappa(p_1)$ has at most finitely many solutions, which are, moreover, effectively determinable. Thus the induction step is completed. Since $\text{ord}_2(\kappa(p)) \ge 2$ for $p > 2$, it follows that every solution d of $\kappa(d) = q$ satisfies $\omega(d) \le \left[\frac{e}{2}\right] + 1$, where $e = \text{ord}_2(q)$. $\Box$

Let $q \in \mathbb{Q}$. The formulation (8) gives rise to the problem whether or not $q \in \tilde{I}$. The following two lemmas turn out to be of some help:

Lemma 11 *Let q be in $\tilde{I}$, that is in the image of κ on the odd squarefree integers. Write $q = q_1/q_2$, with $(q_1, q_2) = 1$. We have $q < 1$. Also $ord_2(q) > 0$ and $ord_2(q)$ is even. If $ord_2(q) = 2$, then q_1 must be a square. Suppose that $ord_{p_1}(q) \neq 0$, with $p_1 \equiv \pm 2 (\text{mod } 5)$ and p_1 prime. Then $ord_{p_1}(q) > 0$ and $ord_{p_1}(q)$ is even.*

Proof. We leave this to the reader, but like to give a hint. If p_2 is a prime and $p^2 - p - 1 \equiv 0 (\text{mod } p_2)$, then $(2p+1)^2 = 4(p^2 - p - 1) + 5 \equiv 5 (\text{mod } p_2)$. Thus, by quadratic reciprocity, $p_2 = 5$ or $p_2 \equiv \pm 1 (\text{mod } 5)$. $\Box$

Lemma 12 *Suppose that $q < 1$, $q \in \mathbb{Q}$ and $ord_2(q) = 4$. Let p be a prime such that $p \equiv \pm 1 (\text{mod } 5)$ and $ord_p(q)$ is odd and positive. Let p_1 be the smallest prime such that $p_1^2 - p_1 - 1 \equiv 0 (\text{mod } p)$. Let p_2 be the smallest prime such that $p_2 \equiv 1 (\text{mod } p)$. If $\kappa(p_1)\kappa(p_2) > q$, then $q \notin \tilde{I}$.*

These lemmas were implemented by Karim Belabas in PARI and it was found that the only pairs $[g, d]$ with $1 < g_1 < 10^6$ satisfying $(g_1, h) = 1$ that could not be dealt with are those satisfying $g_1 = 7185$ and $(g_1, d) = 479$ or $g_1 = 345729$ and $(g_1, d) = 6779$ or $g_1 = 923329$ and $(g_1, d) = 83939$. We leave it to the interested reader to show that these pairs do not give rise to special pairs with $(g_1, h) = 1$. The following example might be helpful in doing so.

We consider the pairs $[g, d]$ with $g_1 = 1184961$, $(g_1, d) = 394987$ and $(g_1, h) = 1$. In this case (7) is satisfied if and only if there exists an odd integer δ such that $A \prod_{p|\delta}(p^2 - p - 1) = B \prod_{p|\delta}(p-1)^2$, where $A = 2^8 \cdot 3041 \cdot 4639$ and $B = 65831^2$. We will make use of the observation that 102059 is the smallest prime such that $4639 | p^2 - p - 1$ for some prime p and that 22511 is the smallest prime p satisfying $4639 | p - 1$.

Notice that $\omega(\delta) \le 4$. First suppose that $\omega(\delta) = 1$. Then we have to solve $A(p_1^2 - p_1 - 1) = B(p_1 - 1)^2$. Note that $p_1 \equiv 1 (\text{mod } 4639)$. Since $4639^2 \nmid A$ and $p^2 - p - 1 \equiv -1 (\text{mod } 4639)$, this is impossible. Next suppose that $\omega(\delta) = 2$. Then we have to solve

$$A(p_1^2 - p_1 - 1)(p_2^2 - p_2 - 1) = B(p_1 - 1)^2 (p_2 - 1)^2. \quad (9)$$

Without loss of generalization we can assume that $p_1 \equiv 1(\mathrm{mod}\ 4639)$. Thus the right hand side of (9) is divisible by at least 4639^2. Since $4639 \nmid A(p_1^2 - p_1 - 1)$, we must have $4639 | p_2^2 - p_2 - 1$. It follows that $p_1 \geq 102059$ and $p_2 \geq 22511$. Thus $\kappa(p_1)\kappa(p_2) \geq \kappa(102059)\kappa(22511) > A/B$. This contradicts (9). Next suppose that $\omega(\delta) = 3$. Then we have to solve

$$A(p_1^2 - p_1 - 1)(p_2^2 - p_2 - 1)(p_3^2 - p_3 - 1) = B(p_1 - 1)^2(p_2 - 1)^2(p_3 - 1)^2. \tag{10}$$

Since $\kappa(22511)^3 > A/B$, at least one of the primes, say p_1, is less than 22511. We have, without loss of generalization, that $p_2 \equiv 1(\mathrm{mod}\ 4639)$, since $4639^2 \nmid A(p_1^2 - p_1 - 1)$, we find reasoning as in the case $\omega(\delta) = 2$, that $\kappa(p_2)\kappa(p_3) \geq \kappa(102059)\kappa(22511)$. Put $\alpha_1 := \max_{p>2}\{A/(B\kappa(p)) \mid A/B < \kappa(p)\}$. Note that $\alpha_1 < .9896$. The maximum of $A/(B\kappa(p))$ not exceeding 1 occurs for $p = 5$. Thus $\kappa(p_2)\kappa(p_3) \geq \kappa(102059)\kappa(22511) > \alpha_1 \geq A/(B\kappa(p_1))$ and so $\kappa(p_1)\kappa(p_2)\kappa(p_3) > A/B$, contradicting (10).

The pairs with $g_1 < 0$ are taken care of using the following elementary observation:

Lemma 13 *We have $P(\alpha, \beta) \equiv \mu(\alpha) + 2 \pmod 4$, if $\alpha > 0$, α is squarefree and $\alpha \equiv 3(\mathrm{mod}\ 4)$.*

Namely if $g_1 < 0$, then $g_1 = -\tilde{g}_1$ with $\tilde{g}_1 \equiv 3(\mathrm{mod}\ 4)$ and $\tilde{g}_1 > 0$. Then by Lemma 13 it follows that $2 || (P(g_1, h) - \mu(g_1))$. (Note that $P(g_1, h) = P(\tilde{g}_1, h)$.) Thus $\mathrm{ord}_2(Q(g, \tilde{\delta})) \leq 0$. Then, by Lemma 11, $Q(g, \tilde{\delta}) \notin \tilde{I}$. Thus:

Lemma 14 *A pair $[g, d]$ with $g_1 < 0$ is never special.*

Lemma 13 does not seem to generalize to higher 2-powers than 4. It does, however, on imposing $(\alpha, \beta) = 1$.

Lemma 15 *If $\alpha > 0$, α is squarefree, and $(\alpha, \beta) = 1$, then $P(\alpha, \beta) \equiv \mu(\alpha) + 4 \pmod 8$ if $\alpha \equiv 5(\mathrm{mod}\ 8)$ and $P(\alpha, \beta) \equiv \mu(\alpha) + 8 \pmod{16}$ if $\alpha \equiv 9(\mathrm{mod}\ 16)$.*

The latter lemma gives one the final tool to prove:

Theorem 7 *Suppose that $[g, d]$ is an exceptional pair. Then $g_1 > 0$, g_1 is not a prime and $g_1/(g_1, d)$ has an odd number of prime divisors. If $(g_1, h) = 1$, then we have, moreover, $g_1 > 10^6$ and $g_1 \equiv 1(\mathrm{mod}\ 16)$.*

Proof. By Lemma 14 we know that $g_1 > 0$. As we have seen, $|g_1|$ is not a prime and $\mu(|b|) = -1$. Thus the second sentence of the statement follows. Now assume $(g_1, h) = 1$. The numerical work done shows that $g_1 > 10^6$. We know that $g_1 \equiv 1(\mathrm{mod}\ 4)$. Since $\tilde{\delta} > 1$ and $(g_1, h) = 1$, $4 | P(\tilde{\delta}, h)$. From Lemma 15 it follows that $\mathrm{ord}_2(Q(g, \tilde{\delta})) \leq 0$ in case $g_1 \equiv 5(\mathrm{mod}\ 8)$ or $g_1 \equiv 9(\mathrm{mod}\ 16)$. Thus, by Lemma 11, $Q(g, \tilde{\delta}) \notin \tilde{I}$ in these cases. On invoking condition (8), it follows that $g_1 \equiv 1(\mathrm{mod}\ 16)$. □

Sofar we fixed g and then considered the possible d such that $[g, d]$ is an exceptional pair. One can also fix d and try to determine the g such that $[g, d]$ is an exceptional pair. It is not difficult to see that, given d, there is a finite set S_d such that if $[g, d]$ is exceptional, then $g_1 \in S_d$. As remarked before a 2-smooth integer is always a good modulus. Also if d is a good modulus, then $2d$ is a good modulus. A more difficult observation is that if $d \geq 3$ and both d and $d^2 - d - 1$ are prime, then d is a good modulus. Using this and a little bit of computation one finds, for example, that all moduli $d \leq 100$ are good. Thus exceptional pairs, if they exist at all, seem to be sparse at least.

The author thanks K. Belabas for helping him with the numerical work reported on in Section 4. He thanks K. Belabas, T. Kleinjung, F. Lemmermeyer, A. Schinzel and P. Stevenhagen for helpful (e-mail) discussions.

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*, Abh. Math. Sem. Univ. Hamburg 67 (1997), 165-171.

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

[7] A. Reznikov and P. Moree, *Three-manifold subgroup growth, homology of coverings and simplicial volume*, MPI-preprint 171, Bonn, 1996. (To appear in the Asian Journal of Mathematics.)

[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] S. Roman, *Field Theory*, Graduate Texts in Mathematics 158, Springer-Verlag, Berlin, 1995.

[10] 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)