ACTA ARITHMETICA
LXXXIX.1 (1999)

Uniform distribution of primes having a prescribed primitive root

by

PIETER MOREE (Bonn and Amsterdam)

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

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

where $\varphi(d)$ denotes Euler's totient function. In case S is infinite the progressions $a \pmod d$ such that the latter asymptotic equivalence holds 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 [7] has written a nice survey on the state of knowledge regarding the (weak) uniform distribution of many important arithmetical sequences.

In this paper 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 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. 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 q for which $\mathcal{P}_q$ is finite. Assuming GRH, C. Hooley [2] proved in 1967 a quantitative version of Artin's conjecture (Theorem 4 below with $f = 1$ and $g \in G \cap \mathbb{Z}$). In this note we will make use of the following straightforward generalization

1991 *Mathematics Subject Classification*: 11R45, 11A07, 11N69.

of Hooley's result. As usual, μ and ζ_n denote the Möbius function and a primitive root of unity of order n, respectively.

THEOREM 1 [4]. *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

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

the so-called *Artin constant*. For example, taking $f = 1$, $g = 2$ and $M = \mathbb{Q}$ in Theorem 4 yields $\mathcal{P}_2(x) \sim Ax/\log x$. In this paper $\delta(M,g)$ will be computed for M cyclotomic (Theorem 4). This result is then used to compute, on GRH, the set D_g of natural numbers $d \geq 1$ such that $\mathcal{P}_g$ is weakly uniformly distributed mod d. In Theorem 2 simple sets S_g are indicated such that $D_g = S_g$. Theorem 4 allows one to prove that $D_g \subseteq S_g$. The work of H. Lenstra [4] is used to prove that $D_g \supseteq S_g$.

In [9] F. Rodier, in connection with a coding-theoretical result involving Dickson polynomials, made the conjecture that

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

Note that weak uniform distribution mod 28 of $\mathcal{P}_2$ would imply Rodier's conjecture. In [6] 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, on GRH, that the true constant in (2) is $21A/82$. Another coding-theoretical application of primitive roots in arithmetic progressions occurs in the theory of perfect arithmetic codes [5].

In Theorem 2, D_g is computed for $g \in G$. Notice that we can uniquely write $g = g_1 g_2^2$, with g_1 a squarefree integer and $g_2 \in \mathbb{Q}_{>0}$. Let h be the largest integer such that g is an hth power. Notice that $g \in G$ implies that h must be odd.

THEOREM 2 (GRH). *Let $g \in G$, and let h be the largest integer such that g is an hth power. Assume that either $g_1 \neq 21$ or $(h,21) \neq 7$. 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* $g_1 \equiv 1 \pmod 4$;
(ii) $\{1,2,4\}$ *if* $g_1 \equiv 2 \pmod 4$;
(iii) $\{1,2\}$ *if* $g_1 \equiv 3 \pmod 4$.

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 and assume that g is ordinary. Then $\mathcal{P}_g$ is weakly uniformly distributed modulo d if and only if for every squarefree $k \geq 1$, $\mathbb{Q}(\zeta_k, g^{1/k}) \cap \mathbb{Q}(\zeta_d) = \mathbb{Q}$.*

Let g be exceptional and d be of the form $2^\alpha 3^\beta$ with $\beta \geq 1$. It turns out, on GRH, that $\mathcal{P}_g$ is weakly uniformly distributed mod d. On the other hand, there exist k such that $\mathbb{Q}(\zeta_k, g^{1/k}) \cap \mathbb{Q}(\zeta_d) = \mathbb{Q}(\sqrt{-3})$ (cf. the remark following Lemma 7). Thus the requirement "g is ordinary" in Theorem 3 cannot be dropped.

2. The density of primes $p \equiv 1 \pmod f$ 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 $p \equiv 1 \pmod f$ and moreover a prescribed integer g is a 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 $\mathbb{Q}(\zeta_{|a_1|})$ if $a_1 \equiv 1 \pmod 4$ and $\mathbb{Q}(\zeta_{4|a_1|})$ otherwise.*

Lemma 1 can also be phrased as: the smallest cyclotomic field containing $\mathbb{Q}(\sqrt{a})$ is $\mathbb{Q}(\zeta_{|\Delta_a|})$, with Δ_a the discriminant of $\mathbb{Q}(\sqrt{a})$.

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 an hth power. Let Δ denote the discriminant of $\mathbb{Q}(\sqrt{g})$. Suppose that $k \mid r$ 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) *for* k *odd*, $n(k,r)=k_1\varphi(r)$;
(ii) *for* k *even and* $\Delta\nmid r$, $n(k,r)=k_1\varphi(r)$;
(iii) *for* k *even and* $\Delta\,|\,r$, $n(k,r)=k_1\varphi(r)/2$.

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

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

is multiplicative.

Proof. For every multiplicative function g and arbitrary integers $a,b\ge 1$, 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. ∎

THEOREM 4. *Let* $g\in G$, *and let* h *be the largest integer such that* g *is an* h*th power. Let* $f\ge 1$ *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*

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

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. *If* $(f,h)>1$, *then* $\delta(\mathbb{Q}(\zeta_f),g)=0$ *and* $N_{\mathbb{Q}(\zeta_f)}(g;x)$ *is bounded above.*

Next assume that $(f,h)=1$. *Then*

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

if either $g_1\equiv 1\pmod 4$, *or* $g_1\equiv 2\pmod 4$ *and* $8\,|\,f$, *or* $g_1\equiv 3\pmod 4$ *and* $4\,|\,f$. *Otherwise*

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

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

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

P r o o f. We have to evaluate

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

From Lemma 2 it follows that

$$\begin{aligned}\varphi(f)\delta(\mathbb{Q}(\zeta_f),g)&=\sum_{\substack{k=1\\ 2\nmid k}}^{\infty}\frac{\mu(k)}{w(k)}+\sum_{\substack{k=1\\ \Delta\nmid \mathrm{lcm}(2k,f)}}^{\infty}\frac{\mu(2k)}{w(2k)}+2\sum_{\substack{k=1\\ \Delta\mid \mathrm{lcm}(2k,f)}}^{\infty}\frac{\mu(2k)}{w(2k)}\\ &=\sum_{k=1}^{\infty}\frac{\mu(k)}{w(k)}+\sum_{\substack{k=1\\ \Delta\mid \mathrm{lcm}(2k,f)}}^{\infty}\frac{\mu(2k)}{w(2k)}=I_1+I_2.\end{aligned}$$

I claim that

$$I_1=\prod_p\left(1-\frac{1}{w(p)}\right)\quad\text{and}\quad I_2=\frac{\mu(2|b|)}{w(|b|)}\prod_{p\nmid b}\left(1-\frac{1}{w(p)}\right).\tag{5}$$

Indeed, the arithmetic function w is multiplicative by Proposition 1 and thus, by Euler's identity, $I_1=\prod_p(1-1/w(p))$. Further, if b is even, then $I_2=\mu(2|b|)=0$. Next assume that b is odd. Now $\Delta\mid\mathrm{lcm}(2k,f)$ is equivalent to $b\mid 2k/(2k,f)$. Since $(b,(2k,f))=1$ and b is odd, $b\mid 2k/(2k,f)$ is equivalent to $b\mid k$. Thus

$$I_2=\sum_{\substack{k=1\\ b\mid k}}^{\infty}\frac{\mu(2k)}{w(2k)}=\frac{\mu(2|b|)}{w(2|b|)}\sum_{\substack{k=1\\ (k,2b)=1}}^{\infty}\frac{\mu(k)}{w(k)}=\frac{\mu(2|b|)}{w(2|b|)}\prod_{p\nmid 2b}\left(1-\frac{1}{w(p)}\right).\tag{6}$$

Using the fact that b is odd and $w(2)=2$ completes the proof of (5).

Using (5) the proof is now easily completed. We distinguish two subcases: $(f,h)>1$ and $(f,h)=1$.

(i) $(f,h)>1$. Since $g\in G$, h is odd. Since $(b,f)\mid 2$ and h is odd, there is an odd prime p_1 such that $p_1\mid h$, $p_1\mid f$ and $p_1\nmid b$. Since $w(p_1)=1$, it follows that $I_1=I_2=0$ and thus $\delta(\mathbb{Q}(\zeta_f),g)=0$. Let p be a prime with $p\equiv 1\pmod f$ and $p\nmid g$. Then the order of g mod p is bounded above by $(p-1)/q_1$, where q_1 is the smallest prime dividing (f,h). Hence $N_{\mathbb{Q}(\zeta_f)}(g;x)$ is bounded above.

(ii) $(f,h)=1$. Then $w(p)>1$ for every prime p. Adding the product expansions in (5) results, on using the fact that $w(p)>1$, in

$$\delta(\mathbb{Q}(\zeta_f),g)=\frac{1}{\varphi(f)}\left(1+\frac{\mu(2|b|)}{\prod_{p\mid b}(w(p)-1)}\right)\prod_p\left(1-\frac{1}{w(p)}\right).\tag{7}$$

Notice that $\prod_p(1-1/w(p)) = A(f,h)$ and 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 $(b,f)\,|\,2$, the latter identity simplifies to

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

Inserting this in (7) we find

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

On invoking Theorem 1, the proof is easily completed. ∎

Let $g \in G$. From [4, 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 let h be the largest integer such that g is an hth power. Let M be an abelian number field of conductor f. Let $N_M(g)$ denote the set of primes $p \in \mathcal{P}_g$ such that p splits completely in M. Suppose that $(f,h)=1$. Then $\delta(M,g)=0$ if and only if $\sqrt{g} \in M$. Moreover, if $N_M(g)$ is infinite, then $\delta(M,g) > 0$.*

We will deduce Theorem 5 from a result of Lenstra [4, Theorem 4.6], which in this context simplifies to:

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

In addition we will make use of:

LEMMA 3. *Let $\mathbb{Q} \not\subseteq \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\zeta_n)$ be a quadratic field of discriminant Δ_d. Then there exists $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ such that $(\sigma|_{\mathbb{Q}(\zeta_l)}) \neq \mathrm{id}_{\mathbb{Q}(\zeta_l)}$ for every odd prime l dividing n and, moreover, $\sigma(\sqrt{d}) = -\sqrt{d}$.*

Proof. Let $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ with $\sigma_a := \zeta_n^a$ and $(a,n)=1$. It is well known that $\sigma(\sqrt{d}) = \sqrt{d}$ if and only if $(\Delta_d/a) = 1$, where (Δ_d/a) denotes the Kronecker symbol. Thus the problem reduces to showing that there exists $1 \le a \le n$, $(a,n)=1$ with $a \not\equiv 1 \pmod{l}$ for every odd prime l

dividing n and $(\Delta_d/a) = -1$. To prove that such an a exists is left to the reader. (If $\Delta_d < 0$, then $a = n-1$ is such an a.) ∎

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 $l \nmid h$ and l is odd, then $\mathbb{Q}(g^{1/l})$ is not normal and hence $\mathbb{Q}(\zeta_l, g^{1/l}) \not\subseteq M(\zeta_\pi)$. If $l \mid h$, then $\mathbb{Q}(\zeta_l, g^{1/l}) = \mathbb{Q}(\zeta_l) \subseteq M(\zeta_\pi)$. Thus the l such that $\mathbb{Q}(\zeta_l, g^{1/l}) \subseteq M(\zeta_\pi)$ are precisely the prime divisors of π and possibly 2. The (easier) case where 2 does not occur is left to the reader, so we may assume that $\sqrt{g} \in M(\zeta_\pi)$. Notice that we are done if we show that if $\sqrt{g} \notin M$, then there exists $\sigma \in \mathrm{Gal}(M(\zeta_\pi)/\mathbb{Q})$ such that $\sigma(\sqrt{g}) = -\sqrt{g}$ and $(\sigma|_{\mathbb{Q}(\zeta_l)}) \neq \mathrm{id}_{\mathbb{Q}(\zeta_l)}$ for every prime divisor l of π.

Since by assumption $\sqrt{g} \in M(\zeta_\pi)$ and $M \subseteq \mathbb{Q}(\zeta_f)$, $\sqrt{g} \in \mathbb{Q}(\zeta_f, \zeta_\pi)$. Put $(\pi, \Delta)^* = (-1)^{((\pi,\Delta)-1)/2}(\pi, \Delta)$. As π is odd, we see that $\sqrt{(\pi,\Delta)^*} \in \mathbb{Q}(\zeta_\pi)$ and, moreover, $\sqrt{(\pi,\Delta)^*\Delta} \in \mathbb{Q}(\zeta_f)$. We distinguish two cases:

(i) $[\mathbb{Q}(\sqrt{(\pi,\Delta)^*}) : \mathbb{Q}] = 2$. Let $\sigma_1 = \mathrm{id} \in \mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q})$. Let σ_2 be an automorphism whose existence is asserted in Lemma 3 (with $n = \pi$ and $d = (\pi,\Delta)^*$). Since by assumption $(f, h) = 1$, $\mathbb{Q}(\zeta_f)$ and $\mathbb{Q}(\zeta_\pi)$ are linearly disjoint and hence the automorphisms σ_1 and σ_2 can be lifted to an automorphism of $\mathbb{Q}(\zeta_f, \zeta_\pi)$. Take its restriction to $M(\zeta_\pi)$. This automorphism has all the required properties.

(ii) $[\mathbb{Q}(\sqrt{(\pi,\Delta)^*}) : \mathbb{Q}] = 1$. In this case $\sqrt{g} \in \mathbb{Q}(\zeta_f)$. Let $\sigma_1 \neq \mathrm{id}$ be the automorphism of $M(\sqrt{g})$ such that $(\sigma_1|_M) = \mathrm{id}|_M$. Since by assumption $\sqrt{g} \notin M$, σ_1 exists. Let $\sigma_2 \in \mathrm{Gal}(\mathbb{Q}(\zeta_\pi)/\mathbb{Q})$ be defined by $\sigma_2(\zeta_\pi) = \zeta_\pi^{-1}$. Since $M(\sqrt{g})$ and $\mathbb{Q}(\zeta_\pi)$ are linearly disjoint, σ_1 and σ_2 can be lifted to an automorphism of $\mathrm{Gal}(M(\zeta_\pi)/\mathbb{Q})$. Notice that this automorphism has all the required properties.

The assertion regarding $N_M(g)$ is now easily deduced on using the latter part of Theorem 6. ∎

We demonstrate Theorem 5 by determining the set $\mathcal{L}$ of odd primes l such that there are infinitely many primes p satisfying $p \equiv \pm 1 \pmod{l}$ with l a primitive root mod p. Then we have to put $M = \mathbb{Q}(\zeta_l + \zeta_l^{-1})$ and $g = l$ in Theorem 5. Since $\sqrt{l} \in \mathbb{R}$ and M is the maximal real subfield of $\mathbb{Q}(\zeta_l)$, we find that $\sqrt{l} \in M$ if and only if $\sqrt{l} \in \mathbb{Q}(\zeta_l)$. Thus, using Lemma 1, we see that on GRH, $\mathcal{L} = \{l : l \equiv 3 \pmod 4\}$. Unconditionally it can be shown [8, Theorem 3.2] that $\mathcal{L}$ equals $\{l : l \equiv 3 \pmod 4\}$ with at most two primes excluded. The fact that $\mathcal{L}$ is non-empty is used in A. Reznikov's [8] proof of a weaker version of a conjecture of Lubotzky and Shalev on three-manifolds.

3. Proof of the main result. In this section Theorem 2 will be proved. First we carry out some preparations.

The next two lemmas are well known (cf. [3]).

LEMMA 4. *Let M be a number field, $\kappa \in M$ and let $n \geq 1$ be an odd integer. If $[M(\zeta_n, \kappa^{1/n}) : M] = n\varphi(n)$, then $M(\zeta_n) : M$ is the maximal abelian subextension of $M(\zeta_n, \kappa^{1/n}) : M$.*

Proof. Let

$$\mathcal{M}_n = \left\{ \begin{pmatrix} 1 & 0 \\ r & s \end{pmatrix} : r \in \mathbb{Z}/n\mathbb{Z},\ s \in (\mathbb{Z}/n\mathbb{Z})^* \right\}.$$

One easily sees that commutators of $\mathcal{M}_n$ are of the form $\left(\begin{smallmatrix} 1 & 0 \\ \star & 1 \end{smallmatrix}\right)$. On noting that the commutator of $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ equals $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, it is seen that $\mathcal{M}_n'$, the commutator subgroup of $\mathcal{M}_n$, equals $\left\{\left(\begin{smallmatrix} 1 & 0 \\ r & 1 \end{smallmatrix}\right) : r \in \mathbb{Z}/n\mathbb{Z}\right\}$. It is enough to show that if the condition of the lemma is satisfied, then $\mathrm{Gal}(M(\zeta_n, \kappa^{1/n}) : M) \cong \mathcal{M}_n$. For then the Galois group of the maximal abelian subextension of $M(\zeta_n, \kappa^{1/n}) : M$ is isomorphic to $\mathcal{M}_n/\mathcal{M}_n' \cong (\mathbb{Z}/n\mathbb{Z})^*$. Since the maximal abelian subextension of $M(\zeta_n, \kappa^{1/n}) : M$ contains $M(\zeta_n) : M$ and the condition of the lemma implies that the latter has Galois group $(\mathbb{Z}/n\mathbb{Z})^*$, we are done.

Let α be a root of $x^n - \kappa$. For any $\sigma \in \mathrm{Gal}(M(\zeta_n, \kappa^{1/n}) : M)$, there exist $l(\sigma) \in (\mathbb{Z}/n\mathbb{Z})$ and $m(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^*$, such that $\sigma(\alpha) = \zeta_n^{l(\sigma)}\alpha$ and $\sigma(\zeta_n) = \zeta_n^{m(\sigma)}$. Now define a map $\psi \mapsto \left(\begin{smallmatrix} 1 & 0 \\ l(\sigma) & m(\sigma) \end{smallmatrix}\right)$. One checks that it is a monomorphism of $\mathrm{Gal}(M(\zeta_n, \kappa^{1/n}) : M)$ into $\mathcal{M}_n$. Since $|\mathcal{M}_n| = n\varphi(n)$ and, by assumption, $|\mathrm{Gal}(M(\zeta_n, \kappa^{1/n}) : M)| = n\varphi(n)$, ψ is actually an isomorphism. ■

LEMMA 5. *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 Lemmas 2 and 4, $\mathbb{Q}(\zeta_k)$ 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 $M = \mathbb{Q}(\sqrt{\gamma_1})$, $\kappa = \sqrt{\gamma_1}$ and $n = k/2$ in Lemma 4, we find, on using Lemma 2, that the maximal abelian subextension of $\mathbb{Q}(\zeta_n, \kappa^{1/n}) : \mathbb{Q}(\sqrt{\gamma_1})$ equals $\mathbb{Q}(\zeta_n, \sqrt{\gamma_1}) = \mathbb{Q}(\zeta_k, \sqrt{g})$. Since $\mathbb{Q}(\zeta_k, \sqrt{g}) : \mathbb{Q}$ is abelian and

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

we are done.

(iii) k is even and $\sqrt{\gamma_1} \in \mathbb{Q}(\zeta_k)$. From 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 6. *Let $g \in G$. If $g_1 \equiv 1 \pmod 4$ 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 5. 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 $k \equiv 2 \pmod 4$ 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, every subfield of degree > 1 of $\mathbb{Q}(\zeta_{2^n})$ is ramified at 2. ∎

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

LEMMA 7. *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 $\mathbb{Q}(\zeta_k, g^{1/k}) \cap \mathbb{Q}(\zeta_d) \subseteq \mathbb{Q}(\sqrt{-3})$.*

Proof. Using Lemma 5 it is seen that $\mathbb{Q}(\zeta_k, g^{1/k}) \cap \mathbb{Q}(\zeta_d) \subseteq \mathbb{Q}(\zeta_k, \sqrt{21}) \cap \mathbb{Q}(\zeta_d)$. Let $3^\alpha \| d$. Notice that $\mathbb{Q}(\zeta_k, \sqrt{g})$ is not ramified at 2 (cf. the proof of the previous lemma). Thus $\mathbb{Q}(\zeta_k, \sqrt{21}) \cap \mathbb{Q}(\zeta_d) \subseteq \mathbb{Q}(\zeta_k, \sqrt{21}) \cap \mathbb{Q}(\zeta_{3^\alpha})$. Now

$$\mathbb{Q}(\zeta_k, \sqrt{21}) \cap \mathbb{Q}(\zeta_{3^\alpha}) \subseteq \mathbb{Q}(\zeta_{\mathrm{lcm}(k,21)}) \cap \mathbb{Q}(\zeta_{3^\alpha}) = \mathbb{Q}(\zeta_3),$$

where the latter equality follows on noticing that $(\mathrm{lcm}(k, 21), 3^\alpha) = 3$. ∎

REMARK. Actually under the conditions of Lemma 7, we have $\mathbb{Q}(\zeta_k, g^{1/k}) \cap \mathbb{Q}(\zeta_d) = \mathbb{Q}(\sqrt{-3})$ if $3 \mid k$ or $14 \mid k$ and $\mathbb{Q}$ otherwise, but this will not be needed in the sequel.

LEMMA 8. *Let $g \in G$ and l be an odd prime. Then $\delta(\mathbb{Q}(\zeta_l), g) = \delta(\mathbb{Q}, g)/\varphi(l)$ if and only if g is exceptional and $l = 3$.*

COROLLARY 1 (GRH). *Let $g \in G$ and l be an odd prime. Then $\mathcal{P}_g$ is weakly uniformly distributed mod l if and only if g is exceptional and $l = 3$.*

Proof (of Lemma 8). Put $P(\alpha, \beta) = \prod_{p \mid \alpha,\, p \mid \beta} (p-2) \prod_{p \mid \alpha,\, p \nmid \beta} (p^2 - p - 1)$.

$\Leftarrow$. By Theorem 4.

$\Rightarrow$. Notice that $l \nmid h$, for otherwise, by Theorem 4, $\delta(\mathbb{Q}(\zeta_l), g) = 0$, whereas $\delta(\mathbb{Q}, g) > 0$. Notice also that $g_1 \equiv 1 \pmod 4$, for otherwise $\delta(\mathbb{Q}(\zeta_l), g) = \delta(\mathbb{Q}, g)/\varphi(l)$ implies, by Theorem 4, that $A(l, h) = A(1, h)$ and hence $1 - (l-2)/(l^2 - l - 1) = 1$, which is impossible. Then, since $g_1 \equiv 1 \pmod 4$, $l \nmid h$ and $\Delta = g_1$, the equality $\delta(\mathbb{Q}(\zeta_l), g) = \delta(\mathbb{Q}, g)/\varphi(l)$ implies, by Theorem 4,

$$\left(1 - \frac{\mu(|g_1|)}{P(g_1, h)}\right) = \left(1 - \frac{l-2}{l^2 - l - 1}\right)\left(1 - \frac{\mu(|b|)}{P(b, h)}\right). \tag{8}$$

Now l must divide g_1, for otherwise $b = g_1$ and hence $1-(l-2)/(l^2-l-1) = 1$, which is impossible. Hence $b = g_1/l$ and thus (8) becomes

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

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

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 $d \in D_g$ and δ divides d, then $\delta \in D_g$.

First consider the case where g is ordinary. Then this observation together with Corollary 1 shows that $D_g \subseteq \{2^n : n \geq 0\}$. Suppose that $g_1 \equiv 3 \pmod 4$. Then Theorem 4 shows that $\mathcal{P}_g$ is not weakly uniformly distributed mod 4. Thus in this case $D_g = \{1,2\}$. If $g_1 \not\equiv 3 \pmod 4$, then it is easy to see, by Theorem 4 again, that $4 \in D_g$. If $g_1 \equiv 2 \pmod 4$ then Theorem 4 again yields that $\mathcal{P}_g$ is not weakly uniformly distributed mod 8. Thus in this case $D_g = \{1,2,4\}$. Finally assume that $g_1 \equiv 1 \pmod 4$. 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 [4], 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.

Let a and d be coprime. The set of primes p such that $p \equiv a \pmod d$, $p \nmid g$, and g is a primitive root mod p, equals $M = M(\mathbb{Q}, \mathbb{Q}(\zeta_d), \sigma_a, \langle g\rangle, 1)$, where we used Lenstra's notation. Here σ_a denotes the automorphism of $\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ determined by $\sigma_a(\zeta_d) = \zeta_d^a$. Under GRH the natural density δ_a, of the set M is, by [4, (2.15)], equal to

$$\delta_a = \sum_{k=1}^{\infty} \frac{\mu(k)c_a(k)}{[\mathbb{Q}(\zeta_d, \zeta_k, g^{1/k}) : \mathbb{Q}]}, \tag{9}$$

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. In case $g_1 \equiv 1 \pmod 4$ and $d = 2^n$, by Lemma 6 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), yield that $\mathcal{P}_g$ is weakly uniformly distributed mod 2^n.

It remains to deal with the case where g is exceptional. By Corollary 1, 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 condition is also sufficient. The analysis of the case $g_1 \equiv 1 \pmod 4$ 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 $(a,6)=1$. By Lemma 7 it follows that $\mathbb{Q}(\zeta_k, g^{1/k}) \cap \mathbb{Q}(\zeta_d) \subseteq \mathbb{Q}(\sqrt{-3})$ for squarefree k. Thus, by (9), there exist $\widetilde{\delta}_1$ and $\widetilde{\delta}_{-1}$ such that $\delta_a = \widetilde{\delta}_1$ if σ_a fixes $\mathbb{Q}(\sqrt{-3})$ (that is, if $a \equiv 1 \pmod 3$) and $\delta_a = \widetilde{\delta}_{-1}$ otherwise. Since, by Corollary 1, $\mathcal{P}_g$ is weakly uniformly distributed mod 3, we see that

$$\sum_{\substack{1\le a\le d,\ (a,d)=1\\ a\equiv 1 \pmod 3}} \delta_a = \sum_{\substack{1\le a\le d,\ (a,d)=1\\ a\equiv -1 \pmod 3}} \delta_a,$$

that is, $\varphi(d)\widetilde{\delta}_1/2 = \varphi(d)\widetilde{\delta}_{-1}/2$. Since $\delta_1 > 0$ (by Theorem 5 for example), it follows that $\mathcal{P}_g$ is weakly uniformly distributed mod d. ∎

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 $g_1 \equiv 1 \pmod 4$ to g satisfying $g_1 \not\equiv 1 \pmod 4$. 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 6 must be false in this case. Indeed, if $g_1 \equiv 3 \pmod 4$, then $\mathbb{Q}(\zeta_{2|g_1|}, g^{1/(2|g_1|)}) \cap \mathbb{Q}(\zeta_{2^n}) \supseteq \mathbb{Q}(i)$ for $n \ge 2$. If $g_1 \equiv 2 \pmod 4$ then, for $n \ge 3$, $\mathbb{Q}(\zeta_{|g_1|}, g^{1/|g_1|}) \cap \mathbb{Q}(\zeta_{2^n})$ contains $\mathbb{Q}(\sqrt{2})$ (respectively $\mathbb{Q}(\sqrt{-2})$) if $g_1/2 \equiv 1 \pmod 4$ (respectively $g_1/2 \equiv 3 \pmod 4$).

The next lemma together with Theorem 2 immediately implies Theorem 3.

Lemma 9. *Let $d \ge 1$ 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 $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\zeta_p, g^{1/p}) \cap \mathbb{Q}(\zeta_d)$ and thus $d = 2^n$ for some $n \ge 0$. Suppose that $g_1 \equiv 2 \pmod 4$. We have to show that $n \le 2$. So assume that $n \ge 3$. 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 $g_1/2 \equiv 1 \pmod 4$ (respectively $g_1/2 \equiv 3 \pmod 4$). Finally suppose that $g_1 \equiv 3 \pmod 4$. We have to show that $n \le 1$. So assume that $n \ge 2$. 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 $g_1 \equiv 1 \pmod 4$, then this follows by Lemma 6. The other cases, except $g_1 \equiv 2 \pmod 4$ and $d = 4$, are trivial. It remains to show that $i \notin \mathbb{Q}(\zeta_k, g^{1/k})$ for k squarefree and $g_1 \equiv 2 \pmod 4$. A way of showing that $i \notin \mathbb{Q}(\zeta_k, g^{1/k})$ is to show that $[\mathbb{Q}(\zeta_{\mathrm{lcm}(4,k)}, g^{1/k}) : \mathbb{Q}] = 2[\mathbb{Q}(\zeta_k, g^{1/k}) : \mathbb{Q}]$. This now follows by computing these degrees using Lemma 2. ∎

4. Conclusion. Let $g \in G$ and assume GRH. We have seen that to a large extent the equidistribution of the primes of $\mathcal{P}_g$ over the residue classes mod d can be understood already from knowing whether or not the progression $1 \pmod d$ gets its fair share of primes from $\mathcal{P}_g$. From Lemma 8 and Corollary 1, one sees that in case d is an odd prime it is even true that the progression $1 \pmod d$ gets its fair share if and only if all primitive progressions get their fair share. A question that thus naturally arises is whether this holds true for arbitrary d (if so this would be rather surprising). Despite a considerable computational effort (together with Karim Belabas), I was not able to find a d for which this is false. On the other hand, I obtained only partial non-existence results for such d.

The author thanks K. Belabas, T. Kleinjung, F. Lemmermeyer, A. Schinzel and P. Stevenhagen for helpful (e-mail) discussions and the referee for his comments (which led to a shortening of some of the proofs). This research was carried out at the Max-Planck-Institut in Bonn, the pleasant research atmosphere of which is gratefully acknowledged.

References

[1] R. Heath-Brown, *A remark on Artin's conjecture*, Quart. J. Math. Oxford Ser. (2) 37 (1986), 27–38.

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

[3] E. T. Jacobson and W. Y. Vélez, *The Galois group of a radical extension of the rationals*, Manuscripta Math. 67 (1990), 271–284.

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

[5] —, *Perfect arithmetic codes*, Sém. Delange–Pisot–Poitou, 19e année 1978/79, Théorie des nombres, Fasc. 1, Exp. 15, 14 pp.

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

[7] W. Narkiewicz, *Uniform Distribution of Sequences of Integers in Residue Classes*, Lecture Notes in Math. 1087, Springer, 1984.

[8] A. Reznikov and P. Moree, *Three-manifold subgroup growth, homology of coverings and simplicial volume*, Asian J. Math. 1 (1997), 764–768.

[9] F. Rodier, *Estimation asymptotique de la distance minimale du dual des codes BCH et polynômes de Dickson*, Discrete Math. 149 (1996), 205–221.
[10] E. Weiss, *Algebraic Number Theory*, New York Univ. Press, New York, 1963.

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

Present address:
Faculteit WINS
Universiteit van Amsterdam
Plantage Muidergracht 24
1018 TV Amsterdam, The Netherlands
E-mail: moree@wins.uva.nl

Received on 7.4.1997
and in revised form on 3.12.1998 (3160)