On some sums connected with primitive roots

Pieter Moree

Abstract

Let g be an integer not equal to -1 or a square. Let $\pi_g(x)$ denote the number of primes $p \le x$ such that g is a primitive root modulo p. Let φ denote Euler's totient. A naive heuristic reasoning suggests that asymptotically $\sum_{p\le x}\varphi(p-1)/(p-1) \sim \pi_g(x)$. Under GRH, the Generalized Riemann Hypothesis, this turns out to be false in general. A slightly less naive heuristic reasoning suggests a modification of this, namely

$$2\sum_{\substack{p\le x,\ (g/p)=-1\\ (h,p-1)=1}} \frac{\varphi(p-1)}{p-1} \sim \pi_g(x),$$

where h is the largest integer such that g is an hth power of an integer. We show, under GRH, that this asymptotic equivalence indeed holds true.

1 Introduction

Let p be a prime. Let $\mathbb{F}_p$ denote the finite field with p elements. Let $\mathbb{F}_p^*$ denote its multiplicative group. This group is cyclic. Let γ be a generator. Every element can be uniquely written as γ^α, with $1 \le \alpha \le p-1$. Those satisfying $(\alpha, p-1) = 1$ are generators, hence there are $\varphi(p-1)$ generators. Let g be an integer. This integer is said to be a primitive root modulo p if it generates $\mathbb{F}_p^*$. A result of Elliott [1, Theorem 1] suggests that the primitive roots mod p are randomly distributed over the integers $1, \cdots, p-1$. If one furthermore assumes that the event 'g is a primitive root mod p_1' is independent from the event 'g is a primitive root mod p_2', for distinct primes p_1 and p_2, then it seems reasonable to expect that

$$\sum_{p\le x} \frac{\varphi(p-1)}{p-1} \sim \pi_g(x),\ \ x \to \infty, \tag{1}$$

where $\pi_g(x)$ denotes the number of primes $p \le x$ such that g is a primitive root modulo p. Under GRH it can be shown that (1) is false in general. However, it turns out that something like (1) is true indeed, namely Theorem 5 below. Establishing Theorem 5, in a motivated way, is the purpose of this note. We start out by recalling some results on $\pi_g(x)$.

2 On the Artin primitive root conjecture

Let G denote the set of integers unequal to -1 or a square. It was conjectured by Emil Artin in 1927 that if $g \in G$, then $\pi_g(x) \to \infty$ as $x \to \infty$. This conjecture is now known as the Artin primitive root conjecture. Clearly if $g \notin G$, then there are only finitely many primes p such that g is a primitive root. Up to date there is no integer g known for which Artin's conjecture has been proved to be true. However, if one assumes the Generalized Riemann Hypothesis the situation is very different.

Theorem 1 [2]. *Let g be an integer that is not equal to -1 or a perfect square. Let h denote the largest integer such that g is an hth power. Let Δ denote the discriminant of the quadratic number field $\mathbb{Q}(\sqrt{g})$. Let μ denote the Möbius function. Put*

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

and

$$A(\Delta, h) = A(h) \left(1 - \mu(\Delta) \prod_{p|\Delta,\ p|h} \frac{1}{p-2} \prod_{p|\Delta,\ p\nmid h} \frac{1}{p^2-p-1}\right).$$

Assume GRH. Then

$$\pi_g(x) = A(\Delta, h)\frac{x}{\log x} + O_g\left(\frac{x \log\log x}{\log^2 x}\right).$$

Notice that the conditions of the theorem ensure that $A(\Delta, h) > 0$. Hence, under GRH, the Artin primitive root conjecture is true. The constant $A(1)$ (≈ 0.373956) is called the Artin constant and is usually denoted by A. Note that g can be uniquely written as $g_1 g_2^2$, with g_1 and g_2 integers and g_1 squarefree. Now $\Delta = g_1$ if $g_1 \equiv 1 (\mathrm{mod}\ 4)$ and $\Delta = 4g_1$ otherwise. In particular it follows that if $g_1 \not\equiv 1(\mathrm{mod}\ 4)$, then $A(\Delta, h) = A(h)$.

3 A first attempt at matching with $\pi_g(x)$

The sum in the l.h.s. of (1) is easily evaluated on using the Siegel-Walfisz theorem, which for the convenience of the reader we recall below. It involves $\pi(x; k, l)$; the number of primes $p \le x$ such that $p \equiv l (\mathrm{mod}\ k)$. Recall that $\mathrm{Li}(x) = \int_2^x dt/\log t$, is the logarithmic integral.

Lemma 1 [7, Satz 4.8.3]. *Let $C > 0$ be arbitrary. Then*

$$\pi(x; k, l) = \frac{\mathrm{Li}(x)}{\varphi(k)} + O(xe^{-c_1\sqrt{\log x}}),$$

uniformly for $1 \le k \le \log^C x$, $(l, k) = 1$, where the constants depend at most on C.

Theorem 2 *Let $C > 0$ be arbitrary. Then*

$$\sum_{p\le x}\frac{\varphi(p-1)}{p-1} = A\ \mathrm{Li}(x) + O_C\left(\frac{x}{\log^C x}\right). \tag{2}$$

Proof. We have $\varphi(n)/n = \prod_{p|n}(p-1)/p = \sum_{d|n}\mu(d)/d$. Thus

$$\sum_{p\le x}\frac{\varphi(p-1)}{p-1} = \sum_{p\le x}\sum_{d|p-1}\frac{\mu(d)}{d} = \sum_{d\le x}\frac{\mu(d)}{d}\pi(x;d,1).$$

Now write

$$\begin{aligned}\sum_{d\le x}\frac{\mu(d)}{d}\pi(x;d,1) &= \sum_{d\le \log^C x}\frac{\mu(d)}{d}\pi(x;d,1) + \sum_{\log^C x<d\le x}\frac{\mu(d)}{d}\pi(x;d,1)\\ &= S_1+S_2,\end{aligned}$$

say. In order to estimate S_1, we invoke Lemma 1. This gives

$$S_1 = \mathrm{Li}(x)\sum_{d\le\log^C x}\frac{\mu(d)}{d\varphi(d)} + O_C\left(\frac{x}{\log^C x}\right).$$

Now

$$\sum_{d\le\log^C x}\frac{\mu(d)}{d\varphi(d)} = \sum_{d=1}^{\infty}\frac{\mu(d)}{d\varphi(d)} + O\left(\sum_{d>\log^C x}\frac{1}{d\varphi(d)}\right).$$

The sum $\sum_{d=1}^{\infty}\mu(d)/d\varphi(d)$ is easily seen to be absolutely convergent. Since, moreover, $\mu/d\varphi$ is multiplicative, it follows by the Euler product identity that

$$\sum_{d=1}^{\infty}\frac{\mu(d)}{d\varphi(d)} = \prod_p\left(1-\frac{1}{p(p-1)}\right) = A.$$

We have $d/\varphi(d) = \prod_{p|d}(1-p^{-1})^{-1} \le \prod_{p\le d}(1-p^{-1})^{-1} \ll \log d$, using Mertens' formula. Thus

$$\sum_{d>\log^C x}\frac{1}{d\varphi(d)} \ll \sum_{d>\log^C x}\frac{\log d}{d^2} \ll \frac{C\log\log x}{\log^C x}.$$

(Actually $\sum_{d>\log^C x}1/d\varphi(d)\sim c_2\log^{-C}x$, for some absolute constant c_2, this can be shown by reasoning as in Landau [4], for example.) The trivial estimate $\pi(x;d,1)<x/d$, leads to $S_2 = O(x\log^{-C}x)$. On putting everything together, the result follows. □

On comparing Theorem 2 with Theorem 1 we see that, on GRH, (1) is false in general. However, it is still true for 2/3th of all squarefree integers g. Some knowledge of the history of the Artin primitive root conjecture suggests a way to modify the sum in (1). We recall a bit of this history in the next section.

4 Second attempt at matching with $\pi_g(x)$

In a discussion with Helmut Hasse, Artin formulated a quantitative version of his conjecture, namely that $\pi_g(x) \sim A\pi(x)$. Well into the 50's this was believed to be true, until numerical computations of D.H. Lehmer showed a dismatch in some cases. It was then realized that on the quadratic level things can go awry. Using algebraic number theory it can be shown that g is a primitive root mod p if and only if g does not split completely in any of the fields $\mathbb{Q}(\zeta_q, g^{1/q})$, with q prime, where $\zeta_q = \exp(2\pi i/q)$. By the Kronecker density theorem (see Lemma 4), a special case of the celebrated Chebotarev density theorem, the density of primes p such that p splits completely in $\mathbb{Q}(\zeta_q, g^{1/q})$ is seen to be equal to $[\mathbb{Q}(\zeta_q, g^{1/q}) : \mathbb{Q}]^{-1}$. Assuming that these infinitely many conditions are independent, one would expect the density of primes such that g is primitive to be

$$\prod_q \left(1 - \frac{1}{[\mathbb{Q}(\zeta_q, g^{1/q}) : \mathbb{Q}]}\right).$$

If g is not an hth power for any $h \geq 2$, this constant equals the Artin constant. The point is now that these conditions are not always independent. Let us consider $g = 5$. Then if p does not split completely in $\mathbb{Q}(\zeta_2, \sqrt{5})$ it also does not split completely in $\mathbb{Q}(\zeta_5, 5^{1/5})$. Assuming there are no further dependencies, one would thus expect a density of $\prod_{p\nmid 5}(1 - 1/p(p-1)) = 20A/19$. By Hooley's theorem this is indeed true on GRH. For general g it is true that dependencies only exist on the quadratic level. This has to do with the fact that the maximal abelian subextension of $\mathbb{Q}(\zeta_k, g^{1/k})$ is contained in $\mathbb{Q}(\zeta_k, \sqrt{g})$. It thus is natural to consider a quadratic modification of the sum in (1). To this end note that if the Legendre symbol of g over p, (g/p), equals 1, then g is not a primitive root mod p. On the other hand if $(g/p) = -1$, then g must belong to one of the $(p-1)/2$ non-squares mod p. The 'probability' then that it is primitive is $2\varphi(p-1)/(p-1)$. This suggests to consider the sum $2\sum_{p\leq x,\ (g/p)=-1} \varphi(p-1)/(p-1)$. The next result gives an evaluation of this sum.

Theorem 3 *Let $C > 0$ be arbitrary. Let $g \in \mathbb{Z}$ be not a square. Let Δ denote the discriminant of the number field $\mathbb{Q}(\sqrt{g})$. Then*

$$2\sum_{\substack{p\leq x\\ (\frac{g}{p})=-1}} \frac{\varphi(p-1)}{p-1} = A\left(1 - \frac{\mu(\Delta)}{\prod_{p|\Delta}(p^2-p-1)}\right)\mathrm{Li}(x) + O_{C,\,g}\left(\frac{x}{\log^C x}\right). \qquad (3)$$

Proof. Proceeding as in the proof of Theorem 2, we find that the sum equals

$$2\sum_{d\leq x}\frac{\mu(d)}{d}\pi(x;d,1) - 2\sum_{\substack{p\leq x\\ (g/p)=0}}\frac{\varphi(p-1)}{p-1} - 2\sum_{d\leq x}\frac{\mu(d)}{d}\sum_{\substack{p\leq x,\ (g/p)=1\\ p\equiv 1 (\mathrm{mod}\ d)}} 1 = S_3 - S_4 - S_5,$$

say. Now S_3 is evaluated in Theorem 2 and $S_4 = O(1)$. Consider the inner sum in S_5. By quadratic reciprocity the condition $(g/p) = 1$, is equivalent with p being a member of any of a certain collection of arithmetic progressions modulo $4g$. Thus using Lemma 1 we see that the inner sum of S_5 equals

$$\frac{\mathrm{Li}(x)}{f(d,g)} + O(xe^{-c_1\sqrt{\log x}}),$$

uniformly for $1 \leq 4dg \leq \log^C x$, where the constants depend at most on C and g, for some $f(d,g)$. On the other hand, the inner sum of S_5 equals, with at most finitely many exceptions, the number of primes p that split completely in $\mathbb{Q}(\zeta_d, \sqrt{g})$. By the Kronecker density theorem it then follows that $f(d,g) = [\mathbb{Q}(\zeta_d, \sqrt{g}) : \mathbb{Q}]$. Proceeding as in the proof of Theorem 2, we see that (3) holds true with constant

$$h(g) = 2A - 2\sum_{d=1}^{\infty} \frac{\mu(d)}{d[\mathbb{Q}(\zeta_d, \sqrt{g}) : \mathbb{Q}]}.$$

Using the well-known fact that $\sqrt{g} \in \mathbb{Q}(\zeta_d)$ if and only if $\Delta | d$, we find that

$$\begin{aligned} h(g) &= 2A - 2\sum_{\substack{d=1 \\ \Delta | d}}^{\infty} \frac{\mu(d)}{d\varphi(d)} - \sum_{\substack{d=1 \\ \Delta \nmid d}}^{\infty} \frac{\mu(d)}{d\varphi(d)} = A - \sum_{\substack{d=1 \\ \Delta | d}}^{\infty} \frac{\mu(d)}{d\varphi(d)} \\ &= A - \frac{\mu(\Delta)}{\Delta\varphi(\Delta)} \sum_{\substack{d=1 \\ (d,\Delta)=1}}^{\infty} \frac{\mu(d)}{d\varphi(d)} = A\left(1 - \frac{\mu(\Delta)}{\prod_{p|\Delta}(p^2-p-1)}\right). \end{aligned}$$

Thus the proof is completed. □

5 Third attempt at matching with $\pi_g(x)$

Comparison of Theorem 1 and Theorem 3 shows that the sum in (3) is not always asymptotically equal, under GRH, to $\pi_g(x)$. However, in contrast with the sum in (2), it is asymptotically equal provided that $h = 1$. Thus it represents a definitive improvement over the sum in (1).

Notice that if $g = g_1^h$, then g cannot be a primitive root for those primes p for which $(p-1, h) > 1$. This suggests to add the restriction $(h, p-1) = 1$ to the sum in (3). We will prove:

Theorem 4 *Let $C > 0$ be arbitrary. Let $g \in G$. Let Δ denote the discriminant of $\mathbb{Q}(\sqrt{g})$. Then*

$$2 \sum_{\substack{p \leq x \\ (\frac{g}{p})=-1 \\ (h,p-1)=1}} \frac{\varphi(p-1)}{p-1} = A(\Delta, h)\ \mathrm{Li}(x) + O_{C,\ g}\left(\frac{x}{\log^C x}\right). \quad (4)$$

Combination of Theorem 1 and Theorem 4 gives the main result of this note:

Theorem 5 (GRH). *Let $g \in G$. Then*

$$2 \sum_{\substack{p \leq x \\ (\frac{g}{p})=-1 \\ (h,p-1)=1}} \frac{\varphi(p-1)}{p-1} = \pi_g(x) + O_g\left(\frac{x \log\log x}{\log^2 x}\right). \quad (5)$$

In the proof of Theorem 4 the following lemma will be used.

Lemma 2 *Let $h>1$ be odd and $C>0$ be arbitrary. Then*

$$\sum_{\substack{p\le x\\ (h,p-1)=1}} \frac{\varphi(p-1)}{p-1} = A(h)\ \mathrm{Li}(x) + O_{C,\ h}\left(\frac{x}{\log^C x}\right). \tag{6}$$

Proof. Consider $N_{d,h}(x)$, the number of primes $p\le x$ such that $p\equiv 1(\mathrm{mod}\ d)$ and $(h,p-1)=1$. If $(d,h)>1$, then $N_{d,h}(x)=0$. Assume $(d,h)=1$. Using that $\sum_{\delta|n}\mu(\delta)=1$ if n is 1 and zero otherwise, we find that $N_{d,h}(x)=\sum_{\delta|h}\mu(\delta)\pi(x;d\delta,1)$. Proceeding as in the proof of Theorem 2, we find that (6) holds with constant

$$\sum_{\substack{d=1\\ (d,h)=1}}^{\infty} \frac{\mu(d)}{d\varphi(d)}\sum_{\delta|h}\frac{\mu(\delta)}{\varphi(\delta)}.$$

But this constant equals $A(h)$. □

Proof of Theorem 4. Using Lemma 2, the proof reduces to showing that

$$2\sum_{\substack{p\le x\\ (\frac{g}{p})=1\\ (h,p-1)=1}} \frac{\varphi(p-1)}{p-1} = \tilde{A}(\Delta,h)\ \mathrm{Li}(x) + O_{C,\ g}\left(\frac{x}{\log^C x}\right). \tag{7}$$

with

$$\tilde{A}(\Delta,h) = A(h)\left(1+\mu(\Delta)\prod_{p|\Delta,\ p|h}\frac{1}{p-2}\prod_{p|\Delta,\ p\nmid h}\frac{1}{p^2-p-1}\right).$$

Now the sum on the l.h.s. of (7) equals

$$2\sum_{d\le x}\frac{\mu(d)}{d}\sum_{\substack{p\le x,\ p\equiv 1(\mathrm{mod}\ d)\\ (g/p)=1,\ (h,p-1)=1}} 1. \tag{8}$$

If $(d,h)>1$, the inner sum in (8) is zero, otherwise it is $\sum_{\delta|h}\mu(\delta)\sum_{\substack{p\le x,\ (g/p)=1\\ p\equiv 1(\mathrm{mod}\ d\delta)}} 1$. Reasoning as in the proof of Theorem 3, we see that (7) holds true with constant

$$\begin{aligned}
h_2(g) &= 2\sum_{\substack{d=1\\ (d,h)=1}}^{\infty}\frac{\mu(d)}{d}\sum_{\delta|h}\frac{\mu(\delta)}{[\mathbb{Q}(\zeta_{d\delta},\sqrt{g}):\mathbb{Q}]}.\\
&= 2\sum_{\delta|h}\frac{\mu(\delta)}{\varphi(\delta)}\sum_{\substack{d=1,\ (d,h)=1\\ \Delta|d\delta}}^{\infty}\frac{\mu(d)}{d\varphi(d)} + \sum_{\delta|h}\frac{\mu(\delta)}{\varphi(\delta)}\sum_{\substack{d=1,\ (d,h)=1\\ \Delta\nmid d\delta}}^{\infty}\frac{\mu(d)}{d\varphi(d)}\\
&= A(h) + \sum_{\delta|h}\frac{\mu(\delta)}{\varphi(\delta)}\sum_{\substack{d=1,\ (d,h)=1\\ \Delta|d\delta}}^{\infty}\frac{\mu(d)}{d\varphi(d)}\\
&= A(h)+h_3(g),
\end{aligned}$$

say. If Δ is not squarefree, $h_3(g)=0$ and we are done. So we may assume that Δ is squarefree. Now $\Delta|d\delta$ if and only if $\Delta/(\Delta,\delta)$ divides d. Since in the inner sum in $h_3(g)$ we only sum over those d such that $(d,h)=1$, we can restrict the summation to those δ such that $(\Delta/(\Delta,\delta),h)=1$. Note that $\delta|h$ and $(\Delta/(\Delta,\delta),h)=1$

implies that $(\Delta,\delta)=(\Delta,h)$. Since Δ is squarefree, we have $(\Delta/(\Delta,h),h)=1$. For convenience we put $\tau=\Delta/(\Delta,h)$. We find that

$$\begin{aligned} h_3(g) &= \sum_{\substack{\delta|h\\(\Delta,\delta)=(\Delta,h)}} \frac{\mu(\delta)}{\varphi(\delta)}\frac{\mu(\tau)}{\tau\varphi(\tau)}\prod_{p\nmid h\tau}\left(1-\frac{1}{p(p-1)}\right)\\ &= \mu(\tau)\frac{\prod_{p\nmid h}(1-\frac{1}{p(p-1)})}{\prod_{p|\tau}(p^2-p-1)}\sum_{\substack{\delta|h\\(\Delta,\delta)=(\Delta,h)}}\frac{\mu(\delta)}{\varphi(\delta)}. \end{aligned}$$

On comparing the latter expression for $h_3(g)$ with $\tilde{A}(\Delta,h)$ and using that $\mu(\Delta)=\mu(\tau)\mu((\Delta,h))$ and that $p|\tau$ if and only if $p|\Delta$ and $p\nmid h$, we see that it remains to show that

$$\sum_{\substack{\delta|h\\(\Delta,\delta)=(\Delta,h)}}\frac{\mu(\delta)}{\varphi(\delta)}=\mu((\Delta,h))\frac{\prod_{p|h}(1-\frac{1}{p-1})}{\prod_{p|(\Delta,h)}(p-2)}.$$

Now

$$\begin{aligned} \sum_{\substack{\delta|h\\(\Delta,\delta)=(\Delta,h)}}\frac{\mu(\delta)}{\varphi(\delta)} &= \sum_{m|\frac{h}{(\Delta,h)}}\frac{\mu(m(\Delta,h))}{\varphi(m(\Delta,h))}=\frac{\mu((\Delta,h))}{\varphi((\Delta,h))}\prod_{p|\frac{h}{(\Delta,h)},\ p\nmid(\Delta,h)}\left(1-\frac{1}{p-1}\right)\\ &= \frac{\mu((\Delta,h))}{\varphi((\Delta,h))}\prod_{\substack{p|h\\p\nmid(\Delta,h)}}\left(1-\frac{1}{p-1}\right)=\frac{\mu((\Delta,h))}{\varphi((\Delta,h))}\frac{\prod_{p|h}\left(1-\frac{1}{p-1}\right)}{\prod_{p|(\Delta,h)}\left(1-\frac{1}{p-1}\right)}\\ &= \mu((\Delta,h))\frac{\prod_{p|h}\left(1-\frac{1}{p-1}\right)}{\prod_{p|(\Delta,h)}(p-2)}. \end{aligned}$$

This completes the proof. □

Remark. One can prove the above theorem without explicitly evaluating the involved sums. Examination of the proof of Hooley's theorem in [2] shows that it is enough to establish that

$$\sum_{\substack{d=1\\\Delta|d}}\frac{\mu(d)(d,h)}{d\varphi(d)}=h_3(g).$$

By taking together the d that have the same value of (d,h), this equality is easily established. However, this proof of Theorem 4 has the disadvantage that it is not selfcontained.

6 A generalization

The results in the previous section can be further generalized. The corresponding proofs get more involved, but are rather similar and will be left to the interested reader.

Lemma 3 *Let $h > 1$ be odd and $C > 0$ be arbitrary. Suppose that $f \geq 1$ and $(f,h) = 1$. Then*

$$\sum_{\substack{p\le x,\ (h,p-1)=1\\ p\equiv 1(\text{mod } f)}} \frac{\varphi(p-1)}{p-1} = \frac{A_1(f,h)}{\varphi(f)}\ \mathrm{Li}(x) + O_{C,\ h,\ f}\left(\frac{x}{\log^C x}\right),$$

where

$$A_1(f,h) = \prod_{p|h}\left(1-\frac{1}{p-1}\right)\prod_{p|f}\left(1-\frac{1}{p}\right)\prod_{p\nmid f,\ p\nmid h}\left(1-\frac{1}{p(p-1)}\right).$$

Theorem 6 *Let $g \in G$ and let Δ denote the discriminant of $\mathbb{Q}(\sqrt{g})$. Let h be the largest integer such that g is a pure hth power. Let $f \geq 1$ satisfy $(f,h) = 1$. Put $b = \Delta/(\Delta, f)$. Then*

$$2\sum_{\substack{p\le x,\ p\equiv 1(\text{mod } f)\\ (\frac{g}{p})=-1\\ (h,p-1)=1}} \frac{\varphi(p-1)}{p-1} = \frac{A_2(f,h)}{\varphi(f)}\ \mathrm{Li}(x) + O_{C,\ g,\ f}\left(\frac{x}{\log^C x}\right), \qquad (9)$$

where

$$A_2(f,h) = A_1(f,h)\left(1 - \frac{\mu(|b|)}{\prod_{p|b,\ p|h}(p-2)\prod_{p|b,\ p\nmid h}(p^2-p-1)}\right)$$

in case $g_1 \equiv 1(\text{mod } 4)$, or $g_1 \equiv 2(\text{mod } 4)$ and $8|f$, or $g_1 \equiv 3(\text{mod } 4)$ and $4|f$ and $A_2(f,h) = A_1(f,h)$ otherwise.

The probabilistic interpretation of the l.h.s. in equation (9) is that it should mimick $\pi_{\mathbb{Q}(\zeta_f),g}(x)$, the counting function of the number of primes $p \leq x$ such that p splits completely in $\mathbb{Q}(\zeta_f)$ and g is a primitive root mod p. In [6, Theorem 4] the function $\pi_{\mathbb{Q}(\zeta_f),g}(x)$ is approximated, on GRH. Comparison of the two results shows that the following holds true.

Theorem 7 (GRH). *Let $g \in G$ and $f \geq 1$. Then*

$$2\sum_{\substack{p\le x,\ p\equiv 1(\text{mod } f)\\ (\frac{g}{p})=-1\\ (h,p-1)=1}} \frac{\varphi(p-1)}{p-1} = \pi_{\mathbb{Q}(\zeta_f),g}(x) + O_{g,\ f}\left(\frac{x\log\log x}{\log^2 x}\right).$$

7 Open problems

If S is a set of primes having positive density say, and $w(p)$ an arithmetic function such that the intersection of its support with S has positive density, then one can wonder whether

$$2 \sum_{\substack{p\le x,\ p\in S\\ (p-1,h)=1,\ (g/p)=-1}} w(p)\frac{\varphi(p-1)}{p-1} \sim \sum_{p\le x,\ g \text{ is a prim. root mod } p} w(p). \tag{10}$$

Possible failure of this asymptotic equivalence says something about the limitations of the probabilistic model proposed here.

In this note we proved results of the type (10) by evaluating both sides separately and then comparing them. It would be interesting to proceed more directly. Thus it would be nice to have a proof of the identity (for $g \in G$)

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{[\mathbb{Q}(\zeta_d, g^{1/d}) : \mathbb{Q}]} = 2 \sum_{\substack{d=1\\ (d,h)=1}}^{\infty} \frac{\mu(d)}{d} \sum_{\delta|h} \mu(\delta) \left(\frac{1}{[\mathbb{Q}(\zeta_{d\delta}) : \mathbb{Q}]} - \frac{1}{[\mathbb{Q}(\zeta_{d\delta}, \sqrt{g}) : \mathbb{Q}]} \right),$$

without explicitly computing the involved field degrees. This would give rise to a more conceptual proof of Theorem 4.

A possible extension of the results in this note is to a probabilistic model for the index $[\mathbb{F}_p^* : \langle g\rangle]$ to be precisely κ, with $\kappa \ge 1$.

8 Concluding remarks

In the results were our error depended possibly on f, g or h we can make the dependency explicit. One thus finds that the error term in (3) can be replaced by $O_C(gx\log^{-C} x)$, the error term in (6) by $O_C(h\nu(h)\log^{-C} x)$, where $\nu(h)$ denotes the number of divisors of h, the one in (4) by $O_C(gh\nu(h)x\log^{-C} x)$, that of (5) by $O(gh\nu(h)x\log\log x\log^{-2} x)$, the error term in Lemma 3 by $O_C(h\nu(h)fx\log^{-C} x)$, that of (9) by $O_C(fgh\nu(h)x\log^{-C} x)$ and finally the error term of Theorem 6 by $O(fgh\nu(h)x\log\log x\log^{-2} x)$.

The field extensions that we ran across in this note were of the form $\mathbb{Q}(\zeta_k, \sqrt{r})$. We needed uniform estimates for primes splitting completely in these extensions. Since these extensions are abelian, these primes are in a set of progressions with modulus the conductor. Hence, we could use the Siegel-Walfisz theorem to obtain such an estimate. Instead we could have used an effective form of the Kronecker density theorem.

Lemma 4 [3]. *If L is a Galois extension of $\mathbb{Q}$ with discriminant d_L and degree n_L, then there exists an absolute constant c such that for*

$$n_L(\max(\log|d_L|, |d_L|^{1/n_L}))^2 \le c\log x,$$

we have that

$$\#\{p \le x \mid p \text{ splits completely in } L\} = \frac{\mathrm{Li}(x)}{n_L} + O(x\exp\{-c_3\sqrt{\log x/n_L}\}),$$

where c_3 is a positive constant depending only on c.

However, this would not have allowed us to establish our theorems for arbitrarily large C.

The reader might wonder about the average behaviour of $(p-1)/\varphi(p-1)$. This should mimick the average behaviour of $g(p)$, the least positive integer which is a primitive root mod p. On noticing that

$$\sum_{p\le x}\frac{p-1}{\varphi(p-1)}=\sum_{d\le x}\frac{\mu(d)^2}{\varphi(d)}\pi(x;d,1),$$

one finds, reasoning as in the proof of Theorem 2, that actually an estimate of the form (2) holds, with constant of proportionality

$$\prod_p\left(1+\frac{1}{(p-1)^2}\right)\approx 2.827.$$

This improves on an estimate due to Murata [5].

References

[1] P.D.T.A. Elliott, The distribution of primitive roots, *Canad. J. Math.* **21** (1969), 822-841.

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

[3] J.C. Lagarias and A.M. Odlyzko, *Effective versions of the Chebotarev Density Theorem.* Algebraic Number Fields (Ed. A. Fröhlich), Academic Press, New York, 1977, pp. 409-464.

[4] E. Landau, Über die zahlentheoretische Funktion $\varphi(n)$ und ihre Beziehung zum Goldbachsen Satz, *Collected Works* (Eds. Mirsky et al.), Vol. 1, 106-115.

[5] L. Murata, On the magnitude of the least prime primitive root, *J. Number Theory* **37** (1991), 47-66.

[6] P. Moree, Uniform distribution of primes having a prescribed rational primitive root, MPI preprint 98-23. (Available on the web under http://www.mpim-bonn.mpg.de/html/preprints/preprints.html.)

[7] K. Prachar, *Primzahlverteilung*, Springer, New York, 1957.

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