Near-primitive roots

by

Pieter Moree

Max-Planck-Institut für Mathematik
Preprint Series 2011 (60)

Near-primitive roots

Pieter Moree

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

MPIM 11-60

NEAR-PRIMITIVE ROOTS

PIETER MOREE

In memory of Alf van der Poorten; a dinkum mathematician

Abstract. Golomb conjectured in 2004 that for every square free integer $g > 1$, and for every positive integer t, there are infinitely many primes $p \equiv 1 (\mathrm{mod}\ t)$ such that the order of g in $(\mathbb{Z}/p\mathbb{Z})^*$ is $(p-1)/t$ (we say that g is a near-primitive root of index t). We show that this conjecture is false and provide a corrected and generalized conjecture that is true under the assumption of the Generalized Riemann Hypothesis (GRH) in case g is a rational number. This relies on bringing a formula of Wagstaff for the density in Euler product form.

This preprint extends the earlier MPIM preprint, MPIM2009-106, [11].

1. Introduction

Let $g \in \mathbb{Q}\backslash\{-1, 0, 1\}$. Let p be a prime. Let $\nu_p(g)$ denote the exponent of p in the canonical factorization of g. If $\nu_p(g) = 0$, then we define $r_g(p) = [(\mathbb{Z}/p\mathbb{Z})^* : \langle g \bmod p\rangle]$, that is $r_g(p)$ is the residual index modulo p of g. Note that $r_g(p) = 1$ iff g is a primitive root modulo p. For any natural number t, let $N_{g,t}$ denote the set of primes p with $\nu_p(g) = 0$ and $r_g(p) = t$ (that is $N_{g,t}$ is the set of near-primitive roots of index t). Let $\delta(g, t)$ be the natural density of this set of primes (if it exists). For arbitrary real $x > 0$, we let $N_{g,t}(x)$ denote the number of primes p in $N_{g,t}$ with $p \leq x$.

In 1927 Emil Artin conjectured that for g not equal to -1 or a square, the set $N_{g,1}$ is infinite and that $N_{g,1}(x) \sim c_g A\pi(x)$, with c_g an explicit rational number,

$$A = \prod_p \Big(1 - \frac{1}{p(p-1)}\Big) \approx 0.3739558,$$

and $\pi(x)$ the number of primes $p \leq x$. The constant A is now called Artin's constant. On the basis of computer experiments by the Lehmers in 1957 Artin had to admit that 'The machine caught up with me' and provided a modified version of c_g. See e.g. Stevenhagen [17] for some of the historical details. On GRH this modified version was shown to be correct by Hooley [4].

During the summer of 2004 Solomon Golomb related the following generalization of Artin's conjecture to Ram Murty [2].

Conjecture 1. *For every square free integer $g > 1$, and for every positive integer t, the set $N_{g,t}$ is infinite. Moreover, the density of such primes is asymptotic to a*

Date: September 28, 2011.

2000 *Mathematics Subject Classification.* 11A07.

constant (expressible in terms of g and t) times the corresponding asymptotic density for the case $t = 1$ (Artin's conjecture).

In a 2008 paper Franc and Murty [1] made some progress towards establishing this conjecture. In particular they prove the conjecture in case g is even and t is odd, assuming GRH. In general though, this conjecture is false, since in case $g \equiv 1(\text{mod } 4)$, t is odd and $g|t$, $N_{g,t}$ is finite. To see this note that in this case we have $(\frac{g}{p}) = 1$ for the primes $p \equiv 1(\text{mod } t)$ by the law of quadratic reciprocity and thus $r_g(p)$ must be even, contradicting the assumption $2 \nmid t$.

Work of Lenstra [5] and Murata [13] suggests a modified version of Golomb's conjecture (with as usual μ the Möbius function and $\zeta_k = e^{2\pi i/k}$).

Conjecture 2. *Let $g > 1$ be a square free integer and $t \geq 1$ an integer. The set $N_{g,t}$ has a natural density $\delta(g,t)$ which is given in Table 1. We have*

$$N_{g,t} \textit{ is finite iff } \delta(g,t) = 0 \text{ iff } g \equiv 1(\text{mod } 4),\ 2 \nmid t,\ g|t.$$

Note that if a set of primes is finite, then its natural density is zero. The converse is often false, but for a wide class of Artin type problems (including the one under consideration in this note) is true (on GRH) as first pointed out by Lenstra [5].

Given an integer a and a prime q, we write a_q to denote the q-part of a (that is $a_q = q^\beta$ with $q^\beta | a$ and $q^{\beta+1} \nmid a$). We put

$$B(g,t) = \prod_{p|g,\ p\nmid t} \frac{-1}{p^2-p-1},\ E(t) = \frac{A}{t^2} \prod_{p|t} \frac{p^2-1}{p^2-p-1}. \tag{1}$$

Note that if $g|t$, then in the definition of $B(g,t)$ we have the empty product and hence $B(g,t) = 1$. It follows that if further t is odd and $g \equiv 1(\text{mod } 4)$, then $\delta(g,t) = 0$. The maximal value of $\delta(g,t)$ that occurs is $2E(t)$. Table 1 we took from a paper by Murata [13]. We will show that the densities in Table 1 can be compressed into one equation, namely (7).

Table 1: The density $\delta(g,t)$ of $N_{g,t}$ (on GRH)

g	t_2	$\delta(g,t)$
$g \equiv 1(\text{mod } 4)$	$t_2 = 1$	$(1 - B(g,t))E(t)$
	$2\|t_2$	$(1 + B(g,t))E(t)$
$g \equiv 2(\text{mod } 4)$	$t_2 < 4$	$E(t)$
	$t_2 = 4$	$(1 - B(g,t)/3)E(t)$
	$t_2 > 4$	$(1 + B(g,t))E(t)$
$g \equiv 3(\text{mod } 4)$	$t_2 = 1$	$E(t)$
	$t_2 = 2$	$(1 - B(g,t)/3)E(t)$
	$t_2 \geq 4$	$(1 + B(g,t))E(t)$

Theorem 1. *Conjecture 2 holds true on GRH.*

The proof is postponed untill Section 2

Note that $\delta(g,t)$ equals a rational constant times $\delta(g,1)$. Thus the constant alluded to in Golomb's conjecture is actually a *rational number.*

2. Generalization to rational g

A natural next problem is to study what happens if one relaxes the condition that g should be square free. Our starting point here will be a result due to Wagstaff [18]. We need some notation. We put

$$S(h,t,m)=\sum_{\substack{n=1\\ m|nt}}^{\infty}\frac{\mu(n)(nt,h)}{nt\varphi(nt)},$$

with φ Euler's totient function.

Theorem 2. [18]. (GRH). *Let $g\in\mathbb{Q}\backslash\{-1,0,1\}$ and $t\ge 1$ be an arbitrary integer. Write $g=\pm g_0^h$, where $g_0\in\mathbb{Q}$ is positive and not an exact power of a rational and $h\ge 1$ an integer. Let $d(g_0)$ denote the discriminant of $\mathbb{Q}(\sqrt{g_0})$. The natural density of the set $N_{g,t}$, $\delta(g,t)$, exists and is given by*

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

which equals a rational number times the Artin constant A. Write $g_0=g_1g_2^2$, where g_1 is a square free integer and g_2 is a rational. If $g>0$, set $m=\operatorname{lcm}(2h_2,d(g_0))$. For $g<0$, define $m=2g_1$ if $2\nmid h$ and $g_1\equiv 3(\mathrm{mod}\ 4)$, or $h_2=2$ and $g_1\equiv 2(\mathrm{mod}\ 4)$; let $m=\operatorname{lcm}(4h_2,d(g_0))$ otherwise. If $g>0$, we have $\delta(g,t)=S(h,t,1)+S(h,t,m)$. If $g<0$ we have

$$\delta(g,t)=S(h,t,1)-\frac{1}{2}S(h,t,2)+\frac{1}{2}S(h,t,2h_2)+S(h,t,m).\tag{3}$$

In case $g>0$ or $2\nmid h$, Wagstaff expressed $\delta(g,t)$ as an Euler product. By the work of Lenstra [5] we know this is also possible in general. The next theorem achieves this. Partial inspiration for it came from recent joint work with Lenstra and Stevenhagen, see Section 7.

Theorem 3. (GRH). *Let $g\in\mathbb{Q}\backslash\{-1,0,1\}$ and $t\ge 1$ be an arbitrary integer. Write $g=\pm g_0^h$, where $g_0\in\mathbb{Q}$ is positive and not an exact power of a rational and $h\ge 1$ an integer. Let $d(g_0)$ denote the discriminant of $\mathbb{Q}(\sqrt{g_0})$. Put $F_p=\mathbb{Q}(\zeta_p,g^{1/p})$. Put*

$$A(g,t)=\frac{(t,h)}{t^2}\prod_{p|t,\ h_p|t_p}(1+\frac{1}{p})\prod_{p\nmid t}(1-\frac{1}{[F_p:\mathbb{Q}]}).$$

Put

$$\Pi_1=\prod_{p|d(g_0),\ p\nmid 2t}\frac{-1}{[F_p:\mathbb{Q}]-1}.$$

Put

$$E_2(m_2)=\begin{cases}1 & \text{if } m_2|t_2;\\ -1/3 & \text{if } m_2=2t_2\neq 2;\\ -1 & \text{if } m_2=2t_2=2;\\ 0 & \text{if } m_2\nmid 2t_2,\end{cases}\tag{4}$$

We have

$$\frac{A(g,t)}{A}=\frac{(t,h)}{t^2}\prod_{p|th}\frac{1}{p^2-p-1}\prod_{\substack{p|t\\ pt_p|h_p}}p(p-1)\prod_{\substack{p|t\\ h_p|t_p}}(p^2-1)\prod_{p|h,\ p\nmid t_1}p(p-2),\tag{5}$$

where

$$t_1=\begin{cases}2t & \text{if } g<0,\ 2|h,\ 2\nmid t;\\ t & \text{otherwise.}\end{cases}$$

Note that $A(g,t)=0$ *iff* $g>0$, $2|h$ *and* $2\nmid t$.

The natural density of the set $N_{g,t}$ *exists, denote it by* $\delta(g,t)$.
Put $v_0=\mathrm{lcm}(2h_2,d(g_0)_2)$ *and* $v=\mathrm{lcm}(2h_2,d(g)_2)$.
If $g>0$, *then* $\delta(g,t)=A(g,t)(1+E_2(v_0)\Pi_1)$.
If h *is odd, then* $\delta(g,t)=A(g,t)(1+E_2(v)\Pi_1)$.
If $g<0$, $2|h$ *and* $2\nmid t$, *we have* $\delta(g,t)=A(g,t)$.

Next assume $g<0$, $2|(h,t)$.
If $h_2=2$ *and* $8|d(g_0)$, *then*

$$\delta(g,t)=\begin{cases}\frac{1}{3}A(g,t)(1-\Pi_1) & \text{if } t_2=2;\\ A(g,t)(1+\Pi_1) & \text{if } 4|t_2.\end{cases}\tag{6}$$

In the remaining cases we have

$$\delta(g,t)=\begin{cases}A(g,t)/2 & \text{if } 2t_2|h_2;\\ A(g,t)/3 & \text{if } t_2=h_2;\\ A(g,t)(1-\frac{1}{3}\Pi_1) & \text{if } t_2=2h_2;\\ A(g,t)(1+\Pi_1) & \text{if } 4h_2|t_2.\end{cases}$$

Corollary 1. (GRH). *Let* $g>1$ *be a square free integer. Then*

$$\delta(g,t)=(1+E_2(\mathrm{lcm}(2,d(g)_2))B(g,t))E(t).\tag{7}$$

Proof. We have $A(g,t)=S(1,t,1)=E(t)$ (see the remark following Lemma 1). Furthermore, if $2|g$ and $2\nmid t$, then $\Pi_1=-B(g,t)$ and $\Pi_1=B(g,t)$ otherwise. Since $E_2(\mathrm{lcm}(2,d(g)_2))=0$ if $g|2$ and $2\nmid t$, we infer that $E_2(\mathrm{lcm}(2,d(g)_2))\Pi_1=E_2(\mathrm{lcm}(2,d(g)_2))B(g,t)$. Now invoke the theorem. □

Corollary 2. (GRH). *If* t *is odd, then*

$$\delta(g,t)=A(g,t)(1-\frac{1}{2}(1-(-1)^{h|d(g)|})\Pi_1).$$

Remark. On putting $t = 1$ one obtains the classical result of Hooley [4].

Proof of Theorem 1. On distinguishing cases according to the value of $d(g)_2$, Corollary 1 yields Table 1. From Table 1 one easily reads off that if $\delta(g,t) = 0$, then $2 \nmid t$, $g \equiv 1(\text{mod } 4)$ and $g|t$. In this case we have $(g/p) = 1$ for the primes $p \nmid g$ with $p \equiv 1(\text{mod } t)$ by the law of quadratic reciprocity and hence $N_{g,t}$ is finite and so $\delta(g,t) = 0$. □

The proof of Theorem 3 will be given in Section 4. It will make use of properties of Wagstaff sums that will be established in the next section.

3. Bringing the Wagstaff sums in Euler product form

Recall the definition of the Wagstaff sum

$$S(h,t,m) = \sum_{\substack{n=1 \\ m|nt}}^{\infty} \frac{\mu(n)(nt,h)}{nt\varphi(nt)}.$$

A trivial observation is that if the divisibility condition forces n to be non-square free, then $\mu(n) = 0$ and hence $S(h,t,m) = 0$. This happens for example if $m_2 \nmid 2t_2$ (cf. Lemma 4).

In case $m = 1$ it is easily written as an Euler product (here we use that μ and φ are multiplicative functions).

Lemma 1. 1). *We have*

$$S(h,t,1) = \frac{(t,h)}{t^2} \prod_{p|t,\ h_p|t_p} (1 + \frac{1}{p}) \prod_{p\nmid t} \Big(1 - \frac{(p,h)}{p(p-1)}\Big).$$

In particular, $S(h,t,1) = 0$ *iff* $2|h$ *and* $2 \nmid t$.
2). *If* $2|h$ *and* $2 \nmid t$, *then*

$$S(h,t,2) = -\frac{(t,h)}{t^2} \prod_{p|t,\ h_p|t_p} (1 + \frac{1}{p}) \prod_{p\nmid 2t} \Big(1 - \frac{(p,h)}{p(p-1)}\Big).$$

Proof. 1) We have

$$S(h,t,1) = \frac{(t,h)}{t\varphi(t)} \sum_n \frac{\mu(n)(nt,h)\varphi(t)}{n\varphi(nt)(t,h)} = \frac{(t,h)}{t\varphi(t)} \prod_p \Big(1 - \frac{(pt,h)\varphi(t)}{p\varphi(pt)(t,h)}\Big),$$

where we used that the sum $S(h,t,1)$ is absolutely convergent and the fact that the argument in the second sum is a multiplicative function in n. The contribution of the primes dividing t to this product is

$$\frac{(t,h)}{t\varphi(t)} \prod_{p|t,\ pt_p|h_p} (1 - \frac{1}{p}) \prod_{p|t,\ h_p|t_p} (1 - \frac{1}{p^2}) = \frac{(t,h)}{t^2} \prod_{p|t,\ h_p|t_p} (1 + \frac{1}{p}),$$

where we used that $\varphi(t)/t=\prod_{p|t}(1-1/p)$. If $p\nmid t$, then

$$1-\frac{(pt,h)\varphi(t)}{p\varphi(pt)(t,h)}=1-\frac{(p,h)}{p(p-1)},$$

and part 1 follows.
2) We have

$$S(h,t,2)=\sum_{2|n}\frac{\mu(n)(nt,h)}{nt\varphi(nt)}=-\sum_{2\nmid n}\frac{\mu(n)(nt,h)}{nt\varphi(nt)}.$$

The latter sum has the same Euler product as $S(h,t,1)$, but with the factor for $p=2$ omitted. □

Remark. The above lemma and the definition of the Artin constant shows that $E(t)=S(1,t,1)$ and $A=S(1,1,1)$.

Write $M=m/(m,t)$ and $H=h/(Mt,h)$. Then we have [18, Lemma 2.1]

$$S(h,t,m)=\mu(M)(Mt,h)E(t)\prod_{q|(M,t)}\frac{1}{q^2-1}\prod_{\substack{q|M\\ q\nmid t}}\frac{1}{q^2-q-1}\prod_{\substack{q|(t,H)\\ q\nmid M}}\frac{q}{q+1}\prod_{\substack{q|H\\ q\nmid Mt}}\frac{q(q-2)}{q^2-q-1}.$$

The parameter H can be avoided as the formula can be rewritten as

$$\frac{\mu(M)(Mt,h)A}{t^2}\prod_{q|mth}\frac{1}{q^2-q-1}\prod_{\substack{q|t,\ qt_q|h_q\\ m_q|t_q}}q(q-1)\prod_{\substack{q|t,\ h_q|t_q\\ m_q|t_q}}(q^2-1)\prod_{\substack{q|h\\ q\nmid mt}}q(q-2). \quad (8)$$

(In order to see this it is helpful to consider the cases $m_q|t_q$, that is $M_q=1$, and $qt_q|m_q$, that is $q|M$, separately.) These formulae relate $S(h,t,m)$ to $S(1,t,1)$ $(=E(t))$, respectively to $S(1,1,1)$ $(=A)$, however, as we will show, expressions simplify considerably if we relate $S(h,t,m)$ to $S(h,t,1)$. We start by showing how to remove odd prime factors from m.

Lemma 2. *Suppose that $p\nmid 2m$. Then*

$$S(h,t,mp)=\begin{cases}-S(h,t,m)/(\frac{p(p-1)}{(p,h)}-1) & \text{if } p\nmid t;\\ S(h,t,m) & \text{if } p|t.\end{cases}$$

Proof. If $p|t$ the summation condition $mp|nt$ in the definition of $S(h,t,mp)$ is equivalent with $m|nt$, that is we have $S(h,t,mp)=S(h,t,m)$.

Next assume that $p\nmid t$. We have

$$S(h,t,mp)=\sum_{\substack{m|nt\\ p|n}}\frac{\mu(n)(nt,h)}{nt\varphi(nt)}=\sum_{m|nt}\frac{\mu(pn)(pnt,h)}{pnt\varphi(pnt)}=-\frac{(p,h)}{p(p-1)}\sum_{\substack{m|nt\\ p\nmid n}}\frac{\mu(n)(nt,h)}{nt\varphi(nt)}.$$

On noting that the latter sum can be written as $S(h,t,m)-S(h,t,mp)$, the proof is then completed. □

Lemma 3. *Suppose that we are not in the case where h is even and t is odd. We have*

$$S(h,t,2t_2)=\begin{cases}-S(h,t,1)/3 & \text{if } \mathrm{lcm}(2,h_2)|t_2;\\ -S(h,t,1) & \text{if } \mathrm{lcm}(2,h_2)\nmid t_2.\end{cases}$$

Proof. We can write

$$S(h,t,2t_2)=\sum_{2|n}\frac{\mu(n)(nt,h)}{nt\varphi(nt)}=-\frac{1}{2}\sum_{2\nmid n}\frac{\mu(n)(2nt,h)}{nt\varphi(2nt)}=\epsilon\sum_{2\nmid n}\frac{\mu(n)(nt,h)}{nt\varphi(nt)},$$

where ϵ is easily determined (and $\epsilon\ne -1$). Since the latter sum is equal to $S(h,t,1)-S(h,t,2t_2)$, we then infer that $S(h,t,2t_2)=\frac{\epsilon}{1+\epsilon}S(h,t,1)$. Working out the remaining details is left to the reader. □

Lemma 4. *Let m be an integer, having square free odd part. Let h and t be integers, with the requirement that t be even in case h is even. Then*

$$S(h,t,m)=S(h,t,1)E_1(m_2)\prod_{p|m,p\nmid 2t}\frac{-1}{\frac{p(p-1)}{(p,h)}-1},$$

where

$$E_1(m_2)=\begin{cases}1 & \text{if } m_2|t_2\\ -1/3 & \text{if } m_2=2t_2 \text{ and } \mathrm{lcm}(2,h_2)|t_2\\ -1 & \text{if } m_2=2t_2 \text{ and } \mathrm{lcm}(2,h_2)\nmid t_2\\ 0 & \text{if } m_2\nmid 2t_2,\end{cases}$$

In case $2h_2|m_2$, we have $E_1(m_2)=E_2(m_2)$, where $E_2(m_2)$ is given by (4).

Proof. By Lemma 1 the conditions imposed on h and t imply that $S(h,t,1)\ne 0$. By Lemma 2 it suffices to show that $S(h,t,m_2)=S(h,t,1)E_1(m_2)$. If $m_2|t_2$, then no divisibility condition on n is imposed in the definition of $S(h,t,m_2)$ and so we obtain $S(h,t,m_2)=S(h,t,1)$ and hence $E_1(m_2)=1$. In case $m_2=2t_2$ we invoke Lemma 3. If $m_2\nmid 2t_2$, then the summation condition $m|nt$ implies $4|n$ and hence $\mu(n)=0$ and so $S(h,t,m_2)=0$ and hence $E_1(m_2)=0$.

The final claim follows on noting that if $2h_2|m_2$ and $m_2=2t_2$, then $h_2|t_2$ and hence $\mathrm{lcm}(2,h_2)\nmid t_2$ iff $2\nmid t_2$. □

4. Proof of Theorem 3

The idea of the proof is to express $\delta(g,t)$ in terms of $S(h,t,1)$, except in case $g<0$, $2|h$ and $2\nmid t$, when $S(h,t,1)=0$, in which case we express $\delta(g,t)$ in terms of $S(h,t,2)$. These two Wagstaff sums are then related to $A(g,t)$ using the following lemma. Note that it shows that the dependence of $A(g,t)$ on g is weak, as only h and the sign of g matter.

Lemma 5. *We have*

$$A(g,t)=\begin{cases}-S(h,t,2)/2 & \text{if } g<0,\ 2|h,\ 2\nmid t;\\ S(h,t,1) & \text{otherwise.}\end{cases}$$

Proof. Note that if $g < 0$ and $2|h$, then $F_2 = \mathbb{Q}(i)$ and $[F_2 : \mathbb{Q}] = 2$. In the remaining cases we have $[F_p : \mathbb{Q}] = p(p-1)/(p,h)$. On invoking Lemma 1 the proof is then completed. □

Proof of Theorem 3. Equation (5) follows by Lemma 5 and (8). We will use a few times, cf. the proof of Lemma 5, that

$$\Pi_1 = \prod_{p|d(g_0),\ p\nmid 2t} \frac{-1}{[F_p : \mathbb{Q}] - 1} = \prod_{p|d(g_0),\ p\nmid 2t} \frac{-1}{\frac{p(p-1)}{(p,h)} - 1}.$$

Assume GRH.

The case $g > 0$.

By Theorem 2 we have $\delta(g,t) = S(h,t,1) + S(h,t,m)$, with $m = \text{lcm}(2h_2, d(g_0))$. First assume that $2|h$ and $2 \nmid t$. Then, by Lemmas 1 and 5, we have $S(h,t,1) = A(g,t) = 0$ and we need to show that $\delta(g,t) = 0$. Since $S(h,t,1) = 0$ it remains to show that $S(h,t,m) = 0$. Since for the n in the summation we have $4|2h_2|n$, this is clear. Next assume we are in the remaining case, that is either h is odd, or $2|(h,t)$. Then $S(h,t,1) = A(g,t)$ by Lemma 5. Note that $m_2 = v_0$. By Lemma 4 we then find that $\delta(g,t) = S(h,t,1)(1 + E_1(v_0)\Pi_1) = A(g,t)(1 + E_2(v_0)\Pi_1)$, where we have used that $2h_2|v_0$.

The case h is odd.

If $g > 0$ then $v = v_0$ and we are done, so assume that $g < 0$. The formula for m in Theorem 2 can be rewritten as $\text{lcm}(2, |d(g)|)$, and one finds that $\delta(g,t) = S(h,t,1) + S(h,t,\text{lcm}(2,|d(g)|))$. This is the same formula as in case $g > 0$ and $2 \nmid h$, but with $d(g_0)$ replaced by $|d(g)|$. On noting that the odd part of $d(g_0)$ equals the odd part of $d(g)$, the result then follows.

The case $g < 0$, $2 \nmid t$ and $2|h$.

We have $S(h,t,1) = S(h,t,m) = S(h,t,2h_2) = 0$ and hence $\delta(g,t) = -S(h,t,2)/2$ by (3). Now invoke Lemma 5 to obtain $\delta(g,t) = A(g,t)$.

The case $g < 0$ and $2|(h,t)$.

Note that $2|m$ and $S(h,t,1) = A(g,t)$. By Lemma 4 we infer that $S(h,t,2) = S(h,t,1)$ and $S(h,t,2h_2) = S(h,t,1)E_2(2h_2)$, where

$$E_2(2h_2) = \begin{cases} 1 & \text{if } 2h_2|t_2; \\ -1/3 & \text{if } h_2 = t_2; \\ 0 & \text{if } h_2 \nmid t_2. \end{cases}$$

Note that

$$E_2(4) = \begin{cases} 1 & \text{if } 4|t_2; \\ -1/3 & \text{if } t_2 = 2. \end{cases}$$

If $h_2 = 2$ and $8|d(g_0)$, then by Theorem 2 we have $m = 2g_1$, which can be rewritten as $m = d(g_0)/2$ (thus $m_2 = 4$) and so

$$\delta(g,t) = S(h,t,1) - \frac{S(h,t,2)}{2} + \frac{S(h,t,4)}{2} + S(h,t,\frac{d(g_0)}{2})$$

$$= S(h,t,1)\Big(\frac{1}{2}+\frac{E_2(4)}{2}+E_2(4)\Pi_1\Big).$$

where we used that, by Lemma 4, $S(h,t,d(g_0)/2)=S(h,t,1)E_2(4)\Pi_1$. Using that $S(h,t,1)=A(g,t)$ and the formula for $E_2(4)$, we then arrive at (6).

In the remaining case, $m=\text{lcm}(4h_2,d(g_0))$. Note that $m_2=4h_2$ and

$$E_2(4h_2)=\begin{cases}1 & \text{if } 4h_2|t_2;\\ -1/3 & \text{if } 2h_2=t_2;\\ 0 & \text{if } 2h_2\nmid t_2.\end{cases}$$

We find that

$$\delta(g,t)=S(h,t,1)-\frac{S(h,t,2)}{2}+\frac{S(h,t,2h_2)}{2}+S(h,t,m)$$
$$= S(h,t,1)\Big(\frac{1}{2}+\frac{E_2(2h_2)}{2}+E_2(4h_2)\Pi_1\Big).$$

Using that $S(h,t,1)=A(g,t)$ and the formulae for $E_2(2h_2)$ and $E_2(4h_2)$ given above, the proof is then completed. □

5. Vanishing of $\delta(g,t)$

The aim of this section is to give a new proof of Theorem 4 (due to Lenstra [5], who stated it without proof). The first published proof was given by Moree in [8]. He introduced a function $w_{g,t}(p)\in\{0,1,2\}$ for which he proved (see [8], for a rather easier reproof see [9]) under GRH that

$$N_{g,t}(x)=(h,t)\sum_{p\le x,\ p\equiv 1(\text{mod }t)} w_{g,t}(p)\frac{\varphi((p-1)/t)}{p-1}+O\Big(\frac{x\log\log x}{\log^2 x}\Big).$$

This function $w_{g,t}(p)$ has the property that, under GRH, $w_{g,t}(p)=0$ for all primes p sufficiently large iff $N_{g,t}$ is finite. Since the definition of $w_{g,t}(p)$ involves nothing more than the Legendre symbol, it is then not difficult to arrive at the cases 1-6. E.g. in case 1 g is a square modulo p, and thus $2|t$, contradicting $2\nmid t$. Likewise for the other 5 cases the obstructions can be written down (it turns out $r_g(p)_2\neq t_2$ in each case). For the complete list of obstructions we refer to Moree [8, pp. 170-171].

Regarding the six vanishing cases Wagstaff [18, p. 143] wrote: ‘It is easy to verify directly that our expression for $\delta(g,t)$ vanishes in each of Lenstra’s cases, but it is tedious to check that these are the only cases in which it vanishes’. We will show that once Wagstaff’s result is brought into Euler product form, as done in Theorem 3, it is straightforward to establish Theorem 4. A more conceptual, shorter and elegant (but less elementary) proof of Theorem 4 will appear in [7].

Theorem 4. (GRH). *The set $N_{g,t}$ is finite iff $\delta(g,t)=0$ iff we are in one of the following six (mutually exclusive) cases:*
1) $2\nmid t$, $d(g)|t$.
2) $g>0$, $2h_2|t_2$, $3\nmid t$, $3|h$, $d(-3g_0)|t$.
3) $g<0$, $h_2=1$, $t_2=2$, $3\nmid t$, $3|h$, $d(3g_0)|t$.
4) $g<0$, $h_2=2$, $t_2=2$, $d(2g_0)|2t$.

5) $g<0$, $h_2=2$, $t_2=4$, $3\nmid t$, $3|h$, $d(-6g_0)|t$.
6) $g<0$, $4h_2|t_2$, $3\nmid t$, $3|h$, $d(-3g_0)|t$.

Example. (GRH). If $g>1$ is square free, then case 1 is the only one to take into account and we find $\delta(g,t)=0$ iff $2\nmid t$, $d(g)|t$, that is iff $2\nmid t$, $g|t$, $g\equiv 1(\text{mod } 4)$.

Table 2: Examples of pairs (g,t) satisfying cases 1-6

	1	2	3	4	5	6
(g,t)	$(5,5)$	$(3^3,4)$	$(-15^3,10)$	$(-6^2,6)$	$(-6^6,4)$	$(-3^3,4)$

Proof of Theorem 4. If one of 1-6 is satisfied, then $N_{g,t}$ is finite. This can be shown by elementary arguments only involving quadratic reciprocity (see Moree [8, pp. 170-171]). It is thus enough to show that $\delta(g,t)=0$ iff one of the six cases is satisfied. For the proof we will split up case 6 into two subcases:
6a) $g<0$, $2|h_2$, $4h_2|t_2$, $3\nmid t$, $3|h$, $d(3g_0)|t$.
6b) $g<0$, $h_2=1$, $4|t_2$, $3\nmid t$, $3|h$, $d(3g_0)|t$.
(For our proof it is more natural to require $d(3g_0)|t$, which, since $4|t$, is equivalent with $d(-3g_0)|t$.) Let us denote by $d^*(g_0)$ the odd part of the discriminant of g_0, that is $d^*(g_0)=d(g_0)/d(g_0)_2$. Note that

$$\Pi_1=\begin{cases}1 & \text{if } d^*(g_0)|t;\\ -1 & \text{if } 3|d(g_0),\ d^*(g_0)|3t,\ 3\nmid t,\ 3|h;\\ \in(-1,1) & \text{otherwise.}\end{cases} \tag{9}$$

The case $2\nmid t$.
If $2|h$ one has $\delta(g,t)=0$ iff $g>0$, that is iff $d(g)|t$.
If $2\nmid h$, then $A(g,t)\neq 0$ and we have $\delta(g,t)=0$ iff $E_2(\text{lcm}(2,d(g)_2))=-1$ and $\Pi_1=1$, that is iff $\text{lcm}(2,d(g)_2)=2$ and $d^*(g)|t$, that is iff $d(g)|t$.
Thus from now on we may assume that $2|t$. This ensures that $A(g,t)\neq 0$.
The case $g>0$ and $2|t$.
Now the possibility $E_2(m_2)=-1$ cannot occur and thus $\delta(g,t)=0$ iff $E_2(m_2)=1$ and $\Pi_1=-1$. The latter two conditions are both satisfied iff $\text{lcm}(2h_2,d(g_0)_2)|t_2$, $3|d(g_0)$, $d^*(g_0)|3t$, $3\nmid t$, $3|h$. These conditions can be reformulated as $2h_2|t_2$, $3|d(g_0)$, $d(g_0)|3t$, $3\nmid t$ and $3|h$. Since $3\nmid t$, $3|d(g_0)$, $d(g_0)|3t$ iff $d(-3g_0)|t$, $3\nmid t$, we are done.

Thus if $g>0$ or $2\nmid t$, then $\delta(g,t)=0$ iff we are in case 1 or in case 2. It remains to consider the case where $g<0$ and $2|t$.
The case $g<0$, $2|t$, $2\nmid h$.
Here we have $\delta(g,t)=0$ iff $E_2(v)=1$ and $\Pi_1=-1$. Note that $E_2(v)=1$ means that we require $\text{lcm}(2,d(g)_2)|t_2$.
If $t_2=2$, then $\text{lcm}(2,d(g)_2)|t_2$ and $\Pi_1=-1$ iff we are in case 3.
If $4|t_2$, then $\text{lcm}(2,d(g)_2)|t_2$ and $\Pi_1=-1$ iff we are in case 6b.
The case $g<0$, $2|(h,t)$.
We have $\delta(g,t)=0$ iff we are in one of the following three cases:
A) $h_2=2,\ t_2=2,\ 8|d(g_0),\ \Pi_1=1$;
B) $h_2=2,\ t_2=4,\ 8|d(g_0),\ \Pi_1=-1$;

C) $2|h_2,\ 4h_2|t_2,\ \Pi_1=-1$.
It is easily checked that these are merely cases 4, 5 and 6a in different guises.

To sum up, we have shown that $\delta(g,t)=0$ iff we are in one of the cases 1,2,3,4,5,6a or 6b. Note that the six cases are mutually exclusive. □

Now we are ready to propose a corrected and generalized version of Golomb's conjecture.

Conjecture 3. *The set $N_{g,t}$ has a natural density $\delta(g,t)$ that is given as in Theorem 3 and is a rational multiple of the Artin constant A. The set $N_{g,t}$ is finite iff $\delta(g,t)=0$ iff we are in one of the six cases of Theorem 4.*

On combining Theorem 3 and Theorem 4 we deduce that Conjecture 3 holds true on GRH.

Theorem 5. *Conjecture 3 is true under GRH.*

6. Two applications

The first application likely inspired Golomb to make his conjecture.
Let $\Phi_n(x)$ denote the n-th cyclotomic polynomial. Let S be the set of primes p such that if $f(x)$ is any irreducible factor of $\Phi_p(x)$ over $\mathbb{F}_2$, then $f(x)$ does not divide any trinomial. Over $\mathbb{F}_2$, $\Phi_p(x)$ factors into $r_2(p)$ irreducible polynomials. Let

$$S_1=(\{p>2:2\nmid r_2(p)\}\}\cup\{p>2:2\le r_2(p)\le 16\})\backslash\{3,7,31,73\}.$$

Theorem 6. *We have $S_1\subseteq S$. The set S_1 contains the primes $p>3$ such that $p\equiv\pm 3(\text{mod }8)$. On GRH the set $S_!$ has density*

$$\delta(S_1)=\frac{1}{2}+A\frac{1323100229}{1099324800}\approx 0.950077195\cdots \qquad (10)$$

Proof. The set $\{p>2:2\nmid r_2(p)\}\}$ equals the set of primes p such that $(\frac{2}{p})=-1$, that is the set of primes p such that $p\equiv\pm 3(\text{mod }8)$. This set has density 1/2. We thus find, on consulting Table 1, that

$$\begin{aligned}\delta(S_1) &= \frac{1}{2}+\sum_{\substack{2\le j\le 16\\ 2|j}}A(2,j)\\ &= \frac{1}{2}+E(2)(1+\frac{2}{3\cdot 4}+\frac{2}{16}+\frac{2}{64})+E(6)(1+\frac{2}{3\cdot 4})+E(10)+E(14),\end{aligned}$$

which yields (10) on invoking the definition (1) of $E(t)$. That $S_1\subseteq S$ is a consequence of the work of Golomb and Lee [3]. □

6.1. **Near-primitive roots in arithmetic progression.** Recently Peter Malicky in connection with work on the periodic orbits of a certain 2-dimensional dynamical system raised the following question:

Question 1. *Are there infinitely many primes $p\equiv 7(\text{mod }8)$ such that 2 generates the group of squares modulo p ?*

Since for such primes p we have $(\frac{2}{p})=1$, 2 cannot generate $(\mathbb{Z}/p\mathbb{Z})^*$ and so we are asking for the primes $p\equiv 7(\text{mod } 8)$ such that 2 is a near-primitive root modulo p of index 2. This leads to the question of determining for a given primitive residue class $a(\text{mod } f)$ (hence $(a,f)=1$) the number of primes $p\le x$ such that $p\equiv a(\text{mod } f)$ and g ia a near-primitive root modulo p of index t. Denote this set by $N_{a,f;g,t}$. Let σ_b be the automorphism of $\mathbb{Q}(\zeta_f)$ that sends ζ_f to ζ_f^b. On GRH it can be shown that $N_{a,f;g,t}$ has a natural density $\delta(a,f;g,t)$ that is given by

$$\delta(a,f;g,t)=\sum_{n=1}^{\infty}\frac{c(n)\mu(n)}{[\mathbb{Q}(\zeta_f,\zeta_{nt},g^{1/nt}):\mathbb{Q}]},$$

where $c(n)=1$ if the restriction of ζ_a on the intersection $\mathbb{Q}(\zeta_f)\cap\mathbb{Q}(\zeta_{nt},g^{1/nt})$ acts like the identity and zero otherwise. Note that if $a=1$ we merely get

$$\delta(1,f;g,t)=\sum_{n=1}^{\infty}\frac{\mu(n)}{[\mathbb{Q}(\zeta_f,\zeta_{nt},g^{1/nt}):\mathbb{Q}]}.$$

Since if 2 is a near-primitive root of index 2, we must have $p\equiv\pm 1(\text{mod } 8)$, we find, under GRH, $\delta(7,8;2,2)=\delta(2,2)-\delta(1,8;2,2)=3A/4-A/4=A/2$, where we leave it to the reader to show that $\delta(1,8;2,2)=A/4$.

Answer 1. *Under GRH there are infinitely many primes* $p\equiv 7(\text{mod } 8)$ *such that* 2 *generates the group of squares. This set has a natural density equal to* $A/2$.

Earlier, in connection with the number of points over $\mathbb{F}_{2^m}$ of the curve $y^2+y=x^p$, p a prime, Rodier [16] had asked the same question and gave a sketch of a proof that under GRH the density should be $A/2$. In this context it is maybe of some interest to recall the result of Murty and Wong [14], who showed that at least one of the following holds true:
1) $N_{2,2}$ is infinite.
2) There exist infinitely many primes p such that 2^p-1 is composite.

Both using the 'classical method' and the 'character sum method' (see next section) it should be possible to determine $\delta(a,f;g,t)$ in full generality. However, this might involve many case distinctions. The density $\delta(a,f;g,1)$ is evaluated in [7, 10] by the character sum, respectively the classical method.

7. Near-primitive roots density through character sum averages

Lenstra, Moree and Stevenhagen [7] show that for a large class of Artin-type problems the set of primes has a natural density δ that is given by

$$\delta=(\prod_p A_p)(1+\prod_p E_p), \tag{11}$$

where $\prod_p A_p$ is the 'generic answer' to the density problem (e.g. A in the original Artin problem) and $1+\prod_p E_p$ a correction factor. For finitely many primes p one has $E_p\neq 1$ and further $-1\le E_p\le 1$ as E_p is a (real) character sum average over a finite set (and hence the correction factor is a rational number). In particular, it is rather easy in this set-up to determine when $\delta=0$. A preview of [7] is given in

[17]. The character sum method makes use of the theory of radical entanglement as developped by Lenstra [6]

For the near-primitive root problem the method leads rather immediately to the formula $\delta(g,t) = A(g,t)(1 + E_2'\Pi_1)$ in case $g > 0$. The only harder part is the determination of E_2'. For the details the reader is referred to [7].

Indeed, the great advance of the newer method is that it very directly leads to a formula for the density in Euler product form. The classical method leads to infinite sums involving the Möbius function and nearly multiplicative functions (in our case Wagstaff's result (Theorem 2). It then requires rather cumbersome manipulations to arrive at a density in Euler product form. Indeed, inspired by the predicted result (11) the author attempted (and managed) to bring Wagstaff's result in Euler product form.

The analogue of Theorem 3 obtained in this approach, Theorem 6.4 of [7], looks slightly different from Theorem 3. However, on noting that s_2 as defined in Theorem 6.4 is merely the 2-part of m as defined in Wagstaff's result Theorem 2, it is not difficult to show that both methods give rise to the same Euler products for the density. By allowing g_0 to be negative in case h is odd and $g < 0$, the above 6 cases where vanishing occurs can be reduced to 5 cases (see Corollary 6.5 of [7]).

The character sum method can also be extended to the situation of radical extensions of arbitrary rank, e.g., if one considers the density of primes p for which a given set of integers $a_1, \ldots, a_r$ generates $\mathbb{F}_p^*$, see [12]. Here it is rather more difficult to decide when $\delta = 0$. Also in the higher rank case the character sum method leads much more directly to the densities (on GRH) in Euler product form.

Acknowledgment 1. Given expressions like (8), my intuition was that expressing $\delta(g,t)$ in Euler product form would lead to very unpleasant formulae and thus I never attempted this. Discussions with Peter Stevenhagen, considering the near-primitive root problem by a much more algebraic method, strongly suggested easier expressions for $\delta(g,t)$ than expected. This led me to try to bring Wagstaff's result in Euler product form, also with the aim of verifying the results found by the character sum method (alluded to in Section 7). The above unfolding of events is a nice demonstration of the power of the character sum method over the classical one.

The memorable discussions with Stevenhagen are gratefully acknowledged. Finally, I like to thank Carl Pomerance for helpful e-mail correspondence.

Acknowledgment 2. The author spent a wonderful year (the academic year 1994) as postdoc of Alf at Macquarie and will always remain grateful to Alf for having made this possible.

References

[1] C. Franc and M. Ram Murty, On a generalization of Artin's conjecture, *Pure Appl. Math. Q.* **4** (2008), 1279–1290.

[2] S.W. Golomb, Letter to M. Ram Murty, June 22, 2004.

[3] S.W. Golomb and P.F. Lee, Irreducible polynomials which divide trinomials over GF(2), *IEEE Trans. Inform. Theory* **53** (2007), 768–774.

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

[5] H.W. Lenstra, Jr., On Artin's conjecture and Euclid's algorithm in global fields, *Invent. Math.* **42** (1977), 202–224.

[6] H.W. Lenstra, Jr., *Entangled radicals*, AMS Colloquium Lectures, San Antonio, 2006.

[7] H.W. Lenstra, Jr., P. Moree and P. Stevenhagen, Character sums for primitive root densities, in preparation.

[8] P. Moree, Asymptotically exact heuristics for (near) primitive roots, *J. Number Theory* **83** (2000), 155–181.

[9] P. Moree, Asymptotically exact heuristics for (near) primitive roots. II, *Japan. J. Math. (N.S.)* **29** (2003), 143–157.

[10] P. Moree, On primes in arithmetic progression having a prescribed primitive root. II, *Funct. Approx. Comment. Math.* **39** (2008), 133144.

[11] P. Moree, On Golomb's near-primitive root conjecture, Max-Planck Institute for Mathematics preprint, MPIM2009-106, pp. 5.

[12] P. Moree and P. Stevenhagen, Computing higher rank primitive root densities, in preparation.

[13] L. Murata, A problem analogous to Artin's conjecture for primitive roots and its applications, *Arch. Math. (Basel)* **57** (1991), 555–565.

[14] M.R. Murty and S. Wong, The *ABC* conjecture and prime divisors of the Lucas and Lehmer sequences, *Number theory for the millennium*, III (Urbana, IL, 2000), A. K. Peters, Natick, MA (2002), 43-54.

[15] W.J. Palenstijn, *PhD. thesis*, Universiteit Leiden (in preparation).

[16] F. Rodier, Minoration de certaines sommes exponentielles binaires, *Coding theory and algebraic geometry* (Luminy, 1991), LNIM **1518**, Springer, Berlin (1992), 199–209.

[17] P. Stevenhagen, The correction factor in Artin's primitive root conjecture, *J. Théor. Nombres Bordeaux* **15** (2003), 383–391.

[18] S.S. Wagstaff, Jr., Pseudoprimes and a generalization of Artin's conjecture, *Acta Arith.* **41** (1982), 141–150.

Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany
E-mail address: moree@mpim-bonn.mpg.de