ON GOLOMB'S NEAR-PRIMITIVE ROOT CONJECTURE

PIETER MOREE

Abstract. Golomb conjectured in 2004 that for every squarefree integer $g > 1$, and for every positive integer t, there are infinitely many primes $p \equiv 1 (\text{mod } t)$ 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.

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 $r_g(p) = [(\mathbb{Z}/p\mathbb{Z})^* : \langle g \text{ mod } p\rangle]$, 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 $A(g, t)$ 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 $p \le x$.

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 $p \le x$. 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 [12] 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 squarefree 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 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

Date: November 13, 2009.
2000 *Mathematics Subject Classification.* 11A07.

is odd, assuming GRH. In general though, this conjecture is false, since in case $g \equiv 1 (\mathrm{mod}\ 4)$, 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 $p \equiv 1 (\mathrm{mod}\ t)$ 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 [10] 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 squarefree integer. The set $N_{g,t}$ has a natural density $A(g,t)$ given by*

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

which is worked out as an Euler product in Table 1. The set $N_{g,t}$ is finite if and only if $g \equiv 1 (\mathrm{mod}\ 4)$, $2 \nmid t$ and $g|t$. We have

$$A(g,t) = 0 \text{ iff } g \equiv 1 (\mathrm{mod}\ 4),\ 2 \nmid t,\ g|t.$$

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].

We put

$$B(g,t) = \prod_{p | \frac{g}{(g,t)}} \frac{-1}{p^2 - p - 1},$$

and let $E(t)$ be as in (2).

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

g	$\tau = \nu_2(t)$	$g\|t$?	$A(g,t)$
$g \equiv 1 (\mathrm{mod}\ 4)$	$\tau = 0$	YES	0
		NO	$(1 - B(g,t))E(t)$
	$\tau \geq 1$	YES	$2E(t)$
		NO	$(1 + B(g,t))E(t)$
$g \equiv 2 (\mathrm{mod}\ 4)$	$\tau < 2$		$E(t)$
	$\tau = 2$		$(1 - B(g,t)/3)E(t)$
	$\tau > 2$		$(1 + B(g,t))E(t)$
$g \equiv 3 (\mathrm{mod}\ 4)$	$\tau = 0$		$E(t)$
	$\tau = 1$		$(1 - B(g,t)/3)E(t)$
	$\tau > 2$		$(1 + B(g,t))E(t)$

Given a rational number g, let $d(g)$ denote the discriminant of $\mathbb{Q}(\sqrt{g})$.

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

Proof. By work of Lenstra [5] it follows that $N_{g,t}$ is finite iff $2 \nmid t$ and $d(g)|t$. By elementary properties of the discriminant this is seen to be equivalent with $g \equiv 1 (\mathrm{mod}\ 4)$, $2 \nmid t$ and $g|t$.

Lenstra's work also shows that $N_{g,t}$ has a natural density $A(g,t)$ that is given by (1), with $A(g,t)/A$ rational. The explicit evaluation of $A(g,t)$ as an Euler product in Table 1 we took from a paper by Murata [10]. (We leave it as an exercise to the reader to show that the results of Wagstaff described below lead to the same results.)

Since by the work of Lenstra $N_{g,t}$ is finite iff $A(g,t)=0$, the final assertion follows. Alternatively, this can be deduced from Table 1. □

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

2. Generalization to rational g

A natural next question is what happens if we relax the condition that g need to be squarefree ? Here we propose the following conjecture. 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. Put $E(t)=S(1,t,1)$. This sum can be evaluated as an Euler product and one finds:

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

Write $M=m/(m,t)$ and $H=h/(Mt,h)$. Then we have [13, Lemma 2.1]

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

Conjecture 3. *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 $e=\nu_2(h)$ and $\tau=\nu_2(t)$. In the following cases there are only finitely many near-primitive roots of index t:*
1) $2\nmid t$, $d(g)|t$.
2) $g>0$, $\tau>e$, $3\nmid t$, $3|h$, $d(-3g_0)|t$.
3) $g<0$, $\tau=e=1$, $d(2g_0)|2t$.
4) $g<0$, $\tau=1$, $e=0$, $3\nmid t$, $3|h$, $d(3g_0)|t$.
5) $g<0$, $\tau=2$, $e=1$, $3\nmid t$, $3|h$, $d(-6g_0)|t$.
6) $g<0$, $\tau>e+1$, $3\nmid t$, $3|h$, $d(-3g_0)|t$.
In the remaining cases, there are infinitely many primes p such that g is a near-primitive root of index t.

The natural density of the set $N_{g,t}$ exists, call it $A(g,t)$, and equals a rational number times the Artin constant A. We have $A(g,t)=0$ iff one of the conditions (1)-(6) applies. To write $A(g,t)$ as A times a correction factor, write $g_0=g_1g_2^2$, where g_1 is a squarefree integer and g_2 is a rational. If $g>0$, set $m=\operatorname{lcm}\{2^{e+1},d(g_0)\}$. For $g<0$, define $m=2g_1$ if $e=0$ and $g_1\equiv 3\pmod 4$, or $e=1$ and $g_1\equiv 2\pmod 4$; let

$m = \mathrm{lcm}(2^{e+2}, d(g_0))$ *otherwise. If* $g > 0$, *we have* $A(g,t) = S(h,t,1) + S(h,t,m)$. *If* $g < 0$ *we have*

$$A(g,t) = S(h,t,1) - \frac{1}{2}S(h,t,2) + \frac{1}{2}S(h,t,2^{e+1}) + S(h,t,m).$$

Note that $S(h,t,m_1)$ has an Euler product that differs in at most finitely many primes p from that of $S(h,t,m_2)$. This allows one to write $A(g,t)$ as an Euler product. It is a rational multiple of A. From the above description it is very cumbersome to determine when $A(g,t) = 0$. However, from the work of Lenstra we know that $A(g,t) = 0$ iff one of the conditions (1)-(6) is satisfied. In each of those cases, one has that $N_{g,t}$ is finite. Examples are given in Table 2.

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

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

Theorem 2. *Conjecture* 3 *holds true on GRH.*

Proof. Most of the proof is a consequence of work of Lenstra [5]. However, he merely indicated conditions (1)-(6) without working this out. Moree [8] by an independent method also arrived at these conditions (see also below). The explicit evaluation of $A(g,t)$ can be found in Wagstaff [13]. □

Moree 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

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

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 conditions (1)-(6). For condition (1) we have that 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. In each of the cases it turns out that $\nu_2(r_g(p)) \ne \nu_2(t)$. For the complete list of obstructions we refer to Moree [8, pp. 170-171].

For a large class of Artin type problems there are conjectural densities, that can be shown to be true on GRH, involving inclusion-exclusion. It is computationally challenging to convert these expressions in to Euler products and determine exactly when the densities are zero. Using the theory of radical entanglement as developped by Lenstra [6] this problem is rather more easily resolved, for two examples see Lenstra et al. [7] (Artin problems over base field $\mathbb{Q}$) and De Smit and Palenstijn [11] (for arbitrary base field). A preview of [7] is given in [12].

3. An application

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

$$\delta(S_1) = \frac{1}{2} + A\frac{1323100229}{1099324800} \approx 0.950077195\cdots \qquad (3)$$

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 $p \equiv \pm 3 (\bmod 8)$. This set has density $1/2$. We thus find, on invoking Theorem 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 (3) on invoking formula (2). That $S_1 \subseteq S$ is a consequence of the work of Golomb and Lee [3]. □

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] L. Murata, A problem analogous to Artin's conjecture for primitive roots and its applications, *Arch. Math. (Basel)* **57** (1991), 555–565.
[11] W.J. Palenstijn, *PhD. thesis*, Universiteit Leiden (2010).
[12] P. Stevenhagen, The correction factor in Artin's primitive root conjecture, *J. Théor. Nombres Bordeaux* **15** (2003), 383–391.
[13] 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