Max-Planck-Institut für Mathematik Bonn

Primes in arithmetic progressions and non-primitive roots

by

Pieter Moree
Min Sha

Max-Planck-Institut für Mathematik
Preprint Series 2019 (7)

Primes in arithmetic progressions and non-primitive roots

Pieter Moree
Min Sha

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

Department of Computing
Macquarie University
Sydney, NSW 2109
Australia

MPIM 19-7

PRIMES IN ARITHMETIC PROGRESSIONS AND NON-PRIMITIVE ROOTS

PIETER MOREE AND MIN SHA

Dedicated to the memory of Prof. Christopher Hooley (1928–2018)

Abstract. Let p be a prime. If an integer g generates a subgroup of index t in $(\mathbb{Z}/p\mathbb{Z})^*$, then we say that g is a t-near primitive root modulo p. We point out the easy result that each coprime residue class contains a positive natural density subset of primes p not having g as a t-near primitive root and prove a more difficult variant.

1. Introduction

1.1. **Background.** Given a set of primes S, the limit

$$\delta(S) = \lim_{x\to\infty} \frac{\#\{p : p \in S,\, p \le x\}}{\#\{p : p \le x\}},$$

if it exists, is called the *natural density* of S. (Here and in the sequel the letter p is used to denote a prime number.)

For any integer $g \notin \{-1, 0, 1\}$, let $\mathcal{P}_g$ be the set of primes p such that g is a primitive root modulo p, that is $p \nmid g$ and the *multiplicative order* of g modulo p, $\mathrm{ord}_p(g)$, equals $p-1 = \#(\mathbb{Z}/p\mathbb{Z})^*$, and so g is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. In 1927, Emil Artin conjectured that the set $\mathcal{P}_g$ is infinite if g is not a square; moreover he also gave a conjectural formula for its natural density $\delta(\mathcal{P}_g)$; see [12] for more details. There is no explicit value of g known for which $\mathcal{P}_g$ can be unconditionally proved to be infinite. However Heath-Brown [3], building on earlier fundamental work by Gupta and Murty [2], showed that, given any three distinct primes p_1, p_2 and p_3, there is at least one i such that $\mathcal{P}_{p_i}$ is infinite.

In 1967, Hooley [4] established Artin's conjecture under the Generalized Riemann Hypothesis (GRH) and determined $\delta(\mathcal{P}_g)$. Ten years later, Lenstra [7] considered a wide class of generalizations of Artin's conjecture. For example, under GRH he showed that the primes in $\mathcal{P}_g$ that are in a prescribed arithmetic progression have a natural density and gave a Galois theoretic formula for it. This was worked out explicitly by the first author [9, 11], who showed that $\delta(\mathcal{P}_g) = r_g A$, with r_g an explicit rational number and the Artin constant

$$A = \prod_p \left(1 - \frac{1}{p(p-1)}\right) = 0.373955\ldots.$$

2010 *Mathematics Subject Classification.* 11N13, 11N69.

Key words and phrases. Primitive root, near-primitive root, Artin's primitive root conjecture, arithmetic progression.

Using a powerful and very general algebraic method, this result was rederived in a very different way by Lenstra et al. [8].

For any integer $t \geq 1$, let

$$\mathcal{P}_g(t) = \{p : \ p \nmid g, \, p \equiv 1 \pmod{t}, \, \mathrm{ord}_p(g) = (p-1)/t\}.$$

If p is in $\mathcal{P}_g(t)$, then it is said to have g as a *t-near primitive root*. Assuming GRH, the first author [13] determined $\delta(\mathcal{P}_g(t))$ in case $g > 1$ is square-free.

A more refined problem is how the primes in $\mathcal{P}_g(t)$ are distributed over arithmetic progressions. To this end, let $a, d \geq 1$ be coprime integers and define

$$\mathcal{P}_g(t, d, a) = \{p : \ p \equiv a \pmod{d}, \, p \in \mathcal{P}_g(t)\}.$$

By the prime number theorem for arithmetic progressions,

$$\#\{p : \ p \leq x, \, p \equiv a \pmod{d}\} \sim \frac{x}{\varphi(d) \log x}, \tag{1.1}$$

where φ denotes Euler's totient function. A straightforward combination of the ideas used in the study of near-primitive roots and those for primitive roots in arithmetic progression, allows one to show, assuming GRH, that $\delta(\mathcal{P}_g(t, d, a))$ exists and derive a Galois theoretic expression $\delta_G(\mathcal{P}_g(t, d, a))$ for it (see Hu et al. [6, Theorem 3.1]). Moreover, it can be unconditionally shown (see [6, Equation (3.7)]) that

$$\limsup_{x \to \infty} \frac{\#\{p \leq x : \ p \in \mathcal{P}_g(t, d, a)\}}{\pi(x)} \leq \delta_G(\mathcal{P}_g(t, d, a)), \tag{1.2}$$

where as usual $\pi(x)$ denotes the prime counting function. The proof is obtained essentially by doing the simple asymptotic sieve up to a range in which the unconditional Chebotarev density theorem is valid.

On the basis of insights from [8], we know that $\delta_G(\mathcal{P}_g(t, d, a))$ equals a rational multiple of the Artin constant A, where the rational multiple can be worked out in full generality. However, this is likely to produce a result involving several case distinctions (as in the restricted case where $t = 1$ and in the case where t is arbitrary and g is square-free). In the much less general case $g = 4$ and $t = 2$, the expression was explicitly worked out in [6]; see Section 1.3 for more background.

1.2. **Our considerations.** In this paper we study, motivated by the following questions, the distribution of primes not having a prescribed near-primitive root in arithmetic progressions.

Questions. *Let $t \geq 1$ and $g \notin \{-1, 0, 1\}$ be integers. Let a, d be positive coprime integers.*

A) *Is the set*

$$\mathcal{Q}_g(t, d, a) = \{p : \ p \equiv a \pmod{d}, \, p \notin \mathcal{P}_g(t)\}$$

infinite?

B) *Does the set $\mathcal{Q}_g(t, d, a)$ have a natural density and can it be computed?*

Since $\mathcal{P}_g(t, d, a) \cup \mathcal{Q}_g(t, d, a) = \{p : \ p \equiv a \pmod{d}\}$, if $\delta(\mathcal{P}_g(t, d, a))$ exists, then using (1.1) we have

$$\delta(\mathcal{Q}_g(t, d, a)) = 1/\varphi(d) - \delta(\mathcal{P}_g(t, d, a)).$$

Question B can currently be answered only assuming GRH. However, in this approach it is far from evident under which conditions on the parameters g, t, d and a we have $\delta(\mathcal{Q}_g(t,d,a)) > 0$, thus guaranteeing the infinitude of the set $\mathcal{Q}_g(t,d,a)$.

Unconditionally using (1.2) we infer that

$$\liminf_{x\to\infty} \frac{\#\{p \le x:\ p \in \mathcal{Q}_g(t,d,a)\}}{\pi(x)} \ge \frac{1}{\varphi(d)} - \delta_G(\mathcal{P}_g(t,d,a)).$$

If there exists a prime $p_0 \nmid t$ satisfying both $p_0 \equiv a \pmod{d}$ and $p_0 \not\equiv 1 \pmod{t}$, then all the primes $p \equiv p_0 \pmod{dt}$ are in $\mathcal{Q}_g(t,d,a)$ (due to $t \nmid (p-1)$). By (1.1), there are infinitely many primes $p \equiv p_0 \pmod{dt}$, and they have a positive natural density. Thus, the first question is only non-trivial when $p \equiv a \pmod{d}$ implies $p \mid t$ or $p \equiv 1 \pmod{t}$, which is true if and only if

$$t \mid d \quad \text{and} \quad t \mid (a-1). \tag{1.3}$$

In this note we will see that answering Question A is actually also rather easy in case (1.3) is satisfied. The answer to Question A is yes, and we can be even a little bit more precise on using Kummerian extensions of cyclotomic number fields $\mathbb{Q}(\zeta_n)$ with $\zeta_n = e^{2\pi i/n}$.

Proposition 1.1. *Let $g \notin \{-1,0,1\}$ and $t \ge 1$ be integers. Let a, d be positive coprime integers. Then, for any integer $q > 2$ coprime to $2dt$, the set $\mathcal{Q}_g(t,d,a)$ contains a positive natural density subset of primes p having natural density*

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

The field degree $[\mathbb{Q}(\zeta_d, \zeta_q, g^{1/q}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{\mathrm{lcm}(d,q)}, g^{1/q}) : \mathbb{Q}]$ is not difficult to compute for any given g, d and q; see [10, Lemma 1] for the general result (which is a direct consequence of [15, Proposition 4.1]). Using this computation the maximum density of the q-dependent subsets arising in Proposition 1.1 can be determined; see the next section for an example. If ℓ is a prime factor of q, then $\mathbb{Q}(\zeta_d, \zeta_\ell, g^{1/\ell}) \subseteq \mathbb{Q}(\zeta_d, \zeta_q, g^{1/q})$, and so a priori the maximum occurs in an odd prime.

We will also establish a more difficult variant of Proposition 1.1. Letting g, t, d, a be as in Proposition 1.1, we define the set

$$\mathcal{R}_g(t,d,a) = \{p:\ p \nmid g,\ p \equiv a \pmod{d},\ p \equiv 1 \pmod{t},\ \mathrm{ord}_p(g) \mid (p-1)/t\}.$$

Clearly, we have $\mathcal{P}_g(t,d,a) \subseteq \mathcal{R}_g(t,d,a)$. Our purpose is to show that if $\mathcal{R}_g(t,d,a)$ is not empty, then $\mathcal{R}_g(t,d,a)$ contains a positive density subset of primes not contained in $\mathcal{P}_g(t,d,a)$.

Theorem 1.2. *Let $g \notin \{-1,0,1\}$ and $t \ge 1$ be integers. Let a, d be positive coprime integers. Suppose the set $\mathcal{R}_g(t,d,a)$ is not empty. Then, for any integer $q > 2$ coprime to $2dgt$, the set $\mathcal{R}_g(t,d,a)$ contains a subset of primes p for which g is a non t-near primitive root modulo p having natural density*

$$\frac{1}{[\mathbb{Q}(\zeta_d, \zeta_{qt}, g^{1/qt}) : \mathbb{Q}]}.$$

Again, given d, g and t, the maximum density of the q-dependent subsets arising in the theorem can be determined, and for this it suffices to consider primes $q \nmid 2dgt$.

Note that for any integer $q \geq 2$, each prime in $\mathcal{R}_g(qt, d, a)$ is not contained in $\mathcal{P}_g(t, d, a)$. So, Theorem 1.2 is derived directly from the following proposition, which might be of independent interest.

Proposition 1.3. *Let $g \notin \{-1, 0, 1\}$ and $t \geq 1$ be integers. Let a, d be positive coprime integers. Suppose the set $\mathcal{R}_g(t, d, a)$ is not empty. Then, for any positive integer q coprime to $2dgt$, we have*

$$\delta(\mathcal{R}_g(qt, d, a)) = \frac{1}{[\mathbb{Q}(\zeta_d, \zeta_{qt}, g^{1/qt}) : \mathbb{Q}]}.$$

1.3. **An application.** Proposition 1.1 has an application to *Genocchi numbers* G_n, which are defined by $G_n = 2(1 - 2^n)B_n$, where B_n is the n^{th} Bernoulli number. The Genocchi numbers are actually integers. As introduced in [6], if a prime $p > 3$ divides at least one of the Genocchi numbers $G_2, G_4, \ldots, G_{p-3}$, it is said to be *G-irregular* and *G-regular* otherwise. The first fifteen G-irregular primes [1] are

$$17, 31, 37, 41, 43, 59, 67, 73, 89, 97, 101, 103, 109, 113, 127.$$

The G-regularity of primes can be linked to the divisibility of certain class numbers of cyclotomic fields. Let S be the set of infinite places of $\mathbb{Q}(\zeta_p)$ and T the set of places above the prime 2. Denote by $h_{p,2}$ the (S, T)*-refined class number* of $\mathbb{Q}(\zeta_p)$ and $h^+_{p,2}$ be the refined class number of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ with respect to its infinite places and places above the prime 2 (for the definition of the refined class number of global fields, see for example Hu and Kim [5, Section 2]). Define $h^-_{p,2} = h_{p,2}/h^+_{p,2}$. It turns out that $h^-_{p,2}$ is an integer (see [5, Proof of Proposition 3.4]). Recall that a *Wieferich prime* is an odd prime p such that $2^{p-1} \equiv 1 \pmod{p^2}$.

Theorem 1.4. [6, Theorem 1.5]. *Let p be an odd prime. Then, if p is G-irregular, we have $p \mid h^-_{p,2}$. If furthermore p is not a Wieferich prime, the converse is also true.*

It is easy to show that if $\operatorname{ord}_p(4) \neq (p-1)/2$, then p is G-irregular; see [6, Theorem 1.6]. Hence, taking $g = 4$ and $t = 2$ in Proposition 1.1 and noting that we have $[\mathbb{Q}(\zeta_d, \zeta_q, 4^{1/q}) : \mathbb{Q}] = \varphi(d)q(q-1)$ for any prime $q \nmid 2d$, we arrive at the following result.

Proposition 1.5. *Let a, d be positive coprime integers. Let q be the smallest prime not dividing $2d$. The set of G-irregular primes p satisfying $p \equiv a \pmod{d}$ contains a subset having natural density*

$$\frac{1}{\varphi(d)q(q-1)}.$$

This result is a weaker version of Theorem 1.11 in [6], however its proof is much more elementary, and it still shows that each coprime residue class contains a subset of G-irregular primes having positive natural density.

2. Preliminaries

Given any integers $d, n \geq 1$ put $K_n = \mathbb{Q}(\zeta_d, \zeta_n, g^{1/n})$. For a coprime to d, let σ_a be the endomorphism of $\mathbb{Q}(\zeta_d)$ over $\mathbb{Q}$ defined by $\sigma_a(\zeta_d) = \zeta_d^a$. Let C_n be the conjugacy class of elements of the Galois group $G_n = \mathrm{Gal}(K_n/\mathbb{Q})$ such that for any $\tau_n \in C_n$,

$$\tau_n\big|_{\mathbb{Q}(\zeta_d)} = \sigma_a, \qquad \tau_n\big|_{\mathbb{Q}(\zeta_n, g^{1/n})} = \mathrm{id}, \tag{2.1}$$

where 'id' stands for the identity map. Note that either C_n is empty, or C_n is non-empty and $|C_n| = 1$. The latter case occurs if and only if

$$\tau_n\big|_{\mathbb{Q}(\zeta_d)\cap\mathbb{Q}(\zeta_n, g^{1/n})} = \mathrm{id}. \tag{2.2}$$

If this condition is satisfied, then by the Chebotarev density theorem (in its natural density form, cf. Serre [14], the original form being for Dirichlet density), the primes unramified in K_n and with Frobenius C_n have natural density $1/[K_n : \mathbb{Q}]$. Note that the primes unramified in K_n are exactly the primes $p \nmid dgn$. The first condition on τ_n ensures that the primes $p \nmid dgn$ having τ_n as Frobenius satisfy $p \equiv a \pmod d$. Likewise the second condition ensures that such primes satisfy $\mathrm{ord}_p(g) \mid (p-1)/n$.

In particular, in case $\mathbb{Q}(\zeta_d)$ and $\mathbb{Q}(\zeta_n, g^{1/n})$ are linearly disjoint over $\mathbb{Q}$, that is,

$$\mathbb{Q}(\zeta_d) \cap \mathbb{Q}(\zeta_n, g^{1/n}) = \mathbb{Q}, \tag{2.3}$$

we have $|C_n| = 1$, and the primes $p \nmid dgn$ with Frobenius C_n satisfy $p \equiv a \pmod d$ and $\mathrm{ord}_p(g) \mid (p-1)/n$, and they have natural density $1/[K_n : \mathbb{Q}]$.

3. Proofs

3.1. **Proof of Proposition 1.1.** Since q is odd, the extension $\mathbb{Q}(\zeta_q, g^{1/q})$ of $\mathbb{Q}(\zeta_q)$ is non-abelian and

$$\mathbb{Q}(\zeta_d) \cap \mathbb{Q}(\zeta_q, g^{1/q}) = \mathbb{Q}(\zeta_d) \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}(\zeta_{\gcd(d,q)}) = \mathbb{Q},$$

as $\gcd(q, d) = 1$. Thus (2.3) is satisfied and consequently there is a set with natural density $1/[K_q : \mathbb{Q}]$ of primes p satisfying $p \equiv a \pmod d$ and $\mathrm{ord}_p(g) \mid (p-1)/q$. Since by assumption $q \nmid t$, it follows that for these primes p, $\mathrm{ord}_p(g) \neq (p-1)/t$, and so for them g is a non t-near primitive root. This completes the proof.

3.2. **Proof of Proposition 1.3.** From now on we assume that g, t, a and d are as in Proposition 1.3. The proof of Proposition 1.3 rests on the Chebotarev density theorem and the following lemma. Recall that $K_n = \mathbb{Q}(\zeta_d, \zeta_n, g^{1/n})$.

Lemma 3.1. *Put $I_n = \mathbb{Q}(\zeta_d) \cap \mathbb{Q}(\zeta_n, g^{1/n})$. Then, for any positive integer q coprime to $2dgt$, we have $I_{qt} = I_t$.*

Proof. Since $I_t \subseteq I_{qt}$, it suffices to show that $[I_{qt} : \mathbb{Q}] = [I_t : \mathbb{Q}]$. Obviously $[d, t] = rt$ for some positive integer r. By elementary Galois theory and noticing that $\gcd(q, dt) = 1$, we see that

$$[I_{qt} : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_d) : \mathbb{Q}] \cdot [\mathbb{Q}(\zeta_{qt}, g^{1/qt}) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_d, \zeta_{qt}, g^{1/qt}) : \mathbb{Q}]} = \frac{\varphi(d)[\mathbb{Q}(\zeta_{qt}, g^{1/qt}) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_{qrt}, g^{1/qt}) : \mathbb{Q}]},$$

and, similarly, $[I_t : \mathbb{Q}] = \varphi(d)[\mathbb{Q}(\zeta_t, g^{1/t}) : \mathbb{Q}]/[\mathbb{Q}(\zeta_{rt}, g^{1/t}) : \mathbb{Q}]$. Then, by Lemma 1 of [10] and noticing $\gcd(q, 2dgt) = 1$, it is straightforward to deduce that $[I_{qt} : \mathbb{Q}] = [I_t : \mathbb{Q}]$. □

We remark that the condition $\gcd(q, 2dgt) = 1$ cannot be removed. For example, choosing $g = 21, d = 3, t = 10, q = 7$ and using [11, Lemma 2.4], we have $I_t = \mathbb{Q}$ and $I_{qt} = \mathbb{Q}(\zeta_d) = \mathbb{Q}(\sqrt{-3}) \neq I_t$.

Proof of Proposition 1.3. By Lemma 3.1 it follows that

$$I_{qt} = I_t. \tag{3.1}$$

By assumption, $\mathcal{R}_g(t, d, a)$ is not empty. Then, this implies that the two automorphisms in (2.1) are compatible and hence (2.2) is satisfied, which leads to the conclusion that $\mathcal{R}_g(t, d, a)$ is not only non-empty, but even has a positive natural density, moreover $\delta(\mathcal{R}_g(t, d, a)) = [K_t : \mathbb{Q}]^{-1}$ by the discussions in Section 2. So, there must be a $\tau_t \in C_t$ such that $\tau_t|_{I_t} = \mathrm{id}$, which by (3.1) implies the existence of an automorphism $\tau_{qt} \in C_{qt}$ such that $\tau_{qt}|_{I_{qt}} = \mathrm{id}$. Then, it follows from the discussions in Section 2 that $\delta(\mathcal{R}_g(qt, d, a)) = [K_{qt} : \mathbb{Q}]^{-1}$. □

3.3. **Proof of Theorem 1.2.**

Proof of Theorem 1.2. A direct consequence of Proposition 1.3. □

Acknowledgement

The research of Min Sha was supported by a Macquarie University Research Fellowship. The authors thank Christine McMeekin and Peter Stevenhagen for very helpful discussions and feedback. The latter pointed out a serious oversight in an earlier version. The feedback of the referee is also gratefully acknowledged.

References

[1] Genocchi irregular primes, On-line encyclopedia of integer sequences, sequence A321217.
[2] R. Gupta and M.R. Murty, *A remark on Artin's conjecture*, Invent. Math. **78** (1984), 127–130.
[3] D.R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) **37** (1986), 27–38.
[4] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.
[5] S. Hu, M.-S. Kim, The $(S, \{2\})$-Iwasawa theory, *J. Number Theory* **158** (2016), 73–89.
[6] S. Hu, M.-S. Kim, P. Moree and M. Sha, *Irregular primes with respect to Genocchi numbers and Artin's primitive root conjecture*, preprint, 2018, available at https://arxiv.org/abs/1809.08431.
[7] H.W. Lenstra, Jr., *On Artin's conjecture and Euclid's algorithm in global fields*, Invent. Math. **42** (1977), 202–224.
[8] H.W. Lenstra, Jr., P. Moree and P. Stevenhagen, *Character sums for primitive root densities*, Math. Proc. Cambridge Philos. Soc. **157** (2014), 489–511.
[9] P. Moree, *On primes in arithmetic progression having a prescribed primitive root*, J. Number Theory **78** (1999), 85–98.
[10] P. Moree, *On the distribution of the order and index of $g \pmod p$ over residue classes I*, J. Number Theory **114** (2005), 238–271.
[11] P. Moree, *On primes in arithmetic progression having a prescribed primitive root II*, Funct. Approx. Comment. Math. **39** (2008), 133–144.

[12] P. Moree, *Artin's primitive root conjecture – a survey*, Integers **12A** (2012), A13.
[13] P. Moree, *Near-primitive roots*, Funct. Approx. Comment. Math. **48** (2013), 133–145.
[14] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401.
[15] 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

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
E-mail address: shamin2010@gmail.com