EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 11, No. 1, 2018, 23-34
ISSN 1307-5543 – www.ejpam.com
Published by New York Business Global

The Generalized Artin Primitive Root Conjecture

N. A. Carella

Department of Mathematics, York College, Jamaica, New York, 10451

Abstract. Asymptotic formulas for the number of integers with the primitive root 2, and the generalized Artin conjecture for subsets of composite integers with fixed admissible primitive roots $u \neq \pm 1, v^2$, are presented here.

2010 Mathematics Subject Classifications: 11A07, 11N05.
Key Words and Phrases: Primitive root, Generalized primitive root

1. Introduction

A generalized Artin conjecture for subsets of composite integers with fixed primitive roots is presented here. The focus is on developing an asymptotic formula for the number of integers with the primitive root 2, modulo the generalized Riemann hypothesis, but the analysis easily extends to all the admissible primitive roots $u \neq \pm 1, v^2$. This analysis spawn new questions about the structure of an L-series associated with the multiplicative subset of integers with a fixed primitive root 2, and related ideas.

1.1. Subset of Integers With Fixed Primitive Root 2

The Artin primitive root conjecture states that the integer 2 is a primitive root mod p for infinitely many primes. Id est,

$$\mathcal{P}_2 = \{3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 107, 131, 139, ...\}. \tag{1}$$

Moreover, it has the counting function $\pi_2(x) = \#\{p \leq x : \text{ord}_p(2) = p-1\} = \alpha_2 \pi(x)$. Here $\pi(x) = \#\{p \leq x\}$ is the primes counting function. Conditional on the generalized Riemann hypothesis, Hooley proved that the subset of primes

$$\mathcal{P}_2 = \{p \in \mathbb{P} : \text{ord}_p(2) = p-1\} \subset \mathbb{P} \tag{2}$$

has nonzero density $\alpha_2 = \delta(\mathcal{P}_2) > 0$, see Theorem 7.1 or [13]. Partial unconditional results on the Artin primitive root conjecture are also available in [10], et alii. The subset $\mathcal{P}_2$ is utilized here to generate the subset of composite integers

$$\mathcal{N}_2 = \{3, 5, 3^2, 11, 3 \cdot 5, 19, 5^2, 3^3, 29, 3 \cdot 11, 37, 45, 53, 55, 3 \cdot 19, 61, ...\} \tag{3}$$

Email address: pobox505@gmail.com (N. A. Carella)

which have $u = 2$ as a primitive root. The underlining structure of an asymptotic counting formula $N_2(x) = \#\{n \leq x : \text{ord}_n(2) = \lambda(n)\}$ for the subset of integers $\mathcal{N}_2 = \{n \in \mathbb{N} : \text{ord}_n(2) = \lambda(n)\}$ will be demonstrated here. This result is consistent with the heuristic explained in [14, p. 10], and has the expected asymptotic order $N_2(x) = o(x)$.

Theorem 1.1. *Assuming the generalized Riemann hypothesis, the integer 2 is a primitive root mod n for infinitely many composite integers $n \geq 1$. Moreover, the number of integers $n \leq x$ such that 2 is a primitive root mod n has the asymptotic formula*

$$N_2(x) = \left(\frac{e^{\gamma_2 - \gamma\alpha_2}}{\Gamma(\alpha_2)} + o(1)\right) \frac{x}{(\log x)^{1-\alpha_2}} \prod_{p \in \mathcal{W}} \left(1 - \frac{1}{p^2}\right), \tag{4}$$

where $\alpha_2 > 0$ is Artin constant, γ_2 is a generalized Euler constant, the gamma function is defined by $\Gamma(s) = \int_0^\infty x^{s-1}e^x dx$, where $s \in \mathbb{C}$ is a complex number, and

$$\mathcal{W} = \left\{p \in \mathbb{P} : 2^{p-1} - 1 \equiv 0 \bmod p \quad \textit{and} \quad 2^{p-1} - 1 \equiv 0 \bmod p^2\right\} \tag{5}$$

is the subset of Wieferich primes for base 2, for all large numbers $x \geq 1$.

The average order of the counting function $N_2(x)$ has the same average order as the counting function $L(x) = \#\{n \leq x : \mu(\lambda(n)) = \pm 1\} = (\kappa + o(1))x(\log x)^{\alpha_2 - 1}$ for the number of squarefree values of the Carmichael function λ, but it has a different density $\kappa \neq e^{\gamma_2 - \gamma\alpha_2}/\Gamma(\alpha_2)$, see [25]. This should be compared to the counting function $\pi_2(x) = \#\{p \leq x : \text{ord}_p(2) = p - 1\} = \alpha_2\pi(x)$ for the set of primes having 2 as a primitive root, and the counting function $T(x) = \#\{p \leq x : \mu(\varphi(n)) = \pm 1\} = \alpha_2\pi(x)$ of squarefree values of the Euler totient function φ. All these asymptotic formulae are closely related and scaled by the constant α_2.

The general asymptotic formula for the number of integers $n \leq x$ such that $u \neq \pm 1, v^2$ is a primitive root mod n has the form

$$N_u(x) = \left(\frac{e^{\gamma_u - \gamma\alpha_u}}{\Gamma(\alpha_u)} + o(1)\right) \frac{x}{(\log x)^{1-\alpha_u}} \prod_{p \in \mathcal{W}} \left(1 - \frac{1}{p^2}\right), \tag{6}$$

where $\alpha_u > 0$ is Artin constant, γ_u is a generalized Euler constant, and

$$\mathcal{W} = \left\{p \in \mathbb{P} : u^{p-1} - 1 \equiv 0 \bmod p \quad \text{and} \quad u^{p-1} - 1 \equiv 0 \bmod p^2\right\} \tag{7}$$

is the subset of Abel-Wieferich primes for base $u \geq 2$, for all large numbers $x \geq 1$. The proof is the same as the proof of Theorem 1.1 mutatis mutandis.

Sections 2 to 6 provide some essential background results. The proof of Theorem 1.1 is settled in Section 7.

2. Some Arithmetic Functions

The Euler totient function counts the number of relatively prime integers $\varphi(n) = \#\{k : \gcd(k, n) = 1\}$. This counting function is compactly expressed by the analytic formula $\varphi(n) = n \prod_{p|n}(1 - 1/p), n \in \mathbb{N}$.

Lemma 2.1. (Fermat-Euler) *If $a \in \mathbb{Z}$ is an integer such that $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \bmod n$.*

The Carmichael function is basically a refinement of the Euler totient function to the finite ring $\mathbb{Z}/n\mathbb{Z}$. Given an integer $n = p_1^{v_1} p_2^{v_2} \cdots p_t^{v_t}$, the Carmichael function is defined by

$$\lambda(n) = \operatorname{lcm}\left(\lambda\left(p_1^{v_1}\right), \lambda\left(p_2^{v_2}\right) \cdots \lambda\left(p_t^{v_t}\right)\right) = \prod_{p^v || \lambda(n)} p^v, \tag{8}$$

where the symbol $p^v \mid\mid n, \nu \geq 0$, denotes the maximal prime power divisor of $n \geq 1$, and

$$\lambda\left(p^v\right) = \begin{cases} \varphi\left(p^v\right) & \text{if } p \geq 3 \text{ or } v \leq 2, \\ 2^{v-2} & \text{if } p = 2 \text{ and } v \geq 3. \end{cases} \tag{9}$$

The two functions coincide, that is, $\varphi(n) = \lambda(n)$ if $n = 2, 4, p^m$, or $2p^m, m \geq 1$. And $\varphi\left(2^m\right) = 2\lambda\left(2^m\right)$. In a few other cases, there are some simple relationships between $\varphi(n)$ and $\lambda(n)$. In fact, it seamlessly improves the Fermat-Euler Theorem: The improvement provides the least exponent $\lambda(n) \mid \varphi(n)$ such that $a^{\lambda(n)} \equiv 1 \bmod n$.

Lemma 2.2. ([4]) *Let $n \in \mathbb{N}$ be any given integer. Then*

(i) *The congruence $a^{\lambda(n)} \equiv 1 \bmod n$ is satisfied by every integer $a \geq 1$ relatively prime to n, that is $\gcd(a, n) = 1$.*

(ii) *In every congruence $x^{\lambda(n)} \equiv 1 \bmod n$, a solution $x = u$ exists which is a primitive root $\bmod n$, and for any such solution u, there are $\varphi(\lambda(n))$ primitive roots congruent to powers of u.*

Proof. (i) The number $\lambda(n)$ is a multiple of every $\lambda\left(p^v\right) = \varphi\left(p^v\right)$ such that $p^v \mid n$. Ergo, for any relatively prime integer $a \geq 2$, the system of congruences

$$a^{\lambda(n)} \equiv 1 \bmod p_1^{v_1}, \quad a^{\lambda(n)} \equiv 1 \bmod p_2^{v_2}, \quad \ldots, \quad a^{\lambda(n)} \equiv 1 \bmod p_t^{v_t}, \tag{10}$$

where $t = \omega(n)$ is the number of prime divisors in n, is valid.

Definition 2.1. *An integer $u \in \mathbb{Z}$ is called a primitive root mod n if the least exponent $\min\{m \in \mathbb{N} : u^m \equiv 1 \bmod n\} = \lambda(n)$.*

Lemma 2.3. *Let $n, u \in \mathbb{N}, \gcd(u, n) = 1$. The integer $u \neq \pm 1, v^2$ is a primitive root modulo n if and only if u is a primitive root modulo p^k for each prime power divisor $p^k \mid n$.*

Proof. Without loss in generality, let $n = pq$ with p, q primes. Suppose that u is a primitive root modulo p and modulo q, but it is not a primitive root modulo n. Then

$$u^{\lambda(n)/r} \equiv 1 \bmod n \qquad \Longleftrightarrow \qquad u^{\lambda(n)/r} = 1 + an, \tag{11}$$

for some prime $r \mid \lambda(n)$, and $a \in \mathbb{Z}$. This in turns implies that both $u^{\lambda(n)/r} \equiv 1 \bmod p$ and $u^{\lambda(n)/r} \equiv 1 \bmod q$. This contradicts the hypothesis that both $u^{\lambda(n)/r} \not\equiv 1 \bmod p$ and $u^{\lambda(n)/r} \not\equiv 1 \bmod q$. Conversely, suppose that u is a primitive root modulo n, but u is not a primitive root either modulo p or modulo q. Write $u^{\lambda(n)/r} \not\equiv 1 \bmod n$, with $r \geq 2$ prime, and proceed as before to derive a contradiction:

$$u^{\lambda(n)/r} \not\equiv 1 \bmod n \qquad \Longleftrightarrow \qquad u^{\lambda(n)/r} \neq 1 + an. \tag{12}$$

This in turns implies that either $u^{\lambda(n)/r} \not\equiv 1 \bmod p$ or $u^{\lambda(n)/r} \not\equiv 1 \bmod q$. But, this contradicts the hypothesis that u is not a primitive root either modulo p or q.

3. Characteristic Function In Finite Rings

The symbol $\operatorname{ord}_{p^k}(u)$ denotes the order of an element $u \in \left(\mathbb{Z}/p^k\,\mathbb{Z}\right)^\times$ in the multiplicative group of the integers modulo p^k. The order satisfies the divisibility condition $\operatorname{ord}_{p^k}(u) \mid \lambda(n)$, and primitive roots have maximal orders $\operatorname{ord}_{p^k}(u) = \lambda(n)$. The basic properties of primitive root are explicated in [1], [30], et cetera. The characteristic function $f : \mathbb{N} \longrightarrow \{0, 1\}$ of a fixed primitive root u in the finite ring $\mathbb{Z}/p^k\,\mathbb{Z}$, the integers modulo p^k, is determined here.

Lemma 3.1. *Let $p^k, k \geq 1$, be a prime power, and let $u \in \mathbb{Z}$ be an integer such that* $\gcd\left(u, p^k\right) = 1$*. Then*

(i) *The characteristic f function of the primitive root $u \bmod p^k$ is given by*

$$f\left(p^k\right) = \begin{cases} 1 & \textit{if } p^k = 2^k, k \leq 2, \\ 0 & \textit{if } p^k = 2^k, k > 2, \\ 1 & \textit{if } \operatorname{ord}_{p^k}(u) = p^{k-1}(p-1), p > 2, \textit{for any } k \geq 1, \\ 0 & \textit{if } \operatorname{ord}_{p^k}(u) \neq p^{k-1}(p-1), \textit{ and } p > 2, k \geq 1. \end{cases} \tag{13}$$

(ii) *The function f is multiplicative, but not completely multiplicative since*

(iii) $f(pq) = f(p)f(q)$, $\gcd(p, q) = 1$,

(iv) $f\left(p^2\right) \neq f(p)f(p)$, *if* $\operatorname{ord}_{p^2}(u) \neq p(p-1)$.

Proof. The function has the value $f\left(p^k\right) = 1$ if and only if the element $u \in \left(\mathbb{Z}/p^k\,\mathbb{Z}\right)^\times$ is a primitive root modulo p^k. Otherwise, it vanishes: $f\left(p^k\right) = 0$. The completely multiplicative property fails because of the existence of Wieferich primes, exempli gratia,

$0 = f\left(40487^2\right) \neq f(40487)f(40487) = 1$, see [28]. Otherwise, it is completely multiplicative, that is, $f\left(p^2\right) = f(p)f(p) = 1$ for any nonWieferich primes $p \geq 2$.

Observe that the conditions $\operatorname{ord}_p(u) = p-1$ and $\operatorname{ord}_{p^2}(u) \neq p(p-1)$ imply that the integer $u \neq \pm 1, v^2$ cannot be extended to a primitive root $u \bmod p^k$, with $k \geq 2$. But that the condition $\operatorname{ord}_{p^2}(u) = p(p-1)$ implies that the integer u can be extended to a primitive root $u \bmod p^k$, with $k \geq 2$.

4. Wirsing Formula

This formula provides decompositions of some summatory multiplicative functions as products over the primes supports of the functions. This technique works well with certain multiplicative functions, which have supports on subsets of primes numbers of nonzero densities.

Lemma 4.1. ([36, p. 71]) *Suppose that $f : \mathbb{N} \longrightarrow \mathbb{C}$ is a multiplicative function with the following properties.*

(i) *$f(n) \geq 0$ for all integers $n \in \mathbb{N}$.*

(ii) *$f\left(p^k\right) \leq c^k$ for all integers $k \in \mathbb{N}$, and $c < 2$ constant.*

(iii) *There is a constant $\tau > 0$ such*

$$\sum_{p \leq x} f(p) = (\tau + o(1))x/\log x \tag{14}$$

as $x \longrightarrow \infty$.

Then

$$\sum_{n \leq x} f(n) = \left(\frac{1}{e^{\gamma\tau}\Gamma(\tau)} + o(1)\right) \frac{x}{\log x} \prod_{p \leq x}\left(1 + \frac{f(p)}{p} + \frac{f\left(p^2\right)}{p^2} + \cdots\right). \tag{15}$$

The gamma function is defined by $\Gamma(s) = \int_0^\infty t^{s-1}e^{-st}dt$, where $s \in \mathbb{C}$ is a complex number. The intricate proof of Wirsing formula appears in [36]. It is also assembled in various papers, such as [12], [27, p. 195], and discussed in [23, p. 70], [33, p. 308]. Various applications are provided in [21], [25], [37], et alii.

5. Harmonic Sums And Products Over Primes With Fixed Primitive Roots

The subset of primes $\mathcal{P}_u = \{p \in \mathbb{P} : \operatorname{ord}_p(u) = p-1\} \subset \mathbb{P}$ consists of all the primes with a fixed primitive root $u \in \mathbb{Z}$. By Hooley theorem, which is conditional on the generalized Riemann hypothesis, it has nonzero density $\alpha_u = \delta\left(\mathcal{P}_u\right) > 0$. The real number

$\alpha_u > 0$ coincides with the corresponding Artin constant, see [13, p. 220], for the formula. The proof of the next result is based on standard analytic number theory methods in the literature, refer to [25, Lemma 4].

Lemma 5.1. *Assume the generalized Riemann hypothesis, and let $x \geq 1$ be a large number. Then, there exists a pair of constants $\beta_u > 0$, and $\gamma_u > 0$ such that*

(i) $$\sum_{p\leq x, p\in\mathcal{P}_u} \frac{1}{p} = \alpha_u \log\log x + \beta_u + O\left(\frac{\log\log x}{\log x}\right).$$

(ii) $$\sum_{p\leq x, p\in\mathcal{P}_u} \frac{\log p}{p-1} = \alpha_u \log x - \gamma_u + O\left(\frac{\log\log x}{\log x}\right).$$

Proof. (i). Let $\pi_u(x) = \#\{p \leq x : \operatorname{ord}_p(u) = p-1\} = \alpha_u \pi(x)$ be the counting measure of the corresponding subset of primes $\mathcal{P}_u$. To estimate the asymptotic order of the prime harmonic sum, use the Stieltjes integral representation:

$$\sum_{p\leq x, p\in\mathcal{P}_u} \frac{1}{p} = \int_{x_0}^{x} \frac{1}{t} d\pi_u(t) = \frac{\pi_u(x)}{x} + c_(x_0) + \int_{x_0}^{x} \frac{\pi_u(t)}{t^2} dt, \tag{16}$$

where $x_0 > 0$ is a constant. Applying Theorem 7.1 yields

$$\begin{aligned} \int_{x_0}^{x} \frac{1}{t} d\pi_u(t) \quad &= \quad \frac{\alpha_u}{\log x} + O\left(\frac{\log\log x}{\log^2(x)}\right) + c_0(x_0) \\ &\quad +\alpha_u \int_{x_0}^{x} \left(\frac{1}{t\log t} + O\left(\frac{\log\log t}{t\log^2(t)}\right)\right) dt \\ &= \quad \alpha_u \log\log x - \log\log x_0 + c_0(x_0) + O\left(\frac{\log\log x}{\log x}\right), \end{aligned} \tag{17}$$

where $\beta_u = -\log\log x_0 + c_0(x_0)$ is the Artin-Mertens constant. The statement (ii) follows from statement (i) and partial summation.

The Artin-Mertens constant β_u and the Artin-Euler constant γ_u have other equivalent definitions such as

$$\beta_u = \lim_{x\to\infty} \left(\sum_{p\leq x, p\in\mathcal{P}_u} \frac{1}{p} - \alpha_u \log\log x\right) \quad \text{and} \quad \beta_u = \gamma_u - \sum_{p\in\mathcal{P}_u,}\sum_{k\geq 2} \frac{1}{kp^k}, \tag{18}$$

respectively. These constants satisfy $\beta_u = \beta_1\alpha_u$ and $\gamma_u = \gamma\alpha_u$. If the density $\alpha_u = 1$, these definitions reduce to the usual Euler constant and the Mertens constant, which are defined by the limits

$$\gamma = \lim_{x\to\infty} \left(\sum_{p\leq x} \frac{\log p}{p-1} - \log x\right) \text{ and } \beta_1 = \lim_{x\to\infty} \left(\sum_{p\leq x} \frac{1}{p} - \log\log x\right), \tag{19}$$

or some other equivalent definitions, respectively. Moreover, the linear independence relation in (18) becomes $\beta = \gamma - \sum_{p\geq 2}\sum_{k\geq 2}\left(kp^k\right)^{-1}$, see [11, Theorem 427].

A numerical experiment for the primitive root $u = 2$ gives the approximate values

(i) $\alpha_2 = \displaystyle\prod_{p\geq 2}\left(1 - \frac{1}{p(p-1)}\right) = 0.3739558667768911078453786\ldots.$

(ii) $\beta_2 \approx \displaystyle\sum_{p\leq 1000, p\in\mathcal{P}_2} \frac{1}{p} - \alpha_2 \log\log x = 0.32864452558480537499995 6\ \ldots$, and

(iii) $\gamma_2 \approx \displaystyle\sum_{p\leq 1000, p\in\mathcal{P}_2} \frac{\log p}{p-1} - \alpha_2 \log x = 0.4249022733662347457966 16\ldots.$

Lemma 5.2. *Assume the generalized Riemann hypothesis, and let $x \geq 1$ be a large number. Then, there exists a pair of constants $\gamma_u > 0$ and $\nu_u > 0$ such that*

(i) $\displaystyle\prod_{p\leq x, p\in\mathcal{P}_u}\left(1 - \frac{1}{p}\right)^{-1} = e^{\gamma_u}\log(x)^{\alpha_u} + O\left(\frac{\log\log x}{\log x}\right).$

(ii) $\displaystyle\prod_{p\leq x, p\in\mathcal{P}_u}\left(1 + \frac{1}{p}\right) = e^{\gamma_u}\prod_{p\in\mathcal{P}_u}\left(1 - p^{-2}\right)\log(x)^{\alpha_u} + O\left(\frac{\log\log x}{\log x}\right).$

(iii) $\displaystyle\prod_{p\leq x, p\in\mathcal{P}_u}\left(1 - \frac{\log p}{p-1}\right)^{-1} = e^{\nu_u - \gamma_u}x^{\alpha_u} + O\left(\frac{x^{\alpha_u}\log\log x}{\log x}\right).$

Proof. (i). Express the logarithm of the product as

$$\sum_{p\leq x, p\in\mathcal{P}_u}\log\left(1 - \frac{1}{p}\right)^{-1} = \sum_{p\leq x, p\in\mathcal{P}_u,\, k\geq 1}\sum \frac{1}{kp^k} = \sum_{p\leq x, p\in\mathcal{P}_u}\frac{1}{p} + \sum_{p\leq x, p\in\mathcal{P}_u,\, k\geq 2}\sum\frac{1}{kp^k}. \tag{20}$$

Apply Lemma 5.1 to complete the verification. For statements (ii) and (iii), use similar methods as in the first one.

The constant $\nu_u > 0$ is defined by the double power series (an approximate numerical value for set $\mathcal{P}_2 = \{3, 5, 11, 13, ...\}$ is shown):

$$\nu_2 = \sum_{p\in\mathcal{P}_2,\, k\geq 2}\sum \frac{1}{k}\left(\frac{\log p}{p-1}\right)^k \approx 0.16350778157097156740800 3...\ . \tag{21}$$

6. Density Correction Factor

The sporadic subsets of Abel-Wieferich primes, see [31, p. 333] for other details, have roles in the determination of the densities of the subsets of integers

$$\mathcal{N}_u = \{n \in \mathbb{N} : \operatorname{ord}_n(u) = \lambda(n)\} \tag{22}$$

with fixed primitive roots $u \in \mathbb{Z}$. The prime product arising from the sporadic existence of the Abel-Wieferich primes $p \geq 3$ is reformulated in the equivalent expression

$$\begin{aligned} P(x) &= \prod_{\substack{p^k \leq x,\\ \operatorname{ord}_p(u)=p-1,\\ \operatorname{ord}_{p^2}(u)\neq p(p-1)}} \left(1+\frac{1}{p}\right) \prod_{\substack{p^k \leq x,\\ \operatorname{ord}_{p^2}(u)=p(p-1)}} \left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right) \\ &= \prod_{p \leq x, p \in \mathcal{W}} \left(1-\frac{1}{p^2}\right) \prod_{p \leq x, p \in \mathcal{P}_u} \left(1-\frac{1}{p}\right)^{-1} + O\left(\frac{1}{x}\right) \\ &= \prod_{p \in \mathcal{W}} \left(1-\frac{1}{p^2}\right) \prod_{p \leq x, p \in \mathcal{P}_u} \left(1-\frac{1}{p}\right)^{-1} + O\left(\frac{1}{x}\right). \end{aligned} \tag{23}$$

Note that the subset of primes has the disjoint partition

$$\mathcal{P}_u = \{p \in \mathbb{P} : \operatorname{ord}_p(u) = p-1\} = \mathcal{W} \cup \overline{\mathcal{W}}, \tag{24}$$

where

$$\mathcal{W} = \left\{p \in \mathbb{P} : \operatorname{ord}_p(u) \mid p-1,\ \operatorname{ord}_{p^2}(u) \neq p(p-1)\right\} \tag{25}$$

and

$$\overline{\mathcal{W}} = \left\{p \in \mathbb{P} : \operatorname{ord}_{p^2}(u) = p(p-1)\right\}. \tag{26}$$

The convergent partial product (23) is replaced with the approximation

$$\prod_{p \leq x, p \in \mathcal{W}} \left(1-\frac{1}{p^2}\right) = \prod_{p \in \mathcal{W}} \left(1-\frac{1}{p^2}\right) + O\left(\frac{1}{x}\right). \tag{27}$$

For $u = 2$, the subset of primes $\mathcal{W}$ is the subset of Wieferich primes. This subset of primes is usually characterized in terms of the congruence

$$\left\{p \in \mathbb{P} : 2^{p-1} \equiv 1 \bmod p^2\right\} = \{1093, 3511, ...\}. \tag{28}$$

Given a fixed $u \neq \pm 1, v^2$, the product $\prod_{p \in \mathcal{W}} \left(1 - p^{-2}\right)$ reduces the density to compensate for those primes for which the primitive root $u \bmod p$ cannot be extended to a primitive root $u \bmod p^2$. This seems to be a density correction factor similar to the case for primitive roots over the prime numbers. The correction required for certain densities of primes with respect to fixed primitive roots over the primes was discovered by the Lehmers, see [32].

7. The Proof Of The Theorem

The result below has served as the foundation for various other results about primitive roots. Most recently, it was used to prove the existence of infinite sequences of primes with fixed prime roots, and bounded gaps, confer [3].

Theorem 7.1. ([13]) *If it be assumed that the extended Riemann hypothesis hold for the Dedekind zeta function over Galois fields of the type $\mathbb{Q}\left(\sqrt[d]{u},\ \sqrt[n]{1}\right)$, where n is a squarefree integer, and $d \mid n$. For a given nonzero integer $u \neq \pm 1, v^2$, let $N_u(x)$ be the number of primes $p \leq x$ for which u is a primitive root modulo p. Let $u = u_1^m \cdot u_2^2$, where $u_1 > 1$ is squarefree, and $m \geq 1$ is odd. Then, there is a constant $\alpha_u \geq 0$ such that*

$$N_u(x) = \alpha_u \frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x}\right) \quad \textit{as } x \longrightarrow \infty. \tag{29}$$

Proof. (Theorem 1.1) By the generalized Riemann hypothesis or Theorem 7.1, the density $\alpha_2 = \delta\left(\mathcal{P}_2\right) > 0$ of the subset of primes $\mathcal{P}_2$ is nonzero. Put $\tau = \alpha_2$ in Wirsing formula, Lemma 4.1, and replace the characteristic function $f(n)$ of primitive roots in the finite ring $\mathbb{Z}\left/p^k\right.\mathbb{Z}, k \geq 1$, see Lemma 4.1, to produce

$$\begin{aligned}
\sum_{n \leq x} f(n) \quad &= \quad \left(\frac{1}{e^{\gamma\tau}\Gamma(\tau)} + o(1)\right) \frac{x}{\log x} \prod_{p^k \leq x} \left(1 + \frac{f(p)}{p} + \frac{f\left(p^2\right)}{p^2} + \cdots\right) \\
&= \quad \left(\frac{1}{e^{\gamma\alpha_2}\Gamma\left(\alpha_2\right)} + o(1)\right) \frac{x}{\log x} \\
&\quad \times \prod_{\substack{p^k \leq x, \\ \mathrm{ord}(2) = p-1, \\ \mathrm{ord}(2) \neq p(p-1)}} \left(1 + \frac{1}{p}\right) \prod_{\substack{p^k \leq x, \\ \mathrm{ord}(2) = p(p-1)}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right).
\end{aligned} \tag{30}$$

In equation (30), line 1, the product over the prime powers $p^k \leq x$ is broken up into two subproducts. In equation (30), line 2, the first subproduct is restricted to the subset of Wieferich prime powers which do not satisfy the completely multiplicative property $f(p^2) \neq f(p)f(p)$ of the characteristic function; the second subproduct is restricted to the subset of nonWieferich prime powers which do satisfy the completely multiplicative property $f(p^2) = f(p)f(p)$ of the characteristic function, Lemma 3.1.

Replacing the equivalent product, see (23) in Section 6, and using Lemma 5.2, yield

$$\sum_{n \leq x} f(n) \quad = \quad \left(\frac{1}{e^{\gamma\alpha_2}\Gamma\left(\alpha_2\right)} + o(1)\right) \frac{x}{\log x} \prod_{p \in \mathcal{W}} \left(1 - \frac{1}{p^2}\right) \prod_{p^k \leq x,\ p \in \mathcal{P}_u} \left(1 - \frac{1}{p}\right)^{-1}$$

$$= \left(\frac{e^{\gamma_2 - \gamma \alpha_2}}{\Gamma(\alpha_2)} + o(1) \right) \frac{x}{(\log x)^{1-\alpha_2}} \prod_{p \in \mathcal{W}} \left(1 - \frac{1}{p^2} \right), \tag{31}$$

where γ_2 is the Artin-Euler constant, see Lemmas 5.1 and 5.2 for details. Lastly, the error term $o\left(x(\log x)^{\alpha_2 - 1}\right)$ absorbs all the errors. Quod erat demonstrandum.

7.1. Summary

This note proves a generalization of Hooley theorem for fixed primitive root $u \neq \pm 1, v^2$ modulo the prime numbers $p \geq 2$, see Theorem 7.1, to Theorem 1.1 for fixed primitive root $u \neq \pm 1, v^2$ in the maximal cyclic groups $G \subset \mathbb{Z}/n\mathbb{Z}$ modulo the integers $n \geq 2$. This technique uses a new characteristic function for primitive roots in the rings $\mathbb{Z}/p^k\mathbb{Z}$, see Lemma 3.1 , and a new application of Wirsing theorem, see Lemma 4.1. Furthermore, the corresponding generalizations for the Euler constant and the Mertens constant are included in Lemma 5.1.

References

[1] Apostol, Tom M. Introduction to analytic number theory. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[2] Balog, Antal; Cojocaru, Alina-Carmen; David, Chantal. Average twin prime conjecture for elliptic curves. Amer. J. Math. 133,(2011), no. 5, 1179-1229.

[3] Roger C. Baker, Paul Pollack, Bounded gaps between primes with a given primitive root, II, arXiv:1407.7186.

[4] Carmichael, R. D. Note on a new number theory function. Bull. Amer. Math. Soc. 16 (1910), no. 5, 232-238.

[5] Peter J. Cameron and D. A. Preece, Notes on primitive lambda-roots, http://www.maths.qmul.ac.uk/˜pjc/csgnotes/lambda.pdf

[6] Joseph Cohen, Primitive roots in quadratic fields, II, Journal of Number Theory 124 (2007) 429-441.

[7] H. Davenport, On Primitive Roots in Finite Fields, Quarterly J. Math. 1937, 308-312.

[8] Rainer Dietmann, Christian Elsholtz, Igor E. Shparlinski, On Gaps Between Primitive Roots in the Hamming Metric, arXiv:1207.0842.

[9] Paul Erdos, Harold N. Shapiro, On The Least Primitive Root Of A Prime, 1957, euclidproject.org.

[10] Gupta, Rajiv; Murty, M. Ram. A remark on Artin's conjecture. Invent. Math. 78 (1984), no. 1, 127-130.

[11] Hardy, G. H.; Wright, E. M. An introduction to the theory of numbers. Sixth edition. Revised by D. R. Heath-Brown and J. H. Silverman. With a foreword by Andrew Wiles. Oxford University Press, 2008.

[12] Hildebrand, Adolf. Quantitative mean value theorems for nonnegative multiplicative functions. II. Acta Arith. 48 (1987), no. 3, 209-260.

[13] C. Hooley, On Artins conjecture, J. Reine Angew. Math. 225, 209-220, 1967.

[14] Li, Shuguang; Pomerance, Carl. Primitive roots: a survey. Number theoretic methods, Iizuka, 2001, 219-231, Dev. Math., 8, Kluwer Acad. Publ., Dordrecht, 2002.

[15] Li, Shuguang; Pomerance, Carl. On generalizing Artin's conjecture on primitive roots to composite moduli. J. Reine Angew. Math. 556 (2003), 205-224.

[16] Iwaniec, Henryk; Kowalski, Emmanuel. Analytic number theory. AMS Colloquium Publications, 53. American Mathematical Society, Providence, RI, 2004.

[17] Konyagin, Sergei V.; Shparlinski, Igor E. On the consecutive powers of a primitive root: gaps and exponential sums. Mathematika 58 (2012), no. 1, 11-20.

[18] H. W. Lenstra Jr, P. Moree, P. Stevenhagen, Character sums for primitive root densities, arXiv:1112.4816.

[19] Lenstra, H. W., Jr. On Artin conjecture and Euclid algorithm in global fields. Invent. Math. 42, (1977), 201-224.

[20] Lidl, Rudolf; Niederreiter, Harald. Finite fields. With a foreword by P. M. Cohn. Second edition. Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997.

[21] Moree, Pieter. Counting numbers in multiplicative sets: Landau versus Ramanujan. Math. Newsl. 21 (2011), no. 3, 73-81.

[22] Pieter Moree. Artin's primitive root conjecture -a survey. arXiv:math/0412262.

[23] Montgomery, Hugh L.; Vaughan, Robert C. Multiplicative number theory. I. Classical theory. Cambridge University Press, Cambridge, 2007.

[24] Narkiewicz, W. The development of prime number theory. From Euclid to Hardy and Littlewood. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000.

[25] Pappalardi, Francesco; Saidak, Filip; Shparlinski, Igor E. Square-free values of the Carmichael function. J. Number Theory 103 (2003), no. 1, 122-131.

[26] Pappalardi, Francesco; Susa, Andrea. An analogue of Artin conjecture for multiplicative subgroups of the rationals. Arch. Math. (Basel) 101, (2013), no. 4, 319-330.

[27] A. G. Postnikov, Introduction to analytic number theory, Translations of Mathematical Monographs, vol. 68, American Mathematical Society, Providence, RI, 1988.

[28] Paszkiewicz, A. A new prime p for which the least primitive root $\mod p$ and the least primitive root $\text{mod} p^2$ are not equal. Math. Comp. 78 (2009), no. 266, 1193-1195.

[29] Roskam, Hans. Artin primitive root conjecture for quadratic fields. J. Theory Nombres Bordeaux, 14, (2002), no. 1, 287-324.

[30] Rose, H. E. A course in number theory. Second edition. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1994.

[31] Ribenboim, Paulo, The new book of prime number records, Berlin, New York: Springer-Verlag, 1996.

[32] Stevenhagen, Peter. The correction factor in Artin's primitive root conjecture. Les XXII emes Journees Arithmetiques (Lille, 2001). J. Theor. Nombres Bordeaux 15 (2003), no. 1, 383-391.

[33] G. Tenenbaum, Introduction to analytic and probabilistic number theory, Cambridge Studies in Advanced Mathematics 46, Cambridge University Press, Cambridge, 1995.

[34] Stephens, P. J. An average result for Artin conjecture. Mathematika 16, (1969), 178-188.

[35] Vaughan, R. C. Some applications of Montgomery's sieve. J. Number Theory 5 (1973), 64-79.

[36] E. Wirsing, Das asymptotische Verhalten von Summen uber multiplikative Funktionen, Math. Ann. 143 (1961) 75-102.

[37] Williams, Kenneth S. Note on integers representable by binary quadratic forms. Canad. Math. Bull. 18 (1975), no. 1, 123-125.