International Journal of Mathematics and
Computer Science, **11**(2016), no. 2, 89–108

Densities of Primes and Primitive Roots

Nelson A. Carella

Department of Mathematics
York College
The City University of New York
Jamaica, NY, USA

email: pobox5050@live.com

(Received July 22, 2016, Accepted August 12, 2016)

Abstract

Let $u \neq \pm 1, v^2$ be a fixed integer, let p be a prime number, and let $\mathrm{ord}_p(u) = d|p-1$ be the order of u mod p. This note provides a lower bound $\#\{p \leq x : \mathrm{ord}_p(u) = p-1\} \gg x(\log x)^{-1}$ for the number of primes $p \leq x$ with a fixed primitive root $u \bmod p$ for all large numbers $x \geq 1$. The current results in the literature have the lower bound $\#\{p \leq x : \mathrm{ord}_p(u) = p-1\} \gg x(\log x)^{-2}$, and restrictions on the fixed primitive root to a subset of at least three or more integers.

1 Introduction

As usual, $\mathbb{Z} = \{0, \pm 1, \pm 2, ...\}$ is the set of integers. The symbol $\mathbb{P} = \{2, 3, 5, ...\}$ denotes the set of prime numbers. The constant $c_u \geq 0$ is the density of the subset of primes.

$$\mathcal{P}_u = \{p \in \mathbb{P} : \mathrm{ord}_p(u) = p-1\} \subset \mathbb{P} \tag{1}$$

with a fixed primitive root $u \in \mathbb{Z}$. Let $u \neq \pm 1, v^2$ be a fixed integer, and let $x \geq 1$ be a large number. The expected number of primes $p \leq x$ with a fixed

Key words and phrases: Prime Number; Primitive Root; Artin Primitive Root.
AMS (MOS) Subject Classifications: Primary 11A07, Secondary 11N37.
ISSN 1814-0432, 2016, http://ijmcs.future-in-tech.net

primitive root u mod p has the asymptotic formula

$$\pi_u(x) = \#\left\{p \leqslant x : \mathrm{ord}_p(u) = p-1\right\} = c_u \mathrm{li}(x) + O\left(x(\log x)^{-2}\right), \quad (2)$$

where $\mathrm{li}(x)$ is the logarithm integral, as $x \to \infty$.

A conditional proof of this result was achieved in [16] with simplified sketches of the proof appearing in [22, p. 8] and similar references. The determination of the constant $c_u \geq 0$ for a fixed integer $u \in \mathbb{Z}$ is an interesting technical problem, [16, p. 218], [19], [20]. An introduction to its historical development and its calculations is covered in [22, pp. 3–10], and [29].

The Artin primitive root conjecture on average is

$$x^{-1}\sum_{u \leqslant x} \pi_u(x) = a_0 \mathrm{li}(x) + O\left(x(\log x)^{-B}\right), \quad (3)$$

where $a_0 = \prod_{p \geq 2}\left(1 - p^{-1}(p-1)^{-1}\right)$ is Artin constant and $B > 1$ is an arbitrary number, was proved in [13] unconditionally, and refined in [29]. These works had shown that almost all admissible integers $u \in \mathbb{Z} - \{-1, 1, v^2 : v \in \mathbb{Z}\}$ are primitive roots for infinitely many primes. The number of exceptions is a subset of zero density in $\mathbb{Z}$. The individual quantity $\pi_u(x)$ in (1.2) can be slightly different from the average quantity in (1.3). The variations, discovered by the Lehmers using numerical experiments, depend on the primes decomposition of the fixed value u, see [16, p. 220], [22, p. 3]and similar references for the exact formula for the density $c_u \geq 0$.

There is no known infinite sequence of primes with a fixed primitive root. The current literature has results on infinite sequences of primes with unknown primitive root in a small finite set. For example, in [14] it was proved that for a fixed primes triple q, r, s, the subset of integers

$$\mathcal{A}(q,r,s) = \left\{q^a r^b s^c : 0 \leq a, b, c \leq 3\right\}, \quad (4)$$

contains a primitive root for infinitely many primes. This result was later reduced to the smaller subset

$$\mathcal{B}(q,r,s) = \left\{q^a r^b s^c : 0 \leq a, b, c \leq 1\right\}, \quad (5)$$

see [15]. In both of these results, the lower bound for the number of primes

$p \le x$ with a fixed primitive root in either of the subset $\mathcal{A}(q,r,s)$ or $\mathcal{B}(q,r,s)$ has the lower bound $\#\{p \le x : \mathrm{ord}_p(u) = p-1\} \gg x(\log x)^{-2}$ for all large number $x \ge 1$.

These results have been extended to quadratic numbers fields in [7], [25], [28], and most recently in [1]. Other related results are given in [23], [12], [26].

The technique explored in this note provides an improved lower bound for the number of primes $p \le x$ with a fixed primitive root u mod p for all large number $x \ge 1$. The fixed primitive root u is not restricted to a small finite subset such as $\mathcal{A}(q,r,s)$ or $\mathcal{B}(q,r,s)$.

***Theorem* 1.1** *A fixed integer $u \ne \pm 1, v^2$ is a primitive root mod p for infinitely many primes $p \ge 2$. In addition, the density of these primes satisfies*

$$\pi_u(x) = \#\{p \le x : \mathrm{ord}_p(u) = p-1\} = c_u \mathrm{li}(x) + O\left(x(\log x)^{-2}\right), \quad (6)$$

where $li(x)$ is the logarithm integral, and $c_u > 0$ is a constant, for all large numbers $x \ge 1$.

The next five sections collect the notations and some standard results related to or applicable to the investigation of primitive roots in cyclic groups. The last section presents a proof of Theorem 1.1.

2 Exponential and Character Sums

A few standard definitions and other basic results in the theory of exponential and character sums are reviewed in this Section. All the estimates are unconditional.

2.1 Simple Characters Sums

Let G be a finite group of order $q = \#G$. The order $\mathrm{ord}(u)$ of an element $u \in G$ is the smallest integer $d|q$ such that $u^d = 1$. An element $\tau \in G$ is called a *primitive element* if it has order $\mathrm{ord}(\tau) = q$. A cyclic group G is

a group generated by a primitive element $\tau \in G$. Given a primitive root $\tau \in G$, every element $0 \neq u \in G$ in a cyclic group has a representation as $u = \tau^v, 0 \leq v < q$. The integer $v = \log u$ is called the *discrete logarithm* of $u \neq 0$ with respect to τ.

A character χ modulo $q \geq 2$, is a complex-valued periodic function $\chi : \mathbb{N} \longrightarrow \mathbb{C}$, and it has order $\text{ord}(\chi) = d \geqslant 1$ if and only if $\chi(n)^d = 1$ for all integers $n \in \mathbb{N}, \gcd(n, q) = 1$. For $q \neq 2^r, r \geq 2$, a multiplicative character χ of order $\text{ord}(\chi) = d|q$ has a representation as

$$\chi(u) = e^{i2\pi k \log u/(p-1)}, \tag{7}$$

where $v = \log u$ is the discrete logarithm of $u \neq 0$ with respect to some primitive root, and for some $k \geq 1$, see [21, p. 187], [24, p. 118], and [17, p. 271] for more details.

Lemma 2.1. *For a fixed integer $u \neq 0$, and an integer $q \in \mathbb{N}$, let $\chi \neq 1$ be nonprincipal character mod q, then*

$$\text{(i)} \sum_{\text{ord}(\chi)=\varphi(q)} \chi(u) = \begin{cases} \varphi(q) & \text{if } u \equiv 1 \bmod q, \\ -1 & \text{if } u \not\equiv 1 \bmod q. \end{cases}$$

$$\text{(ii)} \sum_{1 \leq a < \varphi(q)} \chi(au) = \begin{cases} \varphi(q) & \text{if } u \equiv 1 \bmod q, \\ -1 & \text{if } u \not\equiv 1 \bmod q. \end{cases}$$

An additive character ψ of order $\text{ord}(\psi) = q$ has a representation as

$$\psi(n) = e^{i2\pi kn/q}, \tag{8}$$

for some $k \geq 1, \gcd(k, q) = 1$, see [21, p. 187], [24, p. 118], and [17, p. 271]. The additive character sums are quite similar to Lemma 2.1.

Lemma 2.2. *For a fixed integer u, and an integer $q \in \mathbb{N}$, let ψ be an additive character of order $\text{ord}\psi = q$, then*

$$\text{(i)} \sum_{\text{ord}(\psi)=q} \psi(u) = \begin{cases} q & \text{if } u \equiv 0 \bmod q, \\ 0 & \text{if } u \not\equiv 0 \bmod q. \end{cases}$$

$$\text{(ii)} \sum_{0 \leq a < q} \psi(au) = \begin{cases} q & \text{if } u \equiv 0 \bmod q, \\ 0 & \text{if } u \not\equiv 0 \bmod q. \end{cases}$$

3 Representations of the Characteristic Function

The characteristic function $\Psi : G \longrightarrow \{0, 1\}$ of primitive elements is one of the standard analytic tools employed to investigate the various properties of primitive roots in cyclic groups G. Many equivalent representations of the characteristic function Ψ of primitive elements are possible.

3.1 Divisors Dependent Characteristic Function

A representation of the characteristic function dependent on the orders of the cyclic groups is given below. This representation is sensitive to the primes decompositions $q = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, with p_i prime and $e_i \geq 1$, of the orders of the cyclic groups $q = \#G$.

Lemma 3.1. *Let G be a finite cyclic group of order $p - 1 = \#G$, and let $0 \neq u \in G$ be an invertible element of the group. Then*

$$\Psi(u) = \frac{\varphi(p-1)}{p-1} \sum_{d|p-1} \frac{\mu(d)}{\varphi(d)} \sum_{\mathrm{ord}(\chi)=d} \chi(u) = \begin{cases} 1 & \text{if } \mathrm{ord}_p u = p-1, \\ 0 & \text{if } \mathrm{ord}_p u \neq p-1. \end{cases} \tag{9}$$

The works in [8], and [32] attribute this formula to Vinogradov. The proof and other details on the characteristic function are given in [10, p. 863], [21, p. 258], [22, p. 18]. The characteristic function for multiple primitive roots is used in [6, p. 146] to study consecutive primitive roots. In [9] it is used to study the gap between primitive roots with respect to the Hamming metric. And in [32] it is used to prove the existence of primitive roots in certain small subsets $A \subset \mathbb{F}_p$. In [8] it is used to prove that some finite fields do not have primitive roots of the form $a\tau + b$, with τ primitive and $a, b \in \mathbb{F}_p$ constants.

3.2 Divisors Free Characteristic Function

It often difficult to derive any meaningful result using the usual divisors dependent characteristic function of primitive elements given in Lemma 3.1. This difficulty is due to the large number of terms that can be generated by the divisors, for example, $d|(p-1)$, involved in the calculations, see [10], [9] for typical applications and [22, p. 19] for a discussion.

A new *divisors-free* representation of the characteristic function of primitive element is developed here. This representation can overcomes some of the limitations of its counterpart in certain applications. The *divisors representation* of the characteristic function of primitive roots, Lemma 3.1, detects the order $\mathrm{ord}_p u$ of the element $u \in \mathbb{F}_p$ by means of the divisors of the totient $p-1$. In contrast, the *divisors-free representation* of the characteristic function, Lemma 3.2, detects the order $\mathrm{ord}_p u \geq 1$ of the element $u \in \mathbb{F}_p$ by means of the solutions of the equation $\tau^n - u = 0$ in $\mathbb{F}_p$, where u, τ are constants, and n is a variable such that $1 \leq n < p-1, \gcd(n, p-1) = 1$. Two versions are given: a multiplicative version, and an additive version.

Lemma 3.2. *Let $p \geq 2$ be a prime, and let τ be a primitive root mod p. For a nonzero element $u \in \mathbb{F}_p$, the followings hold*:

(i) *If $\chi \neq 1$ is a nonprincipal multiplicative character of order $\mathrm{ord}\,\chi = p-1$, then*

$$\Psi(u) = \sum_{\gcd(n,p-1)=1} \frac{1}{p-1} \sum_{0 \leq k < p-1} \chi\left((\tau^n \bar{u})^k\right) = \begin{cases} 1 & \text{if } \mathrm{ord}_p u = p-1, \\ 0 & \text{if } \mathrm{ord}_p u \neq p-1, \end{cases} \tag{10}$$

where $\bar{u}$ is the inverse of u mod p.

(ii) *If $\psi \neq 1$ is a nonprincipal additive character of order $\mathrm{ord}\,\psi = p$, then*

$$\Psi(u) = \sum_{\gcd(n,p-1)=1} \frac{1}{p} \sum_{0 \leq k \leq p-1} \psi\left((\tau^n - u)k\right) = \begin{cases} 1 & \text{if } \mathrm{ord}_p u = p-1, \\ 0 & \text{if } \mathrm{ord}_p u \neq p-1. \end{cases} \tag{11}$$

Proof: (ii) As the index $n \geq 1$ ranges over the integers relatively prime to $p-1$, the element $\tau^n \in \mathbb{F}_p$ ranges over the primitive roots mod p. The

equation $\tau^n - u = 0$ has a solution if and only if the fixed element $u \in \mathbb{F}_p$ is a primitive root. Next, replace $\psi(z) = e^{i2\pi kz/p}$ to obtain

$$\Psi(u) = \sum_{\gcd(n,p-1)=1} \frac{1}{p} \sum_{0\le k\le p-1} e^{i2\pi(\tau^n - u)k/p} = \begin{cases} 1 & \text{if } \mathrm{ord}_p u = p-1, \\ 0 & \text{if } \mathrm{ord}_p u \neq p-1. \end{cases} \tag{12}$$

This follows from Lemma 2.2 applied to the inner sum. For (i), use the equation the equation $\tau^n \bar{u} = 1$, where $\bar{u}$ is the inverse of u, and apply Lemma 2.1. ■

4 Estimates Of Exponential Sums

Exponential sums indexed by the powers of elements of nontrivial orders have applications in mathematics and cryptography. These applications have propelled the development of these exponential sums. There are many results on exponential sums indexed by the powers of elements of nontrivial orders, the interested reader should consult the literature, and references within the cited papers.

The trivial upper bound for the exponential sum in question is

$$\sum_{1\le n\le p-1,\, \gcd(n,p-1)=1} e^{i2\pi a\theta^n/p} < \varphi(p-1) \le \frac{p}{\log\log p} \tag{13}$$

for all integers $p > 3$. In addition there are several nontrivial estimates.

Theorem 4.1. ([4], [3, Theorem 2.1]) (i) Given $\delta > 0$, there is $\epsilon > 0$ such that if $\theta \in \mathbb{F}_p$ is of multiplicative order $t \ge t_1 > p^{-\delta}$, then

$$\max_{1\le a\le p-1} \left| \sum_{1\le m\le t_1} e^{i2\pi a\theta^m/p} \right| < t_1 p^{-\epsilon}. \tag{14}$$

(ii) If $H \subset \mathbb{Z}_N$ is a subset of cardinality $\#H \ge N^\delta, \delta > 0$, then

$$\max_{1\le a\le \varphi(N)} \left| \sum_{x\in H} e^{i2\pi ax/N} \right| < N^{1-\delta}. \tag{15}$$

Other estimates for exponential sum over arbitrary subsets $H \subset \mathbb{F}_p$ are also given in the [18]. For the finite rings $\mathbb{Z}/N\mathbb{Z}$ of the integer modulo $N \geqslant 1$, similar results have been proved [3].

Theorem 4.2. ([11, Lemma 4]) For integers $a, k, N \in \mathbb{N}$, assume that $\gcd(a, N) = c$, and that $\gcd(k, t) = d$.
(i) If the element $\theta \in \mathbb{Z}_N$ is of multiplicative order $t \geq t_0$, then

$$\max_{1\leq a\leq p-1} \left| \sum_{1\leq x\leq t} e^{i2\pi a\theta^x/N} \right| < cd^{1/2}N^{1/2}. \tag{16}$$

(ii) If $H \subset \mathbb{Z}/N\mathbb{Z}$ is a subset of cardinality $\#H \geq N^\delta, \delta > 0$, then

$$\max_{\gcd(a,\varphi(N))=1} \left| \sum_{x\in H} e^{i2\pi a\theta^x/N} \right| < N^{1-\delta}. \tag{17}$$

Theorem 4.3. ([5]) Let $p \geq 2$ be a large prime, and let $x \geq 1$ be a large real number. If the element $\theta \in \mathbb{F}_p$ is of multiplicative order $p-1$, and $a \in \mathbb{Z}, \gcd(a, p) = 1$ constant, then

$$\max_{\gcd(a,\varphi(N))=1} \left| \sum_{x\in H} e^{i2\pi a\theta^x/N} \right| < N^{1-\delta}. \tag{18}$$

5 Estimates For The Error Term

The upper bounds of exponential sums over subsets of elements in finite rings $(\mathbb{Z}/N\mathbb{Z})^\times$ stated in the last Section are used to estimate the error term $E(x)$ in the proof of Theorem 1.1. Two estimates will be considered. The first one in Lemma 5.1 is based on the trivial upper bound (4.13); and the second estimate in Lemma 5.2 is based the nontrivial results in Theorems 4.1, 4.2, and 4.3.

Lemma 5.1. *Let $p \geq 2$ be a large prime, let $\psi \neq 1$ be an additive character, and let τ be a primitive root mod p. If the element $u \neq 0$ is not a primitive root, then,*

$$\sum_{x \leq p \leq 2x} \frac{1}{p} \sum_{\gcd(n,p-1)=1,\ 0<k\leq p-1} \psi\left((\tau^n - u)k\right) \ll \frac{x}{(\log\log x)(\log x)} \tag{19}$$

for all sufficiently large numbers $x \geq 1$.

Proof: By hypothesis $u \neq \tau^n$ for any $n \geq 1$ such that $\gcd(n, p-1) = 1$. Therefore,

$$\sum_{x \leq p \leq 2x,} \frac{1}{p} \sum_{\gcd(n,p-1)=1,\ 0<k\leq p-1} \psi\left((\tau^n - u)k\right) < \sum_{x \leq p \leq 2x} \frac{p-1}{p} < \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right). \tag{20}$$

This implies that there is a nontrivial upper bound. To sharpen this upper bound, let $\psi(z) = e^{i2\pi kz/p}$ with $0 < k < p$, and rearrange the triple finite sum in the following way:

$$\sum_{x \leq p \leq 2x,} \frac{1}{p} \sum_{0<k\leq p-1,\ \gcd(n,p-1)=1} \sum \psi((\tau^n - u)k) \leq \sum_{x \leq p \leq 2x} \frac{1}{p} \left| \sum_{0<k\leq p-1} e^{-i2\pi uk/p} \sum_{\gcd(n,p-1)=1} e^{i2\pi k\tau^n/p} \right|. \tag{21}$$

and let

$$U_p = \sum_{0<k\leq p-1} e^{-i2\pi uk/p} \qquad \text{and} \qquad V_p = \frac{1}{p} \sum_{\gcd(n,p-1)=1} e^{i2\pi k\tau^n/p}. \tag{22}$$

The Holder inequality $||AB||_1 \leq ||A||_\infty \cdot ||B||_1$ takes the form

$$\sum_{x \leq p \leq 2x} |U_p V_p| \leq \max_{x \leq p \leq 2x} |U_p| \cdot \sum_{x \leq p \leq 2x} |V_p|. \tag{23}$$

The maximal absolute value of the exponential sum U_p is given by

$$\max_{x \leq p \leq 2x} |U_p| = \max_{x \leq p \leq 2x} \left| \sum_{0<k\leq p-1} e^{-i2\pi uk/p} \right| = 1. \tag{24}$$

This follows from $\sum_{0<k\leq p-1} e^{i2\pi uk/p} = -1$, refer to Lemma 2.2.

The trivial absolute value of the exponential sum $V_p = V_p(k)$ is given by

$$|V_p| = \left| \frac{1}{p} \sum_{\gcd(n,p-1)=1} e^{i2\pi k\tau^n} \right| \leq \frac{1}{p} \cdot \frac{p}{\log\log p} = \frac{1}{\log\log p}, \tag{25}$$

since $\varphi(n) \leq n/\log\log n$ for all $n \geq 3$. The corresponding 1-norm is

$$\sum_{x\leq p\leq 2x} |V_p| \leq \sum_{x\leq p\leq 2x} \frac{1}{\log\log p} \leq \frac{1}{\log\log x} \sum_{x\leq p\leq 2x} 1 \ll \frac{x}{(\log\log x)(\log x)}. \tag{26}$$

Now, replace the estimates (5.24) and (5.26) into (5.21), the Holder inequality, to reach

$$\sum_{x\leq p\leq 2x} \frac{1}{p} \left| \sum_{0<k\leq p-1} e^{-i2\pi uk/p} \sum_{\gcd(n,p-1)=1} e^{i2\pi k\tau^n/p} \right| \leq \max_{x\leq p\leq 2x} |U_p| \cdot \sum_{x\leq p\leq 2x} |V_p|$$

$\ll \frac{x}{(\log\log x)(\log x)}$.
This completes the verification. ■

An application of any of the Theorems 4.1, or 4.2 or 4.3 leads to a sharper result, this is completed below.

Lemma 5.2. *Let $p \geq 2$ be a large prime, let $\psi \neq 1$ be an additive character, and let τ be a primitive root mod p. If the element $u \neq 0$ is not a primitive root, then,*

$$\sum_{p\leq x} \frac{1}{p} \sum_{\gcd(n,p-1)=1,\ 0<k\leq p-1} \psi\left((\tau^n - u)k\right) \ll x^{1-\varepsilon} \tag{27}$$

for all sufficiently large numbers $x \geq 1$ and an arbitrarily small number $\varepsilon > 0$.

Proof: By hypothesis $u \neq \tau^n$ for any $n \geq 1$ such that $\gcd(n, p-1) = 1$. Therefore,

$$\sum_{p\leq x,} \frac{1}{p} \sum_{\gcd(n,p-1)=1,\ 0<k\leq p-1} \psi\left((\tau^n - u)k\right) < \sum_{p\leq x} \frac{p-1}{p} < \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right). \tag{28}$$

This implies that there is a nontrivial upper bound. To sharpen this upper bound, let $\psi(z) = e^{i2\pi kz/p}$ with $0 < k < p$, and rearrange the triple finite sum in the form

$$\sum_{p\le x,}\frac{1}{p}\sum_{0<k\le p-1,\ \gcd(n,p-1)=1}\ \sum \psi((\tau^n-u)k) \le \sum_{p\le x}\frac{1}{p}\left|\sum_{0<k\le p-1} e^{-i2\pi uk/p}\sum_{\gcd(n,p-1)=1} e^{i2\pi k\tau^n/p}\right|, \tag{29}$$

and let

$$U_p = \frac{1}{p^{1/2}}\sum_{0<k\le p-1} e^{-i2\pi uk/p} \qquad \text{and} \qquad V_p = \frac{1}{p^{1/2}}\sum_{\gcd(n,p-1)=1} e^{i2\pi k\tau^n/p}. \tag{30}$$

Now consider the Holder inequality $||AB||_1 \le ||A||_r \cdot ||B||_s$ with $1/r+1/s = 1$. In terms of the components in (5.30) this inequality has the explicit form

$$\sum_{2\le p\le x}|U_pV_p| \le \left(\sum_{2\le p\le x}|U_p|^r\right)^{1/r}\left(\sum_{2\le p\le x}|V_p|^s\right)^{1/s}. \tag{31}$$

The absolute value of the first exponential sum U_p is given by

$$|U_p| = \left|\frac{1}{p^{1/2}}\sum_{0<k\le p-1} e^{-i2\pi uk/p}\right| = \frac{1}{p^{1/2}}. \tag{32}$$

This follows from $\sum_{0<k\le p-1} e^{i2\pi uk/p} = -1$, refer to Lemma 2.2. The corresponding r-norm is

$$\sum_{p\le x}|U_p|^r = \sum_{2\le p\le x}\left|\frac{1}{p^{1/2}}\right|^r \le x^{1-r/2}. \tag{33}$$

The finite sum over the primes is estimated using integral

$$\sum_{p\le x}\frac{1}{p^{r/2}} \ll \int_1^x \frac{1}{t^{r/2}}d\pi(t) = O(x^{1-r/2}), \tag{34}$$

where $\pi(x) = x/\log x + O(x/\log^2 x)$ is the prime counting measure.

The absolute value of the second exponential sum $V_p = V_p(k)$ is given by

$$|V_p| = \left| \frac{1}{p^{1/2}} \sum_{\gcd(n,p-1)=1} e^{i2\pi k\tau^n} \right| \leq p^{1/2-\varepsilon}. \tag{35}$$

This exponential sum dependents on k; but it has a uniform, and independent of k upper bound

$$\sum_{\gcd(n,p-1)=1,} e^{i2\pi k\tau^n/p} \leq \max_{1\leq k\leq p-1} \left| \sum_{m\in H} e^{i2\pi km/p} \right| \leq p^{1-\varepsilon}, \tag{36}$$

where $H = \{\tau^n : 1 \leq n \leq p-2, \text{ and } \gcd(n, p-1) = 1\}$, and $\varepsilon > 0$ is an arbitrarily small number, see Theorem 4.1 or 4,2 or 4.3.

The corresponding s-norm is

$$\sum_{p\leq x} |V_p|^s \leq \sum_{2\leq p\leq x} \left|p^{1/2-\varepsilon}\right|^s \leq x^{1+s/2-\varepsilon s}. \tag{37}$$

The finite sum over the primes is estimated using integral

$$\sum_{p\leq x} p^{s/2-\varepsilon s} \ll \int_1^x t^{s/2-\varepsilon s} d\pi(t) = O(x^{1+s/2-\varepsilon s}). \tag{38}$$

Now, replace the estimates (5.33) and (5.37) into (5.29), the Holder inequality, to reach

$$\begin{aligned} \sum_{p\leq x} \frac{1}{p} \left| \sum_{0<k\leq p-1} e^{-i2\pi uk/p} \sum_{\gcd(n,p-1)=1} e^{i2\pi k\tau^n/p} \right| &\leq \left(\sum_{2\leq p\leq x} |U_p|^r \right)^{1/r} \left(\sum_{2\leq p\leq x} |V_p|^s \right)^{1/s} \\ &\ll \left(x^{1-r/2}\right)^{1/r} \left(x^{1+s/2-\varepsilon s}\right)^{1/s} \\ &\ll \left(x^{1/r-1/2}\right) \left(x^{1/s+1/2-\varepsilon}\right) \\ &\ll x^{1/r+1/s-\varepsilon} \\ &\ll x^{1-\varepsilon}. \end{aligned} \tag{39}$$

Note that this result is independent of the parameter $1/r + 1/s = 1$. ■

6 Evaluation Of The Main Term

Finite products over the primes numbers occur on various problems concerned with primitive roots. These products involve the normalized totient function $\varphi(n)/n = \prod_{p|n}(1 - 1/p)$ and the corresponding estimates, and the asymptotic formulas.

Lemma 6.1. ([30], [31]) *Let $x \geq 1$ be a large number, and let $\varphi(n)$ be the Euler totient function. For $k \geq 1$, the kth moment*

$$\sum_{p\leq x}\left(\frac{\varphi(p-1)}{p-1}\right)^k = \mathrm{li}(x)\prod_{p\geq 2}\left(1-\frac{\left(1-(1-1/p)^k\right)}{(p-1)}\right)+O\left(\frac{x}{\log^B x}\right), \quad (40)$$

where li(x) is the logarithm integral, and $B > 1$ is a constant, as $x \to \infty$.

The case $k = 1$ is ubiquitous in various results in Number Theory. Slightly different form occur in the proof of Theorem 1.1.

Lemma 6.2. *Let $x \geq 1$ be a large number, and let $\varphi(n)$ be the Euler totient function. Then*

$$\sum_{p\leq x}\frac{1}{p}\sum_{\gcd(n,p-1)=1}1 = \mathrm{li}(x)\prod_{p\geq 2}\left(1-\frac{1}{p(p-1)}\right)+O\left(\frac{x}{\log^B x}\right). \quad (41)$$

Proof: A routine rearrangement gives

$$\begin{aligned}\sum_{p\leq x}\frac{1}{p}\sum_{\gcd(n,p-1)=1}1 &= \sum_{p\leq x}\frac{\varphi(p-1)}{p} \\ &= \sum_{p\leq x}\frac{\varphi(p-1)}{p-1}-\sum_{p\leq x}\frac{\varphi(p-1)}{p(p-1)}.\end{aligned} \quad (42)$$

To proceed, apply Lemma 6.1 to reach

$$\begin{aligned}\sum_{p\leq x}\frac{\varphi(p-1)}{p-1}-\sum_{p\leq x}\frac{\varphi(p-1)}{p(p-1)} &= a_0\mathrm{li}(x)+O\left(\frac{x}{\log^B x}\right)-\sum_{p\leq x}\frac{\varphi(p-1)}{p(p-1)}\\ &= a_0\mathrm{li}(x)+O\left(\frac{x}{\log^B x}\right), \qquad (43)\end{aligned}$$

where the second finite sum is absorbed into the error term, $B>1$ is an arbitrary constant, and the constant $a_0=\prod_{p\geq 2}\left(1-\frac{1}{p(p-1)}\right)$. ■

The logarithm integral has the asymptotic formula

$$\mathrm{li}(x)=\int_2^x\frac{1}{\log z}dz=\frac{x}{\log x}+O\left(\frac{x}{\log^2 x}\right). \qquad (44)$$

7 Primes With Fixed Primitive Roots

The representations of the characteristic function of primitive roots, Lemma 3.1, and Lemma 3.2, easily detect certain local and global properties of the elements $u\in\mathbb{F}_p$ in a finite field. Exempli gratia, it vanishes

$$\Psi(u)=0 \text{ if and only if } u=\pm 1, v^2, v^k \text{ for any proper divisor } k|p-1. \qquad (45)$$

The constraints $u\neq\pm 1, v^2$ with $v\in\mathbb{Z}$, are necessary global constraints to be a primitive element in $\mathbb{F}_p$, $p\geq 2$ an arbitrary prime. But the constraints $u\neq v^q, q\in\mathcal{Q}$, where $\mathcal{Q}$ is a finite subset of primes, are not necessary global constraints since there are infinitely many primes for which $q\nmid p-1, q\in\mathcal{Q}$. The requirement of being dth power nonresidues mod p for all $d|p-1$, which is equivalent to the definition of primitive root, are necessary local properties.

7.1 Elementary Proof

The simpler and more elementary estimate for the error term given in Lemma 5.1 leads to the weaker but effective result

***Theorem* 7.1** *A fixed integer $u \neq \pm 1, v^2$ is a primitive root mod p for infinitely many primes $p \geq 2$. In addition, the density of these primes satisfies*

$$\pi_u(x) = \#\{p \leq x : \mathrm{ord}_p(u) = p-1\} = c_u \frac{x}{\log x} + O\left(\frac{x}{(\log\log x)(\log x)}\right), \tag{46}$$

where $c_u > 0$ is a constant, for all large numbers $x \geq 1$.

Proof: Suppose that $u \neq \pm 1, v^2$ is not a primitive root for all primes $p \geq x_0$, with $x_0 \geq 1$ constant. Let $x > x_0$ be a large number, and consider the sum of the characteristic function over the short interval $[x, 2x]$, that is,

$$0 = \sum_{x \leq p \leq 2x} \Psi(u). \tag{47}$$

Replacing the characteristic function, Lemma 3.2, and expanding the nonexistence equation (7.47) yield

$$\begin{aligned} 0 &= \sum_{x \leq p \leq 2x} \Psi(u) \\ &= \sum_{x \leq p \leq 2x} \frac{1}{p} \sum_{\gcd(n,p-1)=1,\ 0 \leq k \leq p-1} \psi\left((\tau^n - u)k\right) \qquad (48) \\ &= a_u \sum_{x \leq p \leq 2x} \frac{1}{p} \sum_{\gcd(n,p-1)=1} 1 + \sum_{x \leq p \leq 2x} \frac{1}{p} \sum_{\gcd(n,p-1)=1,\ 0 < k \leq p-1} \psi\left((\tau^n - u)k\right) \\ &= M(x) + E(x), \end{aligned}$$

where $a_u \geq 0$ is a constant depending on the fixed integer $u \neq 0$.

The main term $M(x)$ is determined by a finite sum over the trivial additive character $\psi = 1$, and the error term $E(x)$ is determined by a finite sum over the nontrivial additive characters $\psi = e^{i2\pi k/p} \neq 1$.

Applying Lemma 6.2 to the main term, and Lemma 5.1 to the error term yield

$$\begin{aligned}\sum_{x\leq p\leq 2x}\Psi(u) &= M(x)+E(x)\\ &= c_u\left(\mathrm{li}(2x)-\mathrm{li}(x)\right)+O\left(\frac{x}{\log^B x}\right)+O\left(\frac{x}{(\log\log x)(\log x)}\right)\\ &= c_u\left(\mathrm{li}(2x)-\mathrm{li}(x)\right)+O\left(\frac{x}{\log^B x}\right)\\ &= c_u\frac{x}{\log x}+O\left(\frac{x}{(\log\log x)(\log x)}\right)\\ &> 0,\end{aligned}\tag{49}$$

where the constant $c_u = a_u a_0 > 0$ depending on u, and $B > 1$. This contradict the hypothesis (7.47). The short interval $[x, 2x]$ contains primes with the fixed primitive root u. ■

7.2 Improved Error Term

This subsection uses the sharper result in Lemma 5.2 to reduce the error term down to the level of the error term of the Prime Number Theorem.

Proof of Theorem 1.1. Suppose that $u \neq \pm 1, v^2$ is not a primitive root for all primes $p \geq x_0$, with $x_0 \geq 1$ constant. Let $x > x_0$ be a large number, and consider the sum of the characteristic function over the short interval $[x, 2x]$, that is,

$$0 = \sum_{x\leq p\leq 2x}\Psi(u).\tag{50}$$

Replacing the characteristic function, Lemma 3.2, and expanding the nonexistence equation (7.50) yield

$$\begin{aligned} 0 &= \sum_{x\le p\le 2x} \Psi(u) \\ &= \sum_{x\le p\le 2x} \frac{1}{p} \sum_{\gcd(n,p-1)=1,\ 0\le k\le p-1} \psi\left((\tau^n-u)k\right) \qquad (51) \\ &= a_u \sum_{x\le p\le 2x} \frac{1}{p} \sum_{\gcd(n,p-1)=1} 1 + \sum_{x\le p\le 2x} \frac{1}{p} \sum_{\gcd(n,p-1)=1,\ 0<k\le p-1} \sum \psi\left((\tau^n-u)k\right) \\ &= M(x)+E(x), \end{aligned}$$

where $a_u \ge 0$ is a constant depending on the fixed integer $u \ne 0$.

The main term $M(x)$ is determined by a finite sum over the trivial additive character $\psi = 1$, and the error term $E(x)$ is determined by a finite sum over the nontrivial additive characters $\psi = e^{i2\pi k/p} \ne 1$.

Applying Lemma 6.2 to the main term, and Lemma 5.2 to the error term yield

$$\begin{aligned} \sum_{x\le p\le 2x} \Psi(u) &= M(x)+E(x) \\ &= c_u\left(\mathrm{li}(2x)-\mathrm{li}(x)\right) + O\left(\frac{x}{\log^B x}\right) + O(x^{1-\varepsilon}) \qquad (52) \\ &= c_u\left(\mathrm{li}(2x)-\mathrm{li}(x)\right) + O\left(\frac{x}{\log^B x}\right) \\ &= c_u \frac{x}{\log x} + O\left(\frac{x}{\log^B x}\right) \\ &> 0, \end{aligned}$$

where the constant $c_u = a_u a_0 > 0$ depending on u, and $B > 1$. This contradict the hypothesis (7.50). Ergo, the short interval $[x, 2x]$ contains primes with the fixed primitive root u. ■

The determination of the constant $c_u = a_u a_0 > 0$, which is the density of primes with a fixed primitive root $u \ne \pm 1, v^2$, is a very interesting technical

problem in algebraic number theory, see [16, p. 218], [19], [20], [22, p. 10], [2], et cetera. Some historical information on this constant appears in [29]. The calculations of the constants for some cases for primitive roots in quadratic fields are given in [28], [7], et cetera. Other calculations of the constants for the related cases for elliptic primitive roots are given in [2], et alii.

References

[1] Christopher Ambrose, Artin primitive root conjecture and a problem of Rohrlich, Math. Proc. Cambridge Philos. Soc., **157,** no. 1, 2014, 79-99.

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

[3] Jean Bourgain, Exponential sum estimates in finite commutative rings and applications, J. Anal. Math., **101,** 2007, 325-355.

[4] Jean Bourgain, New bounds on exponential sums related to the Diffie-Hellman distributions, C. R. Math. Acad. Sci. Paris, **338,** no. 11, 2004, 825-830.

[5] Cristian Cobeli, On a Problem of Mordell with Primitive Roots, arXiv:0911.2832.

[6] Cristian Cobeli, Alexandru Zaharescu, On the distribution of primitive roots mod p, Acta Arith., **83,**, no. 2, 1998, 143-153.

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

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

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

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

[11] John B. Friedlander, Sergei V. Konyagin, Igor E. Shparlinski, Some doubly exponential sums over Zm, Acta Arith., **105,** no. 4, 2002, 349-370.

[12] Adam Tyler Felix, Variations on Artin Primitive Root Conjecture, PhD Thesis, Queen University, Canada, August 2011.

[13] Morris Goldfeld, Artin conjecture on the average, Mathematika 15, 1968, 223-226.

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

[15] D. R. Heath-Brown, Artin's conjecture for primitive roots, Quart. J. Math. Oxford Ser. 2, **37,** no. 145, 1986, 27-38.

[16] C. Hooley, On Artin's conjecture, J. Reine Angew. Math., **225,** 1967, 209-220.

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

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

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

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

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

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

[23] Pieter Moree, Artin prime producing quadratics, Abh. Math. Sem. Univ. Hamburg, **77,** 2007, 109-127.

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

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

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

[27] Francesco Pappalardi, Igor Shparlinski, On Artin's conjecture over function fields, Finite Fields Appl., **1,** no. 4, 1995, 399-404.

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

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

[30] P. J. Stephens, An average result for Artin conjecture, Mathematika, **16,** 1969, 178-188.

[31] Robert C. Vaughan, Some applications of Montgomery's sieve, J. Number Theory, **5** 1973, 64-79.

[32] Arne Winterhof, Character sums, primitive elements, and powers in finite fields, J. Number Theory, **91,** no. 1, 2001, 153-163.