International Journal of Mathematics and
Computer Science, **15**(2020), no. 2, 717–744

Addendum and Corrigendum Densities of Primes and Primitive Roots

(11(2016), no. 2, 89–108)

N. A. Carella

Department of Mathematics
York College
The City University of New York
Jamaica, NY 11451, USA

email: pobox5050@live.com

Abstract

Let $u \neq \pm 1, v^2$ be a fixed integer, let $p \geq 2$ be a prime, and let $\mathrm{ord}_p(u) = d \mid p-1$ be the order of $u \bmod p$. This paper provides an effective 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

The symbol $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ denotes the set of integers, and the symbol $\mathbb{P} = \{2, 3, 5, \ldots\}$ denotes the set of prime numbers. The constant $\delta(u) \geq 0$ 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 Conjecture.
AMS (MOS) Subject Classifications: Primary 11A07, Secondary 11N37.
ISSN 1814-0432, 2020, http://ijmcs.future-in-tech.net

primitive root $u \bmod p$ has the asymptotic formula

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

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

A conditional proof of this result was achieved in [24], and simplified sketches of the proof appear in [32, p. 8], and similar references. The determination of the constant $\delta(u) \geq 0$ for a fixed integer $u \in \mathbb{Z}$ is an interesting technical problem, [24, p. 218], [29], [30], et alii. An introduction to its historical development, and its calculations is covered in [32, pp. 3–10], and [44].

The Artin primitive root conjecture on average

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

where $a_0 = \prod_{p\geq 2}(1-p^{-1}(p-1)^{-1})$ is Artin constant, and $B > 1$ is an arbitrary number, was proved in [19] unconditionally, and refined in [44]. 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 (2) can be slightly different from the average quantity in (3). The variations, discovered by the Lehmers using numerical experiments, depend on the primes decomposition of the fixed value u, see [24, p. 220], [32, p. 3], and similar references for the exact formula for the density $\delta(u) \geq 0$.

The Artin primitive root conjecture for functions fields was proved by Bilharz, see [42, Theorem 10.11], and the same conjecture for polynomials over finite fields was proved in [40]. However, there is no known infinite sequence of primes with a fixed primitive root. The current literature has results infinite sequences of primes with unknown primitive root in a small finite set. For example, in [20] it was proved that for a fixed primes triple $q > r > s \geq 2$, 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 [23]. 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 [9], [38], [43], and most recently in [1]. Other related results are given in [33], [17], [39], et alii.

The technique explored in this note provides an improved lower bound for the number of primes $p \le x$ with a fixed primitive root $u \bmod p$ for all large number $x \ge 1$. And 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*

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

where $\mathrm{li}(x)$ *is the logarithm integral, and* $\delta(u) > 0$ *is a constant, for all large numbers* $x \ge 1$.

Sections 2 to 6 introduce the notation 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 Exponentials 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 $d \mid q$ 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 $\operatorname{ord}(\chi) = d \geqslant 1$ 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 $\operatorname{ord}(\chi) = d \mid q$ 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 [31, p. 187], [36, p. 118], and [26, 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*

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

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

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

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

for some $k \geq 1, \gcd(k, q) = 1$, see [31, p. 187], [36, p. 118], and [26, 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* $\operatorname{ord} \psi = q$, *then*

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

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

3 Representations of the Characteristic Functions

he 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. Several of these representations are studied in this section.

3.1 Primitive Roots Tests

For a prime $p \geq 2$, the multiplicative group of the finite fields $\mathbb{F}_p$ is a cyclic group for all primes.

Definition 3.1. *The order* $\min\{k \in \mathbb{N} : u^k \equiv 1 \bmod p\}$ *of an element* $u \in \mathbb{F}_p$ *is denoted by* $\mathrm{ord}_p(u)$. *An element is a primitive root if and only if* $\mathrm{ord}_p(u) = p - 1$.

Lemma 3.1. (Primitive root test) *An integer* $u \in \mathbb{Z}$ *is a primitive root modulo an integer* $n \in \mathbb{N}$ *if and only if*

$$u^{\lambda(n)/p} - 1 \not\equiv 0 \mod n$$

for all prime divisors $p \mid \lambda(n)$.

The primitive root test is a special case of the Lucas primality test, introduced in [28, p. 302]. A more recent version appears in [7, Theorem 4.1.1], and similar sources.

3.2 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 $q = \#G$.

Definition 3.2. *The order of an element in the cyclic group* $\mathbb{F}_p^{\times}$ *is defined by* $\mathrm{ord}_p(v) = \min\{k : v^k \equiv 1 \bmod p\}$. *Primitive elements in this cyclic group have order* $p - 1 = \#G$.

Lemma 3.2. *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*

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

Proof. Assume that $u=\tau^{qm}$ is a qth power residue modulo p, where $q\mid p-1$ and $\gcd(m,p-1)=1$. Then, the inner sum

$$\sum_{\mathrm{ord}(\psi)=q}\chi(u)=\sum_{\mathrm{ord}(\psi)=q}\chi(\tau^{qm})=\sum_{\mathrm{ord}(\psi)=q}\chi(\tau^m)^q=\varphi(q)=q-1,\tag{10}$$

where $\chi(v)^q=1$. Replacing this information into the product

$$\begin{aligned}\frac{\phi(p-1)}{p-1}\sum_{d|p-1}\frac{\mu(d)}{\varphi(d)}\sum_{\mathrm{ord}(\chi)=d}\chi(u) &= \frac{\phi(p-1)}{p-1}\prod_{q|p-1}\left(1-\frac{\sum_{\mathrm{ord}(\chi)=q}\chi(u)}{q-1}\right)\\ &= \frac{\phi(p-1)}{p-1}\prod_{q|p-1}\left(1-\frac{q-1}{q-1}\right)=0.\end{aligned}\tag{11}$$

shows that both sides of the equation vanish if the element $u\in G$ has order $\mathrm{ord}_p(u)=q\mid p-1$ and $q<p-1$. Now, assume that $u=\tau^m$ is not qth power residue modulo p for any $q\mid p-1$, where $\gcd(m,p-1)=1$. Then, the inner sum

$$\sum_{\mathrm{ord}(\psi)=q}\chi(u)=\sum_{\mathrm{ord}(\psi)=q}\chi(\tau^m)=-1.\tag{12}$$

Replacing this information into the product

$$\begin{aligned}\frac{\phi(p-1)}{p-1}\sum_{d|p-1}\frac{\mu(d)}{\varphi(d)}\sum_{\mathrm{ord}(\chi)=d}\chi(u) &= \frac{\phi(p-1)}{p-1}\prod_{q|p-1}\left(1-\frac{\sum_{\mathrm{ord}(\chi)=q}\chi(u)}{q-1}\right)\\ &= \frac{\phi(p-1)}{p-1}\prod_{q|p-1}\left(1-\frac{-1}{q-1}\right)=1.\end{aligned}\tag{13}$$

These verify that both sides of the equation vanishes if and only if the element $u\in G$ has order $\mathrm{ord}_p(u)=q\mid p-1$ and $q<p-1$. ∎

Note that a multiplicative character χ of order $\mathrm{ord}(\chi)=q\mid p-1$ has the form $\chi(u)=\chi_a(u)=e^{i2\pi a\log(u)/q}$, where $v=\log u$ is the discrete logarithm of $u\neq 0$. This immediately gives a closed form evaluation of the characters

$$\sum_{\mathrm{ord}(\psi)=q}\chi(u)=\begin{cases}\varphi(q) & \text{if } a\equiv 0 \bmod q,\\ 0 & \text{if } a\not\equiv 0 \bmod q,\end{cases}\tag{14}$$

where $\chi \neq 1$. The works in [10], and [48] attribute this formula to Vinogradov. The proof and other details on the characteristic function are given in [13, p. 863], [31, p. 258], [33, p. 18]. The characteristic function for multiple primitive roots is used in [8, p. 146] to study consecutive primitive roots. In [11] it is used to study the gap between primitive roots with respect to the Hamming metric. And in [48] it is used to prove the existence of primitive roots in certain small subsets $A \subset \mathbb{F}_p$. In [10] 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. In addition, the Artin primitive root conjecture for polynomials over finite fields was proved in [40] using this formula.

3.3 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 3.2. This difficulty is due to the large number of terms that can be generated by the divisors, for example, $d \mid p-1$, involved in the calculations, see [13], [11] for typical applications and [32, 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 3.2, 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 3.3, 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 $1 \leq n < p-1, \gcd(n, p-1) = 1$, is a variable. Two versions are given: a multiplicative version, and an additive version.

Lemma 3.3. *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 $\psi \neq 1$ is a nonprincipal additive character of order* $\mathrm{ord}\,\psi = p$*, then*

$$\Psi(u) = \sum_{\gcd(n,p-1)=1} \frac{1}{p} \sum_{0 \leq k \leq p-1} \psi\left((\tau^n - u)k\right) = \begin{cases} 1 & \text{if } \mathrm{ord}_p(u) = p-1, \\ 0 & \text{if } \mathrm{ord}_p(u) \neq p-1. \end{cases} \tag{15}$$

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

then

$$\Psi(u) = \sum_{\gcd(n,p-1)=1} \frac{1}{p-1} \sum_{0\leq k<p-1} \chi\left((\tau^n \bar{u})^k\right) = \begin{cases} 1 & \text{if } \operatorname{ord}_p(u) = p-1, \\ 0 & \text{if } \operatorname{ord}_p(u) \neq p-1, \end{cases} \tag{16}$$

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

Proof. (i) 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. Ergo, the equation

$$\tau^n - u = 0 \tag{17}$$

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

$$\Psi(u) = \sum_{\gcd(n,p-1)=1} \frac{1}{p} \sum_{0\leq k\leq p-1} e^{i2\pi(\tau^n-u)k/p} = \begin{cases} 1 & \text{if } \operatorname{ord}_p(u) = p-1, \\ 0 & \text{if } \operatorname{ord}_p(u) \neq p-1. \end{cases} \tag{18}$$

This follows from the geometric series identity $\sum_{0\leq k\leq N-1} w^k = (w^N - 1)/(w-1)$ with $w \neq 1$, applied to the inner sum. For (ii), use the equation $\tau^n \bar{u} = 1$, where $\bar{u}$ is the inverse of u, and apply the geometric series identity. ∎

4 Estimates Of Exponential Sums

This section provides simple estimates for the exponential sums of interest in this analysis. There are two objectives: To determine an upper bound, proved in Theorem 4.2, and to show that

$$\sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} = \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} + E(p), \tag{19}$$

where $E(p)$ is an error term, this is proved in Lemma 4.1. These are indirectly implied by the equidistribution of the subsets

$$\{\tau^n : \gcd(n, p-1) = 1\} = \{b\tau^n : \gcd(n, p-1) = 1\} \subset \mathbb{F}_p, \tag{20}$$

for any $0 \neq b \in \mathbb{F}_p$. The proofs of these results are entirely based on established results and elementary techniques.

4.1 Incomplete And Complete Exponential Sums

Let $f : \mathbb{C} \longrightarrow \mathbb{C}$ be a function, and let $q \in \mathbb{N}$ be a large integer. The finite Fourier transform

$$\hat{f}(t) = \frac{1}{q} \sum_{0 \le s \le q-1} e^{i\pi st/q} \tag{21}$$

and its inverse are used here to derive a summation kernel function, which is almost identical to the Dirichlet kernel.

Definition 4.1. Let p and q be primes, and let $\omega = e^{i2\pi/q}$, and $\zeta = e^{i2\pi/p}$ be roots of unity. The *finite summation kernel* is defined by the finite Fourier transform identity

$$\mathcal{K}(f(n)) = \frac{1}{q} \sum_{0 \le t \le q-1,\ 0 \le s \le p-1} \omega^{t(n-s)} f(s) = f(n). \tag{22}$$

This simple identity is very effective in computing upper bounds of some exponential sums

$$\sum_{n \le x} f(n) = \sum_{n \le x} \mathcal{K}(f(n)), \tag{23}$$

where $x \le p < q$. Two applications are illustrated here.

Theorem 4.1. ([46], [34]) *Let $p \ge 2$ be a large prime, and let $\tau \in \mathbb{F}_p$ be an element of large multiplicative order $\mathrm{ord}_p(\tau) \mid p-1$. Then, for any $b \in [1, p-1]$, and $x \le p-1$,*

$$\sum_{n \le x} e^{i2\pi b\tau^n/p} \ll p^{1/2} \log p. \tag{24}$$

Proof. Let $q = p + o(p)$ be a large prime, and let $f(n) = e^{i2\pi b\tau^n/p}$, where τ is a primitive root modulo p. Applying the finite summation kernel in Definition 4.1, yields

$$\sum_{n \le x} e^{i2\pi b\tau^n/p} = \sum_{n \le x} \frac{1}{q} \sum_{0 \le t \le q-1,\ 1 \le s \le p-1} \omega^{t(n-s)} e^{i2\pi b\tau^s/p}. \tag{25}$$

The term $t = 0$ contributes $-x/q$, and rearranging it yield

$$\begin{aligned} \sum_{n \le x} e^{i2\pi b\tau^n/p} &= \frac{1}{q} \sum_{n \le x,\ 1 \le t \le q-1,\ 1 \le s \le p-1} \omega^{t(n-s)} e^{i2\pi b\tau^s/p} - \frac{x}{q} \\ &= \frac{1}{q} \sum_{1 \le t \le q-1} \left(\sum_{1 \le s \le p-1} \omega^{-ts} e^{i2\pi b\tau^s/p} \right) \left(\sum_{n \le x} \omega^{tn} \right) - \frac{x}{q}. \end{aligned} \tag{26}$$

Taking absolute value, and applying Lemma 4.3, and Lemma 4.5, yield

$$\begin{aligned}\left|\sum_{n\leq x} e^{i2\pi b\tau^n/p}\right| &\leq \frac{1}{q}\sum_{1\leq t\leq q-1}\left|\sum_{0\leq s\leq p-1}\omega^{-ts}e^{i2\pi b\tau^s/p}\right|\cdot\left|\sum_{n\leq x}\omega^{tn}\right|+\frac{x}{q}\\ &\ll \frac{1}{q}\sum_{1\leq t\leq q-1}\left(2q^{1/2}\log q\right)\cdot\left(\frac{2q}{\pi t}\right)+\frac{x}{q} \qquad (27)\\ &\ll p^{1/2}\log^2 p.\end{aligned}$$

The last summation in (27) uses the estimate

$$\sum_{1\leq t\leq q-1}\frac{1}{t}\ll \log q\ll \log p \qquad (28)$$

since $q=p+o(p)$, and $x/q\leq 1$. ■

This appears to be the best possible upper bound. The above proof generalizes the sum of resolvents method used in [34]. Here, it is reformulated as a finite Fourier transform method, which is applicable to a wide range of functions. A similar upper bound for composite moduli $p=m$ is also proved, [op. cit., equation (2.29)].

Theorem 4.2. *Let $p\geq 2$ be a large prime, and let τ be a primitive root modulo p. Then,*

$$\sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p}\ll p^{1-\varepsilon} \qquad (29)$$

for any $b\in[1,p-1]$, and any arbitrary small number $\varepsilon\in(0,1/2)$.

Proof. Let $q=p+o(p)$ be a large prime, and let $f(n)=e^{i2\pi b\tau^n/p}$, where τ is a primitive root modulo p. Start with the representation

$$\sum_{\gcd(n,p-1)=1} e^{\frac{i2\pi b\tau^n}{p}}=\sum_{\gcd(n,p-1)=1}\frac{1}{q}\sum_{0\leq t\leq q-1,\ 1\leq s\leq p-1}\omega^{t(n-s)}e^{\frac{i2\pi b\tau^s}{p}}, \qquad (30)$$

see Definition 4.1. Use the inclusion exclusion principle to rewrite the exponential sum as

$$\sum_{\gcd(n,p-1)=1} e^{\frac{i2\pi b\tau^n}{p}}=\sum_{n\leq p-1}\frac{1}{q}\sum_{0\leq t\leq q-1,\ 1\leq s\leq p-1}\omega^{t(n-s)}e^{\frac{i2\pi b\tau^s}{p}}\sum_{\substack{d|p-1\\ d|n}}\mu(d). \qquad (31)$$

The term $t = 0$ contributes $-\varphi(p)/q$, and rearranging it yield

$$\begin{aligned} & \sum_{\gcd(n,p-1)=1} e^{\frac{i2\pi b\tau^n}{p}} \qquad (32) \\ = & \sum_{n\le p-1} \frac{1}{q} \sum_{1\le t\le q-1,\ 1\le s\le p-1} \omega^{t(n-s)} e^{\frac{i2\pi b\tau^s}{p}} \sum_{\substack{d|p-1\\ d|n}} \mu(d) - \frac{\varphi(p)}{q} \\ = & \frac{1}{q} \sum_{1\le t\le q-1} \left(\sum_{1\le s\le p-1} \omega^{-ts} e^{\frac{i2\pi b\tau^s}{p}} \right) \left(\sum_{d|p-1} \mu(d) \sum_{\substack{n\le p-1,\\ d|n}} \omega^{tn} \right) - \frac{\varphi(p)}{q}. \end{aligned}$$

Taking absolute value, and applying Lemma 4.4, and Lemma 4.5, yield

$$\begin{aligned} & \left| \sum_{\gcd(n,p-1)=1} e^{\frac{i2\pi b\tau^n}{p}} \right| \qquad (33) \\ \le & \frac{1}{q} \sum_{1\le t\le q-1} \left| \sum_{1\le s\le p-1} \omega^{-ts} e^{i2\pi b\tau^s/p} \right| \cdot \left| \sum_{d|p-1} \mu(d) \sum_{\substack{n\le p-1,\\ d|n}} \omega^{tn} \right| + \frac{\varphi(p)}{q} \\ \ll & \frac{1}{q} \sum_{1\le t\le q-1} \left(2q^{1/2}\log q\right) \cdot \left(\frac{4q\log\log p}{\pi t} \right) + \frac{\varphi(p)}{q} \\ \ll & \ p^{1/2}\log^3 p. \end{aligned}$$

The last summation in (33) uses the estimate

$$\sum_{1\le t\le q-1} \frac{1}{t} \ll \log q \ll \log p \qquad (34)$$

since $q = p + o(p)$, and $\varphi(p)/q \le 1$. This is restated in the simpler notation $p^{1/2}\log^3 p \le p^{1-\varepsilon}$ for any arbitrary small number $\varepsilon \in (0, 1/2)$. ■

The upper bound given in Theorem 4.2 seems to be optimum. A different proof, which has a weaker upper bound is included here as a reference for a second independent proof.

Theorem 4.3. ([16, Theorem 6]) *Let $p \ge 2$ be a large prime, and let τ be a primitive root modulo p. Then,*

$$\sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} \ll p^{1-\varepsilon} \qquad (35)$$

for any $b \in [1, p-1]$, and any arbitrary small number $\varepsilon > 0$ is a small number.

Other related results are given in [6], [15], [21], and [22, Theorem 1].

4.2 Equivalent Exponential Sums

For any fixed $0 \neq b \in \mathbb{F}_p$, the map $\tau^n \longrightarrow b\tau^n$ is one-to-one in $\mathbb{F}_p$. Consequently, the subsets

$$\{\tau^n : \gcd(n, p-1) = 1\} \quad \text{and} \quad \{b\tau^n : \gcd(n, p-1) = 1\} \subset \mathbb{F}_p \tag{36}$$

have the same cardinalities. As a direct consequence the exponential sums

$$\sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} \quad \text{and} \quad \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p}, \tag{37}$$

have the same upper bound up to an error term. An asymptotic relation for the exponential sums (37) is provided in Lemma 4.1. This result expresses the first exponential sum in (37) as a sum of simpler exponential sum and an error term.

Lemma 4.1. *Let $p \geq 2$ be a large primes. If τ be a primitive root modulo p, then,*

$$\sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} = \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} + O(p^{1/2}\log^3 p), \tag{38}$$

for any $b \in [1, p-1]$.

Proof. For $b \neq 1$, the exponential sum has the representation

$$\sum_{\gcd(n,p-1)=1} e^{\frac{i2\pi b\tau^n}{p}} \tag{39}$$

$$= \frac{1}{q}\sum_{1\leq t\leq q-1}\left(\sum_{1\leq s\leq p-1}\omega^{-ts}e^{\frac{i2\pi b\tau^s}{p}}\right)\left(\sum_{d|p-1}\mu(d)\sum_{\substack{n\leq p-1,\\ d|n}}\omega^{tn}\right) - \frac{\varphi(p)}{q},$$

confer equation (32) for details. And, for $b = 1$,

$$\sum_{\gcd(n,p-1)=1} e^{\frac{i2\pi\tau^n}{p}} \tag{40}$$

$$= \frac{1}{q}\sum_{1\leq t\leq q-1}\left(\sum_{1\leq s\leq p-1}\omega^{-ts}e^{\frac{i2\pi\tau^s}{p}}\right)\left(\sum_{d|p-1}\mu(d)\sum_{\substack{n\leq p-1,\\ d|n}}\omega^{tn}\right) - \frac{\varphi(p)}{q},$$

respectively, see (32). Differencing (39) and (40) produces

$$\begin{aligned} & \sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} - \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} \qquad (41) \\ = \; & \frac{1}{q} \sum_{0\le t\le q-1} \left(\sum_{1\le s\le p-1} \omega^{-ts} e^{\frac{i2\pi b\tau^s}{p}} - \sum_{1\le s\le p-1} \omega^{-ts} e^{\frac{i2\pi\tau^s}{p}} \right) \\ & \times \left(\sum_{d|p-1} \mu(d) \sum_{\substack{n\le p-1,\\ d|n}} \omega^{tn} \right). \end{aligned}$$

By Lemma 4.4, the relatively prime summation kernel is bounded by

$$\begin{aligned} \left| \sum_{d|p-1} \mu(d) \sum_{\substack{n\le p-1,\\ d|n}} \omega^{tn} \right| &= \left| \sum_{\gcd(n,p-1)=1} \omega^{tn} \right| \\ &\le \frac{4q\log\log p}{\pi t}, \qquad (42) \end{aligned}$$

and by Lemma 4.5, the difference of two Gauss sums is bounded by

$$\begin{aligned} & \left| \sum_{1\le s\le p-1} \omega^{-ts} e^{\frac{i2\pi b\tau^s}{p}} - \sum_{1\le s\le p-1} \omega^{-ts} e^{\frac{i2\pi\tau^s}{p}} \right| \\ = \; & \left| \sum_{1\le s\le p-1} \chi(s)\psi_b(s) - \sum_{1\le s\le p-1} \chi(s)\psi_1(s) \right| \\ \le \; & 4p^{1/2}\log p, \qquad (43) \end{aligned}$$

where $\chi(s) = e^{i\pi st/p}$, and $\psi_b(s) = e^{i2\pi b\tau^s/p}$. Taking absolute value in (41) and replacing (42), and (43), return

$$\begin{aligned} & \left| \sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} - \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} \right| \\ \le \; & \frac{1}{q} \sum_{0\le t\le q-1} \left(4q^{1/2}\log q\right) \cdot \left(\frac{4q\log\log p}{t} \right) \qquad (44) \\ \le \; & 16q^{1/2}(\log q)(\log q)(\log\log p) \\ \le \; & 16p^{1/2}\log^3 p, \end{aligned}$$

where $q = p + o(p) > p$. ■

The same proof works for many other subsets of elements $\mathcal{A} \subset \mathbb{F}_p$. For example,

$$\sum_{n\in\mathcal{A}} e^{i2\pi b\tau^n/p} = \sum_{n\in\mathcal{A}} e^{i2\pi\tau^n/p} + O(p^{1/2}\log^c p), \tag{45}$$

for some constant $c > 0$.

A second independent proof based on the earlier result in Theorem 4.3 is derived here.

Lemma 4.2. *Let $p \geq 2$ be a large primes. If τ be a primitive root modulo p, then,*

$$\sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} = \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} + O(p^{1-\varepsilon}), \tag{46}$$

for any $b \in [1, p-1]$, and any small number $\varepsilon > 0$.

Proof. Let $\mathcal{Z} = \{\tau^n : \gcd(n, p-1) = 1\}$. By Theorem 4.3,

$$-c_0 p^{1-\varepsilon} \leq \sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} \leq c_1 p^{1-\varepsilon}, \tag{47}$$

and

$$-c_2 p^{1-\varepsilon} \leq \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} \leq c_3 p^{1-\varepsilon}, \tag{48}$$

for some constants $c_0, c_1, c_2, c_3 > 0$. Differencing yields

$$\left| \sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} - \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} \right| = O\left(p^{1-\varepsilon}\right). \tag{49}$$

The claim follows from this. ■

4.3 Finite Summation Kernels and Gaussian Sums

Lemma 4.3. *Let $p \geq 2$ and $q = p + o(p) > p$ be large primes. Let $\omega = e^{i2\pi/q}$ be a qth root of unity, and let $t \in [1, p-1]$. Then*

1. $$\sum_{n\leq p-1} \omega^{tn} = \frac{\omega^t - \omega^{tp}}{1-\omega^t},$$

2.

$$\left| \sum_{n \le p-1} \omega^{tn} \right| \le \frac{2q}{\pi t}.$$

Proof. (i) Use the geometric series to compute this simple exponential sum as

$$\sum_{n \le p-1} \omega^{tn} \;=\; \frac{\omega^t - \omega^{tp}}{1 - \omega^t}.$$

(ii) Observe that the parameters $q = p + o(p) > p$ is prime, $\omega = e^{i2\pi/q}$, the integers $t \in [1, p-1]$, and $d \le p-1 < q-1$. This data implies that $\pi t/q \ne k\pi$ with $k \in \mathbb{Z}$, so the sine function $\sin(\pi t/q) \ne 0$ is well defined. Using standard manipulations, and $z/2 \le \sin(z) < z$ for $0 < |z| < \pi/2$, the last expression becomes

$$\left| \frac{\omega^t - \omega^{tp}}{1 - \omega^t} \right| \le \left| \frac{2}{\sin(\pi t/q)} \right| \le \frac{2q}{\pi t}. \tag{50}$$

■

Lemma 4.4. *Let $p \ge 2$ and $q = p + o(p) > p$ be large primes, and let $\omega = e^{i2\pi/q}$ be a qth root of unity. Then,*

1.

$$\sum_{\gcd(n,p-1)=1} \omega^{tn} = \sum_{d \mid p-1} \mu(d) \frac{\omega^{dt} - \omega^{dt((p-1)/d+1)}}{1 - \omega^{dt}},$$

2.

$$\left| \sum_{\gcd(n,p-1)=1} \omega^{tn} \right| \le \frac{4q \log\log p}{\pi t},$$

where $\mu(k)$ is the M$'$obius function, for any fixed pair $d \mid p-1$ and $t \in [1, p-1]$.

Proof. (i) Use the inclusion-exclusion principle to rewrite the exponential

sum as

$$\begin{aligned}\sum_{\gcd(n,p-1)=1} \omega^{tn} &= \sum_{n\leq p-1} \omega^{tn} \sum_{\substack{d|p-1\\ d|n}} \mu(d)\\ &= \sum_{d|p-1} \mu(d) \sum_{\substack{n\leq p-1\\ d|n}} \omega^{tn}\\ &= \sum_{d|p-1} \mu(d) \sum_{m\leq (p-1)/d} \omega^{dtm} \qquad (51)\\ &= \sum_{d|p-1} \mu(d) \frac{\omega^{dt}-\omega^{dt((p-1)/d+1)}}{1-\omega^{dt}}.\end{aligned}$$

(ii) Observe that the parameters $q = p + o(p) > p$ is prime, $\omega = e^{i2\pi/q}$, the integers $t \in [1, p-1]$, and $d \leq p-1 < q-1$. This data implies that $\pi dt/q \neq k\pi$ with $k \in \mathbb{Z}$, so the sine function $\sin(\pi dt/q) \neq 0$ is well defined. Using standard manipulations, and $z/2 \leq \sin(z) < z$ for $0 < |z| < \pi/2$, the last expression becomes

$$\left|\frac{\omega^{dt}-\omega^{dtp}}{1-\omega^{dt}}\right| \leq \left|\frac{2}{\sin(\pi dt/q)}\right| \leq \frac{2q}{\pi dt} \qquad (52)$$

for $1 \leq d \leq p-1$. Finally, the upper bound is

$$\begin{aligned}\left|\sum_{d|p-1} \mu(d) \frac{\omega^{dt}-\omega^{dt((p-1)/d+1)}}{1-\omega^{dt}}\right| &\leq \frac{2q}{\pi t} \sum_{d|p-1} \frac{1}{d} \qquad (53)\\ &\leq \frac{4q \log\log p}{\pi t}.\end{aligned}$$

The last inequality uses the elementary estimate $\sum_{d|n} d^{-1} \leq 2\log\log n$. ■

Lemma 4.5. (Gauss sums) *Let $p \geq 2$ and q be large primes. Let $\chi(t) = e^{i2\pi t/q}$ and $\psi(t) = e^{i2\pi\tau^t/p}$ be a pair of characters. Then, the Gaussian sum has the upper bound*

$$\left|\sum_{1\leq t\leq q-1} \chi(t)\psi(t)\right| \leq 2q^{1/2}\log q. \qquad (54)$$

5 Evaluation Of The Main Term

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

Lemma 5.1. ([45, Lemma 1]) *Let $x \geq 1$ be a large number, and let $\varphi(n)$ be the Euler totient function. Then*

$$\sum_{p \leq x} \frac{\varphi(p-1)}{p-1} = a_1 \operatorname{li}(x) + O\left(\frac{x}{\log^B x}\right), \tag{55}$$

where $\operatorname{li}(x)$ is the logarithm integral, $a_1 = 0.373955\ldots$, and $B > 1$ is an arbitrary constant, as $x \to \infty$.

A more general version of this Lemma is proved in [47], and related discussions are given in [32, p. 16]. The generalization to number fields appears in [25]. These results are ubiquitous in various results in Number Theory. Here, the logarithm integral is defined by

$$\operatorname{li}(x) = \int_2^x \frac{1}{\log t} dt = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right). \tag{56}$$

In this application, the constant

$$a_1 = \prod_{p \geq 2} \left(1 - \frac{1}{p(p-1)}\right) \tag{57}$$

coincides to the average density of primitive roots modulo p. The average density of primitive roots was proved in [19] and [45], (the heuristic is due to Artin, and the average density is known as Artin constant).

Lemma 5.2. *Let $x \geq 1$ be a large number, and let $\varphi(n)$ be the Euler totient function. Then*

$$\sum_{p \leq x} \frac{1}{p} \sum_{\gcd(n,p-1)=1} 1 = a_1 \operatorname{li}(x) + O\left(\frac{x}{\log^B x}\right). \tag{58}$$

Proof. A routine rearrangement gives

$$\begin{aligned}\sum_{p\leq x}\frac{1}{p}\sum_{\gcd(n,p-1)=1}1 &= \sum_{p\leq x}\frac{\varphi(p-1)}{p} \\ &= \sum_{p\leq x}\frac{\varphi(p-1)}{p-1}-\sum_{p\leq x}\frac{\varphi(p-1)}{p(p-1)}.\end{aligned} \tag{59}$$

To proceed, apply Lemma 5.1 to reach

$$\begin{aligned}\sum_{p\leq x}\frac{\varphi(p-1)}{p-1}-\sum_{p\leq x}\frac{\varphi(p-1)}{p(p-1)} &= a_1\,\mathrm{li}(x)+O\left(\frac{x}{\log^B x}\right)-\sum_{p\leq x}\frac{\varphi(p-1)}{p(p-1)} \\ &= a_1\,\mathrm{li}(x)+O\left(\frac{x}{\log^B x}\right),\end{aligned} \tag{60}$$

where the second finite sum

$$\sum_{p\leq x}\frac{\varphi(p-1)}{p(p-1)}=O\left(\log\log x\right) \tag{61}$$

is absorbed into the error term, which has $B>1$ as an arbitrary constant. ■

6 Estimate For The Error Term

The upper bounds for exponential sums over subsets of elements in finite rings $\mathbb{Z}/m\mathbb{Z}$ or finite fields $\mathbb{F}_p$ studied in Lemma 4.1 and Theorem 4.2 are used to estimate the error term $E(x)$ in the proof of Theorem 1.1.

Lemma 6.1. *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,*

$$\sum_{x\leq p\leq 2x}\frac{1}{p}\sum_{\gcd(n,p-1)=1,\,0<k\leq p-1}\psi\left((\tau^n-u)k\right)\ll\frac{x^{1-\varepsilon}}{\log x} \tag{62}$$

for all sufficiently large numbers $x\geq 1$ and an arbitrarily small number $\varepsilon<1/16$.

Proof. Let $\psi(z)=e^{i2\pi z/p}$. By hypothesis $u\neq\tau^n$ for any $n\geq 1$ such that $\gcd(n,p-1)=1$. Thus,

$$\sum_{0<k\leq p-1}\psi((\tau^n-u)k)=\sum_{0<k\leq p-1}e^{i2\pi(\tau^n-u)k/p}=-1. \tag{63}$$

Therefore,

$$\begin{aligned} |E(x)| &= \left| \sum_{x\le p\le 2x} \frac{1}{p} \sum_{\gcd(n,p-1)=1,\ 0<k\le p-1} \psi\left((\tau^n - u)k\right) \right| \\ &\le \sum_{p\le x} \frac{\varphi(p-1)}{p} \\ &\le \frac{1}{2}\sum_{p\le x} 1 \qquad (64) \\ &\le \frac{1}{2}\frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right). \end{aligned}$$

To sharpen this upper bound, rearrange the triple finite sum in the form

$$\begin{aligned} E(x) &= \sum_{x\le p\le 2x} \frac{1}{p} \sum_{0<k\le p-1,\ \gcd(n,p-1)=1} \psi((\tau^n - u)k) \qquad (65) \\ &= \sum_{x\le p\le 2x} \left(\frac{1}{p} \sum_{0<k\le p-1} e^{-i2\pi\frac{uk}{p}}\right) \left(\sum_{\gcd(n,p-1)=1} e^{i2\pi\frac{k\tau^n}{p}}\right) \\ &= \sum_{x\le p\le 2x} \left(\frac{1}{p} \sum_{0<k\le p-1} e^{-i2\pi\frac{uk}{p}}\right) \left(\sum_{\gcd(n,p-1)=1} e^{i2\pi\frac{\tau^n}{p}} + O(p^{1/2}\log^3 p)\right) \\ &= \sum_{x\le p\le 2x} U_p V_p, \end{aligned}$$

where the third line in equation (65) follows from Lemma 4.1 or Lemma 4.2 . The absolute value of the first exponential sum U_p is given by

$$|U_p| = \left| \frac{1}{p} \sum_{0<k\le p-1} e^{-i2\pi uk/p} \right| = \frac{1}{p}. \qquad (66)$$

This follows from the exact value $\sum_{0<k\le p-1} e^{i2\pi uk/p} = -1$ for $u \ne 0$. And the

absolute value of the second exponential sum V_p has the upper bound

$$\begin{aligned} |V_p| &= \left| \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} + O\left(p^{1/2}\log^3 p\right) \right| \\ &\ll \left| \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} \right| + p^{1/2}\log^3 p \\ &\ll p^{1-\varepsilon}, \end{aligned} \tag{67}$$

where $\varepsilon < 1/2$ is an arbitrarily small number, see Theorem 4.2 or Theorem 4.3. A related exponential sum application appears in [37, p. 1286].

Taking absolute value in (65), and replacing the estimates (66) and (67) return

$$\begin{aligned} \sum_{x\leq p\leq 2x} |U_pV_p| &\leq \sum_{x\leq p\leq 2x} |U_p|\,|V_p| \\ &\ll \sum_{x\leq p\leq 2x} \frac{1}{p}\cdot p^{1-\varepsilon} \\ &\ll \frac{1}{x^\varepsilon} \sum_{x\leq p\leq 2x} 1 \\ &\ll \frac{x^{1-\varepsilon}}{\log x}, \end{aligned} \tag{68}$$

where the number of primes in the short interval $[x, 2x]$ is $\pi(2x) - \pi(x) \leq 2x/\log x$. ■

7 Main Result

The representations of the characteristic function of primitive roots, Lemma 3.2, and Lemma 3.3, easily detect certain local and global properties of the elements $u \in \mathbb{F}_p$ in a finite field. Exempli gratia, it vanishes

$$\Psi(u) = 0 \text{ if and only if } u = \pm 1, v^2, v^m \text{ for any proper divisor } m \mid p-1. \tag{69}$$

Ergo, 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 $q \mid p-1, q \in \mathcal{Q}$. The requirement of being dth power nonresidues mod p for all $d \mid p-1$, which is equivalent to the definition of primitive root, are necessary local properties, see Lemma 3.1.

Proof. (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

$$\Psi(u) = \begin{cases} 1 & \text{if } \operatorname{ord}_p(u) = p-1, \\ 0 & \text{if } \operatorname{ord}_p(u) \neq p-1, \end{cases} \tag{70}$$

over the short interval $[x, 2x]$, that is,

$$0 = \sum_{x \leq p \leq 2x} \Psi(u). \tag{71}$$

Replacing the characteristic function, Lemma 3.3, and expanding the nonexistence equation (71) yield

$$\begin{aligned} 0 &= \sum_{x \leq p \leq 2x} \Psi(u) \\ &= \sum_{x \leq p \leq 2x} \frac{1}{p} \sum_{\gcd(n,p-1)=1,\ 0 \leq k \leq p-1} \psi\left((\tau^n - u)k\right) \qquad (72) \\ &= \delta(u) \sum_{x \leq p \leq 2x} \frac{1}{p} \sum_{\gcd(n,p-1)=1} 1 + \sum_{x \leq p \leq 2x} \frac{1}{p} \sum_{\gcd(n,p-1)=1,\ 0 < k \leq p-1} \psi\left((\tau^n - u)k\right) \\ &= M(x) + E(x). \end{aligned}$$

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 $\psi(t) = e^{i2\pi t/p} \neq 1$.

Applying Lemma 5.2 to the main term, and Lemma 6.1 to the error term yield

$$\begin{aligned}\sum_{x\leq p\leq 2x}\Psi(u) &= M(x)+E(x)\\ &= \delta(u)\left(\mathrm{li}(2x)-\mathrm{li}(x)\right)+O\left(\frac{x}{\log^B x}\right)+O\left(\frac{x^{1-\varepsilon}}{\log x}\right) \quad (73)\\ &= \delta(u)\frac{x}{\log x}+O\left(\frac{x}{\log^B x}\right)\\ &> 0,\end{aligned}$$

where $\delta(u)\geq 0$ is the density, and $B>1$ is a constant. However, $\delta(u)>0$ contradicts the hypothesis (71) for all sufficiently large numbers $x\geq x_0$. Ergo, the short interval $[x,2x]$ contains primes with the fixed primitive root u. ■

A formula for computing the density $\delta(u)\geq 0$ of primes with a fixed primitive root $u\neq\pm 1, v^2$ is derived in [24, p. 220]. This formula specifies the density as follows. Let $u=(st^2)^k\neq\pm 1, v^2$ with s squarefree, and $k\geq 1$, and let

$$a_k(u)=\prod_{p|k}\frac{1}{p-1}\prod_{p\nmid k}\left(1-\frac{1}{p(p-1)}\right). \quad (74)$$

1. If $s\not\equiv 1 \bmod 4$, then,
$$\delta(u)=a_k(u). \quad (75)$$

2. If $s\equiv 1 \bmod 4$, then,
$$\delta(u)=\left(1-\mu(s)\prod_{\substack{p|s\\ p|k}}\frac{1}{p-2}\prod_{\substack{p|s\\ p\nmid k}}\frac{1}{p^2-p-1}\right)a_k(u). \quad (76)$$

In the case of a decimal base $u=10$, the density

$$\delta(10)=\prod_{p\geq 2}\left(1-\frac{1}{p(p-1)}\right)=0.37395581361920228805472 80\ldots \quad (77)$$

was computed in [49].

The argument can be repeated for any other squarefree base $u=2,3,\ldots$.

8 Application To Repeated Decimals

Let $p \geq 2$ be a prime. The period of the repeating decimal number

$$1/p = 0.\overline{x_{d-1} \ldots x_1 x_0}, \tag{78}$$

with $x_i \in \{0, 1, 2, \ldots, 9\}$, was investigated by Gauss and earlier authors centuries ago, see [5] for a historical account, and [35] for recent developments. As discussed in Articles 14-18 in [18], the period, denoted by $\mathrm{ord}_p(10) = d \geq 1$, is a divisor of $p-1$. The problem of computing the densities for the subsets of primes for which the repeating decimals have very large periods such as $d = (p-1)/2$, and $d = p-1$, is a recent problem. This note considers the following result.

Theorem 8.1. *There are infinitely many primes $p \geq 7$ with maximal repeating decimal $1/p = 0.\overline{x_{p-2}x_{p-3} \cdots x_1 x_0}$, where $0 \leq x_i \leq 9$. Moreover, the counting function for these primes satisfies the lower bound*

$$\pi_{10}(x) = \#\{p \leq x : \mathrm{ord}_p(10) = p-1\} = \delta(10)\frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right), \tag{79}$$

where $\delta(10) = 0.373955\ldots$ is a constant, see (77)*, for all large numbers $x \geq 1$.*

The proof of Theorem 8.1 is a corollary of the more general result in Theorem 1.1 presented in Section 7. This analysis generalizes to repeating ℓ-adic expansions $1/p = 0.\overline{x_{d-1}x_{d-2} \cdots x_1 x_0}$, where $0 \leq x_i \leq \ell - 1$, in any numbers system with nonsquare integer base $\ell \geq 2$.

9 Proof of Theorem 8.1

The repeating decimal fractions have the squarefree base $u = 10$. In particular, the repeated fraction representation

$$\frac{1}{p} = \frac{m}{10^d} + \frac{m}{10^{2d}} + \cdots = m\sum_{n \geq 1} \frac{1}{10^{dn}} = \frac{m}{10^d - 1} \tag{80}$$

has the maximal period $d = p-1$ if and only if 10 has order $\mathrm{ord}_p(10) = p-1$ modulo p. This follows from the Fermat little theorem and $10^d - 1 = mp$. The subset of Abel-Wieferich primes, which satisfy the congruence

$$10^{p-1} - 1 \equiv 0 \bmod p^2, \tag{81}$$

are also important in the calculation of the period modulo p^2, confer [41, p. 333], [12] for other details.

The result for repeating decimal of maximal period is a simple corollary of the previous result.

Proof. (Theorem 8.1) This follows from Theorem 1.1 replacing the base $u = 10$. That is,

$$\pi_{10}(x) = \sum_{p \leq x} \Psi(10) = \delta(10)\,\mathrm{li}(x) + O\left(\frac{x}{\log^B x}\right), \tag{82}$$

where $B > 1$ is a constant. ■

10 Numerical Data For Small u

In the 1950's the Lehmers used contemporary super computer technology to study the density of primes $p \leq 20000$ and the associated primitive roots. They discovered that the average density a_1 does not hold for every fixed primitive root u modulo p, a historical survey appears in [44], and advanced the theory involved in the correction, see [29] and related references. A numerical experiment was conducted to demonstrates this phenomenon. The numerical experiment employed $\pi(x) = 1000000$ primes for each fixed primitive root $u = 2, 3, 5, 6, 7, 8$, and 10.

Root u	Density $\delta(u)$	Actual Count $\pi_u(x)$	Prediction $\delta(u)\frac{x}{\log x}$	Error $R_1(x)$
2	a_1	374023	373955.8	67.2
3	a_1	373959	373955.8	−16.8
5	$\frac{20a_1}{19}$	393815	393637.7	177.3
6	a_1	374346	373955.8	390.2
7	a_1	374118	373955.8	162.2
8	$\frac{3a_1}{5}$	224404	224373.5	30.5
10	a_1	374125	373955.8	169.2

The average density is $a_1 = 0.3739558136\ldots$, and the corrected densities were computed with formulas (74) to (77). The error rate is within the

optimum predicted range

$$R_1(x) = \left|\pi_u(x) - \delta(u)\frac{x}{\log x}\right| = O\left(x^{1/2}\log x\right). \tag{83}$$

References

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

[2] Tom M. Apostol, Introduction to analytic number theory, 1976.

[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., **338,** no. 11, (2004), 825–830.

[5] Maarten Bullynck, Decimal periods and their tables: a German research topic (1765–1801), Historia Math., **36,** no. 2, (2009), 137–160.

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

[7] Richard Crandall, Carl Pomerance, Prime numbers, A computational perspective, Second edition, 2005.

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

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

[10] H. Davenport, On Primitive Roots in Finite Fields, Quarterly J. Math.,**OS-8,** no. 1, (1937), 308–312.

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

[12] Franois G. Dorais, Dominic Klyve, A Wieferich prime search up to 6.7×10^15, J. Integer Seq., **14,** no. 9, (2011), Article 11.9.2, 14 pp.

[13] Paul Erdos, Harold N. Shapiro, On the Least Primitive Root Of a Prime, (1957), euclidproject.org.

[14] John B. Friedlander, Sergei Konyagin, Igor E. Shparlinski, Some doubly exponential sums over Zm, Acta Arith., **105,** no. 4, (2002), 349–370.

[15] John B. Friedlander, Igor E. Shparlinski, Double exponential sums over thin sets, Proc. AMS, **129,** no. 6, (2001), 1617–1621.

[16] John B. Friedlander, Jan Hansen, Igor E. Shparlinski, Character sums with exponential functions, Mathematika, **47,** nos. 1-2, (2000), 75–85.

[17] Adam Tyler Felix, Variations on Artin Primitive Root Conjecture, Ph. D Dissertation, Queen University, Canada, 2011.

[18] Carl Friedrich Gauss, Disquisitiones arithmeticae, Translated by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither, A. W. Grootendorst, Springer-Verlag, New York, 1986.

[19] Morris Goldfeld, Artin conjecture on the average, Mathematika, **15,** (1968), 223–226.

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

[21] M. Z. Garaev, Double exponential sums related to Diffie-Hellman distributions, Int. Math. Res. Notes, 2005, no. 17, 1005–1014.

[22] M. Z. Garaev, A. A. Karatsuba, New estimates of double trigonometric sums with exponential functions, arXiv:math/0504026.

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

[24] C. Hooley, On Artin's conjecture, J. Reine Angew. Math., **225,** (1967), 209–220.

[25] Jurgen G. Hinz, Some applications of sieve methods in algebraic number fields, Manuscripta Math., **48,** nos. 1-3, (1984), 117–137.

[26] Henryk Iwaniec, Emmanuel Kowalski, Analytic number theory, AMS Colloquium Publications, **53,** AMS, 2004.

[27] 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.

[28] Edouard Lucas, Theorie des Fonctions Numeriques Simplement Periodiques, Amer. J. Math., **1,** no. 4, (1878), 289–321.

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

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

[31] Rudolf Lidl, Harald Niederreiter, Finite fields, Second edition, Encyclopedia of Mathematics and its Applications, **20,** Cambridge University Press, Cambridge, 1997.

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

[33] Pieter Moree, Artin prime producing quadratics, Abh. Math. Sem. Univ. Hamburg, **77,** (2007), 109–127.

[34] L. J. Mordell, On the exponential sum $\sum_{1\leq x\leq X} exp(2\pi i(ax+bg^x)/p)$, Mathematika, **19 ,** (1972), 84–87.

[35] M. Ram Murty, Artin's conjecture for primitive roots, Math. Intelligencer, **10,** no. 4, (1988), 59–67.

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

[37] M. Ram Murty, R. Thangadurai, The class number of $Q(\sqrt{-p})$ and digits of $1/p$, Proc. AMS, **139 ,** no. 4, (2011), 1277–1289.

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

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

[40] Francesco Pappalardi, Igor Shparlinski, On Artin's conjecture over function fields, Finite Fields App., **1,** no. 4, (1995), 399–404.

[41] Paulo Ribenboim, The new book of prime number records, 1996.

[42] Michael Rosen, Number theory in function fields, 2002.

[43] Hans Roskam, Artin primitive root conjecture for quadratic fields, J. Theorie Nombres (Bordeaux), **14,** no. 1, (2002), 287–324.

[44] 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.

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

[46] R. G. Stoneham, On the uniform e-distribution of residues within the periods of rational fractions with applications to normal numbers, Acta Arith., **22,** (1973), 371–389.

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

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

[49] John W. Wrench, Evaluation of Artin's constant and the twin-prime constant, Math. Comp., **15,** (1961), 396–398.