4-18-2019

Densities For The Repeating Decimals Problems

Nelson A. Carella
CUNY Bronx Community College

Densities For The Repeating Decimals Problems

Nelson Carella

Abstract: Let $p \geq 2$ be a prime, and let $1/p = 0.\overline{x_{w-1} \ldots x_1 x_0}$, $x_i \in \{0, 1, 2, \ldots, 9\}$. The period $w \geq 1$ of the repeating decimal $1/p$ is a divisor of $p-1$. This note shows that the counting function for the number of primes with maximal period $w = p-1$ has an effective lower bound $\pi_{10}(x) = \#\{p \leq x : \operatorname{ord}_p(10) = p-1\} \gg x/\log x$. This is a lower bound for the number of primes $p \leq x$ with a fixed primitive root 10 mod p for all large numbers $x \geq 1$. An extension to repeating decimal $1/p$ with near maximal period $w = (p-1)/r$, where $r \geq 1$ is a small integer, is also provided.

Contents

April 18, 2019
AMS MSC: Primary 11A07; Secondary 11R45.
Keywords: Repeated Decima; Distribution of Prime; Primitive Root; Near Primitive Root; Artin Conjecture.

1 Introduction

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

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

with $x_i \in \{0, 1, 2, \ldots, 9\}$, was investigated by Gauss and earlier authors centuries ago, see [2] for a historical account, and [27] for recent developments. As discussed in Articles 14-18 in [7], the period, denoted by $\operatorname{ord}_p(10) = w \geq 1$, 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 $w = p-1$, and $w = (p-1)/r$, with $r \geq 1$, is a recent problem. This note considers the following results.

Theorem 1.1. *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 primes counting function has the asymptotic formula*

$$\begin{aligned} \pi_{10}(x) &= \#\{p \leq x : \operatorname{ord}_p(10) = p-1\} \\ &= \delta(10)\operatorname{li}(x) + O\left(\frac{x}{\log^b x}\right), \end{aligned} \tag{2}$$

where $\delta(10) > 0$ is the density, and $b > 1$ is a constant, for all large numbers $x \geq 1$.

An extension to repeated decimal of near maximal period is provided below. Here, the parameter

$$r = [(\mathbb{Z}/p\mathbb{Z})^\times : \langle u \mod p \rangle] \tag{3}$$

is the index of the subgroup $\langle u \mod p\rangle$ generated by the element $u \neq 0, \pm 1$.

Theorem 1.2. *Let $x \geq 1$ be a large number, let $r \geq 1$ be a small integer, $r = O(\log^c x)$, with $c \geq 0$. The number of primes $p \leq x$ with near maximal repeating decimal $1/p = 0.\overline{x_{w-1}x_{w-2} \cdots x_1 x_0}$, where $0 \leq x_i \leq 9$, and period $w = (p-1)/r$ has the asymptotic formula*

$$\begin{aligned} \pi_{10}(x, r) &= \#\{p \leq x : \operatorname{ord}_p(10) = (p-1)/r\} \\ &= \delta(10, r)\operatorname{li}(x) + O\left(\frac{x}{r\log^b x}\right), \end{aligned} \tag{4}$$

where $\delta(10, r) > 0$ is the density, and $b \geq c+1$ is a constant, for all large numbers $x \geq 1$.

The proofs and results are classified by the index $r \geq 1$. The case $r = 1$ corresponds to repeated decimal fractions of maximal periods, and the case $r > 1$ corresponds to repeated decimal fractions of near maximal periods, (equivalently, this corresponds to primitive root). The preliminary background, notation and results are discussed in Sections 2 to 5. Section 6 presents a general result for primitive root $u \neq \pm 1, v^2$ in Theorem 6.1; and Theorem 1.1, which is a corollary of this result, is presented in Section 7. The numerical data for index $r = 1$ appears in Section 8. Theorem 9.1 in Section 9 presents a general result for near primitive root $u \neq \pm 1$, (equivalently, this corresponds to near primitive root), and the proof of Theorem 1.2, which is a corollary of this result, is assembled in Section 10. The numerical data for index $r > 1$ appears in Section 11. This analysis generalizes to repeating ℓ-adic expansions $1/p = 0.\overline{x_{w-1}x_{d-2} \cdots x_1 x_0}$, where $0 \leq x_i \leq \ell - 1$, in any numbers system with nonsquare integer base $\ell \geq 2$, and index $r \geq 1$.

2 Representations of the Characteristic Functions

The *order* of an element in the cyclic group $G = \mathbb{F}_p^\times$ is defined by $\operatorname{ord}_p(v) = \min\{k : v^k \equiv 1 \bmod p\}$. Primitive elements in this cyclic group have order $p - 1 = \#G$. 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. The standard characteristic function is discussed in [17, p. 258]. It detects a primitive element by means of the divisors of $p-1$.

A new representation of the characteristic function for primitive elements is developed here. It detects the order $\operatorname{ord}_p(u) \mid p-1$ of an 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 $1 \leq n < p-1$.

2.1 Characteristic Function For Index $r = 1$

The characteristic function of primitive roots is simpler and has simpler notation.

Lemma 2.1. *Let $p \geq 2$ be a prime, and let τ be a primitive root mod p. Let $u \in \mathbb{F}_p$ be a nonzero element, and let, $\psi \neq 1$ be a nonprincipal additive character of order* $\operatorname{ord} \psi = p$. *Then*

$$\sum_{\gcd(n,p-1)=1} \frac{1}{p} \sum_{0 \leq m \leq p-1} \psi\left((\tau^n - u)m\right) = \begin{cases} 1 & \text{if } \operatorname{ord}_p(u) = p-1, \\ 0 & \text{if } \operatorname{ord}_p(u) \neq p-1. \end{cases} \tag{5}$$

Proof. Let $\tau \in \mathbb{F}_p$ be a fixed primitive root. 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

$$\tau^n - u = 0 \tag{6}$$

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

$$\sum_{\gcd(n,p-1)=1} \frac{1}{p} \sum_{0 \leq m \leq p-1} e^{i2\pi(\tau^n - u)m/p} = \begin{cases} 1 & \text{if } \operatorname{ord}_p(u) = p-1, \\ 0 & \text{if } \operatorname{ord}_p(u) \neq p-1. \end{cases} \tag{7}$$

This follows from the geometric series identity $\sum_{0 \leq n \leq N-1} w^n = (w^N - 1)/(w-1), w \neq 1$ applied to the inner sum. ■

2.2 Characteristic Function For Index $r > 1$

A more general version for elements $u \in \mathbb{Z}/p\mathbb{Z}$ of order $\operatorname{ord}_p(u) = (p-1)/r$ is taken up on the next result.

Lemma 2.2. *Let $p \geq 2$ be a prime, and let τ be a primitive root mod p. Let $u \in \mathbb{F}_p$ be a nonzero element, and let, $\psi \neq 1$ be a nonprincipal additive character of order* $\operatorname{ord} \psi = p$. *For any divisor $r \mid p-1$, the characteristic function of index r is*

$$\sum_{\gcd(n,(p-1)/r)=1} \frac{1}{p} \sum_{0 \leq m \leq p-1} \psi\left((\tau^{rn} - u)m\right) = \begin{cases} 1 & \text{if } \operatorname{ord}_p(u) = (p-1)/r, \\ 0 & \text{if } \operatorname{ord}_p(u) \neq (p-1)/r. \end{cases} \tag{8}$$

Proof. For any fixed divisor $r \mid p-1$, let $\mathcal{T}_r = \{\tau^{rn} : \gcd(n, (p-1)/r) = 1\} \subset \mathbb{F}_p$ be the subset of elements of order $(p-1)/r$. Accordingly, the equation

$$x - u = 0 \tag{9}$$

has a solution $x \in \mathcal{T}_r$ if and only if the fixed element $u \in \mathbb{F}_p$ is an element of order $\operatorname{ord}_p(u) = (p-1)/r$. Replace $\psi(z) = e^{i2\pi z/p}$ to obtain

$$\sum_{x \in \mathcal{T}_r} \frac{1}{p} \sum_{0 \leq m \leq p-1} e^{i2\pi(x-u)m/p} = \begin{cases} 1 & \text{if } \operatorname{ord}_p(u) = (p-1)/r, \\ 0 & \text{if } \operatorname{ord}_p(u) \neq (p-1)/r. \end{cases} \tag{10}$$

This follows from the geometric series applied to the inner sum. ■

3 Estimates Of Exponential Sums

This section provides simple estimates for the exponential sums of interest in this analysis. There are two objectives: To determine the upper bounds, proved in Theorem 3.2, and Theorem 3.3, and to show that

$$\sum_{\gcd(n,(p-1)/r)=1} e^{i2\pi b\tau^{rn}/p} = \sum_{\gcd(n,(p-1)/r)=1} e^{i2\pi\tau^{rn}/p} + E(p), \tag{11}$$

where $E(p)$ is an error term, this is proved in Lemma 3.1 and Lemma 3.5. These are indirectly implied by the equidistribution of the subsets

$$\{\tau^{rn} : \gcd(n,(p-1)/r)=1\} = \{b\tau^{rn} : \gcd(n,(p-1)/r)=1\} \subset \mathbb{F}_p, \tag{12}$$

for any $0 \neq b \in \mathbb{F}_p$. The proofs of these results are entirely based on established results and elementary techniques. The two cases for index $r=1$ and index $r>1$ are treated separately.

3.1 Incomplete And Complete Exponential Sums For Index $r = 1$

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

$$\hat{f}(t) = \frac{1}{q} \sum_{0 \leq s \leq q-1} e^{i\pi st/q} \tag{13}$$

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

Definition 3.1. 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

$$\mathcal{K}(f(n)) = \frac{1}{q} \sum_{0 \leq t \leq q-1,\; 0 \leq s \leq p-1} \omega^{t(n-s)} f(s) = f(n). \tag{14}$$

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

$$\sum_{n \leq x} f(n) = \sum_{n \leq x} \mathcal{K}(f(n)), \tag{15}$$

where $x \leq p \leq q$. A few applications are demonstrated here.

Theorem 3.1. ([33], [21]) *Let $p \geq 2$ be a large prime, and let $\tau \in \mathbb{F}_p$ be an element of large multiplicative order* $\operatorname{ord}_p(\tau) \mid p-1$. *Then, for any $b \in [1, p-1]$, and $x \leq p-1$,*

$$\sum_{n \leq x} e^{i2\pi b\tau^n/p} \ll p^{1/2} \log^2 p. \tag{16}$$

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 3.1, yields

$$\sum_{n \leq x} e^{i2\pi b\tau^n/p} = \sum_{n \leq x} \frac{1}{q} \sum_{0 \leq t \leq q-1,\; 1 \leq s \leq p-1} \omega^{t(n-s)} e^{i2\pi b\tau^s/p}. \tag{17}$$

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

$$\begin{aligned} \sum_{n \leq x} e^{i2\pi b\tau^n/p} &= \frac{1}{q} \sum_{n \leq x,\; 1 \leq t \leq q-1,\; 1 \leq s \leq p-1} \omega^{t(n-s)} e^{i2\pi b\tau^s/p} - \frac{x}{q} \\ &= \frac{1}{q} \sum_{1 \leq t \leq q-1} \left(\sum_{1 \leq s \leq p-1} \omega^{-ts} e^{i2\pi b\tau^s/p} \right) \left(\sum_{n \leq x} \omega^{tn} \right) - \frac{x}{q}. \end{aligned} \tag{18}$$

Taking absolute value, and applying Lemma 3.2, and Lemma 3.4, yield

$$\begin{aligned}
\left|\sum_{n\le x} e^{i2\pi b\tau^n/p}\right| &\le \frac{1}{q}\sum_{1\le t\le q-1}\left|\sum_{0\le s\le p-1}\omega^{-ts}e^{i2\pi b\tau^s/p}\right|\cdot\left|\sum_{n\le x}\omega^{tn}\right|+\frac{x}{q}\\
&\ll \frac{1}{q}\sum_{1\le t\le q-1}\left(2q^{1/2}\log q\right)\cdot\left(\frac{2q}{\pi t}\right)+\frac{x}{q} \qquad (19)\\
&\ll p^{1/2}\log^2 p.
\end{aligned}$$

The last summation in (19) uses the estimate

$$\sum_{1\le t\le q-1}\frac{1}{t}\ll \log q\ll \log p \tag{20}$$

since $q=p+o(p)$, and $x/q\le 1$. ■

This appears to be the best possible upper bound. The above proof generalizes the sum of resolvents method used in [21]. 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 3.2. *Let $p\ge 2$ be a large prime, and let τ be a primitive root modulo p. Then,*

$$\sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p}\ll p^{1-\varepsilon} \tag{21}$$

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

$$\sum_{\gcd(n,p-1)=1} e^{\frac{i2\pi b\tau^n}{p}}=\sum_{\gcd(n,p-1)=1}\frac{1}{q}\sum_{0\le t\le q-1,}\sum_{1\le s\le p-1}\omega^{t(n-s)}e^{\frac{i2\pi b\tau^s}{p}}, \tag{22}$$

see Definition 3.1. Use the inclusion exclusion principle to rewrite the exponential sum as

$$\begin{aligned}
&\sum_{\gcd(n,p-1)=1} e^{\frac{i2\pi b\tau^n}{p}} \qquad (23)\\
&=\sum_{n\le p-1}\frac{1}{q}\sum_{0\le t\le q-1,}\sum_{1\le s\le p-1}\omega^{t(n-s)}e^{\frac{i2\pi b\tau^s}{p}}\sum_{\substack{d\mid p-1\\ d\mid n}}\mu(d).
\end{aligned}$$

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

$$\begin{aligned}
&\sum_{\gcd(n,p-1)=1} e^{\frac{i2\pi b\tau^n}{p}} \qquad (24)\\
&=\sum_{n\le p-1}\frac{1}{q}\sum_{1\le t\le q-1,}\sum_{1\le s\le p-1}\omega^{t(n-s)}e^{\frac{i2\pi b\tau^s}{p}}\sum_{\substack{d\mid p-1\\ d\mid n}}\mu(d)-\frac{\varphi(p)}{q}\\
&=\frac{1}{q}\sum_{0\le t\le q-1}\left(\sum_{1\le s\le p-1}\omega^{-ts}e^{\frac{i2\pi b\tau^s}{p}}\right)\left(\sum_{d\mid p-1}\mu(d)\sum_{\substack{n\le p-1,\\ d\mid n}}\omega^{tn}\right)-\frac{\varphi(p)}{q}.
\end{aligned}$$

Taking absolute value, and applying Lemma 3.3, and Lemma 3.4, yield

$$\begin{aligned}
&\left| \sum_{\gcd(n,p-1)=1} e^{\frac{i2\pi b\tau^n}{p}} \right| && (25)\\
\le\ & \frac{1}{q} \sum_{1\le t\le q-1} \left| \sum_{0\le s\le p-1} \omega^{-ts} e^{i2\pi b\tau^s/p} \right| \cdot \left| \sum_{d\mid p-1} \mu(d) \sum_{\substack{n\le p-1,\\ d\mid n}} \omega^{tn} \right| \\
\ll\ & \frac{1}{q} \sum_{1\le t\le q-1} \left(2q^{1/2}\log q\right) \cdot \left(\frac{4q\log\log p}{\pi t}\right) + \frac{\varphi(p)}{q} \\
\ll\ & p^{1/2}\log^3 p.
\end{aligned}$$

The last summation in (25) uses the estimate

$$\sum_{1\le t\le q-1} \frac{1}{t} \ll \log q \ll \log p \tag{26}$$

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 3.2 seems to be optimum. A different proof, which has a weaker upper bound, appears in [6, Theorem 6], and related results are given in [3], [8], and [9, Theorem 1].

3.2 Equivalent Exponential Sums For Index $r = 1$

An asymptotic relation for the exponential sums

$$\sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} \quad \text{and} \quad \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p}, \tag{27}$$

is provided in Lemma 3.1. This result expresses the first exponential sum in (27) as a sum of simpler exponential sum and an error term.

Lemma 3.1. *Let $p \ge 2$ and $q = p + o(p) \ge p$ be large primes. If τ be a primitive root modulo p, then,*

$$\sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} = \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} + O(p^{1/2}\log^3 p), \tag{28}$$

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

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

$$\begin{aligned}
&\sum_{\gcd(n,p-1)=1} e^{\frac{i2\pi b\tau^n}{p}} && (29)\\
=\ & \frac{1}{q} \sum_{1\le t\le q-1} \left(\sum_{1\le s\le p-1} \omega^{-ts} e^{\frac{i2\pi b\tau^s}{p}} \right) \left(\sum_{d\mid p-1} \mu(d) \sum_{\substack{n\le p-1,\\ d\mid n}} \omega^{tn} \right) - \frac{\varphi(p)}{q},
\end{aligned}$$

confer (23) and (24). For $b = 1$,

$$\begin{aligned}
&\sum_{\gcd(n,p-1)=1} e^{\frac{i2\pi\tau^n}{p}} && (30)\\
=\ & \frac{1}{q} \sum_{1\le t\le q-1} \left(\sum_{1\le s\le p-1} \omega^{-ts} e^{\frac{i2\pi\tau^s}{p}} \right) \left(\sum_{d\mid p-1} \mu(d) \sum_{\substack{n\le p-1,\\ d\mid n}} \omega^{tn} \right) - \frac{\varphi(p)}{q},
\end{aligned}$$

respectively, see (24). Differencing (29) and (30) produces

$$\begin{aligned}
&\sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} - \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} \qquad (31)\\
=\ & \frac{1}{q}\sum_{0\le t\le q-1}\left(\sum_{1\le s\le p-1}\omega^{-ts}e^{\frac{i2\pi b\tau^s}{p}} - \sum_{1\le s\le p-1}\omega^{-ts}e^{\frac{i2\pi\tau^s}{p}}\right)\\
&\times\left(\sum_{d\mid p-1}\mu(d)\sum_{\substack{n\le p-1,\\ d\mid n}}\omega^{tn}\right).
\end{aligned}$$

By Lemma 3.3, the relatively prime kernel is bounded by

$$\begin{aligned}
\left|\sum_{d\mid p-1}\mu(d)\sum_{\substack{n\le p-1,\\ d\mid n}}\omega^{tn}\right| &= \left|\sum_{\gcd(n,p-1)=1}\omega^{tn}\right|\\
&\le \frac{4q\log\log p}{\pi t}, \qquad (32)
\end{aligned}$$

and by Lemma 3.4, the difference of two Gauss sums is bounded by

$$\begin{aligned}
&\left|\sum_{1\le s\le p-1}\omega^{-ts}e^{\frac{i2\pi b\tau^s}{p}} - \sum_{1\le s\le p-1}\omega^{-ts}e^{\frac{i2\pi\tau^s}{p}}\right|\\
=\ &\left|\sum_{1\le s\le p-1}\chi(t)\psi_b(t) - \sum_{1\le s\le p-1}\chi(t)\psi_1(t)\right|\\
\le\ & 4p^{1/2}\log p. \qquad (33)
\end{aligned}$$

Taking absolute value in (31) and replacing (32), and (33), return

$$\begin{aligned}
&\left|\sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} - \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p}\right|\\
\le\ & \frac{1}{q}\sum_{0\le t\le q-1}\left(4q^{1/2}\log q\right)\cdot\left(\frac{4q\log\log p}{t}\right) \qquad (34)\\
\le\ & 16q^{1/2}(\log q)(\log q)(\log\log p)\\
\le\ & 16p^{1/2}\log^3 p,
\end{aligned}$$

where $q = p + o(p)$. ■

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

$$\sum_{n\in\mathcal{A}} e^{i2\pi b\tau^n/p} = \sum_{n\in\mathcal{A}} e^{i2\pi\tau^n/p} + O(p^{1/2}\log^c p), \qquad (35)$$

for some constant $c > 0$.

3.3 Finite Summation Kernels And Gaussian Sums For Index $r = 1$

Lemma 3.2. *Let $p\ge 2$ and $q = p + o(p) \ge p$ be large primes. Let $\omega = e^{i2\pi/q}$ be a qth root of unity, and let $t\in[1,p-1]$. Then, for $x \le q-1$,*

(i)

$$\sum_{n\le x}\omega^{tn} = \frac{\omega^t - \omega^{t(x+2)}}{1-\omega^t},$$

(ii)
$$\left|\sum_{n\le x}\omega^{tn}\right|\le\frac{2q}{\pi t}.$$

Proof. (i) Use the geometric series to compute this simple exponential sum as
$$\sum_{n\le x}\omega^{tn}\quad=\quad\frac{\omega^{t}-\omega^{t(x+2)}}{1-\omega^{t}}.$$

(ii) Observe that the parameters $q=p+o(p)\ge p$ is prime, $\omega=e^{i2\pi/q}$, the integers $t\in[1,p-1]$, and $d\le p-1\le q-1$. 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
$$\left|\frac{\omega^{t}-\omega^{t(x+2)}}{1-\omega^{t}}\right|\le\left|\frac{2}{\sin(\pi t/q)}\right|\le\frac{2q}{\pi t}. \tag{36}$$

■

Lemma 3.3. *Let $p\ge 2$ and $q=p+o(p)\ge p$ be large primes, and let $\omega=e^{i2\pi/q}$ be a qth root of unity. Then,*

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

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

where $\mu(k)$ is the Mobius 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
$$\begin{aligned}\sum_{\gcd(n,p-1)=1}\omega^{tn}\quad&=\quad\sum_{n\le p-1}\omega^{tn}\sum_{\substack{d\mid p-1\\ d\mid n}}\mu(d)\\&=\quad\sum_{d\mid p-1}\mu(d)\sum_{\substack{n\le p-1\\ d\mid n}}\omega^{tn}\\&=\quad\sum_{d\mid p-1}\mu(d)\sum_{m\le(p-1)/d}\omega^{dtm}\\&=\quad\sum_{d\mid p-1}\mu(d)\frac{\omega^{dt}-\omega^{dt((p-1)/d+1)}}{1-\omega^{dt}}.\end{aligned}\tag{37}$$

(ii) Observe that the parameters $q=p+o(p)\ge p$ is prime, $\omega=e^{i2\pi/q}$, the integers $t\in[1,p-1]$, and $d\le p-1\le q-1$. This data implies that $\pi dt/q\ne k\pi$ with $k\in\mathbb{Z}$, so the sine function $\sin(\pi dt/q)\ne 0$ is well defined. Using standard manipulations, and $z/2\le\sin(z)<z$ for $0<|z|<\pi/2$, the last expression becomes
$$\left|\frac{\omega^{dt}-\omega^{dt((p-1)/d+1)}}{1-\omega^{dt}}\right|\le\left|\frac{2}{\sin(\pi dt/q)}\right|\le\frac{2q}{\pi dt} \tag{38}$$
for $1\le d\le p-1$. Finally, the upper bound is
$$\begin{aligned}\left|\sum_{d\mid p-1}\mu(d)\frac{\omega^{dt}-\omega^{dt((p-1)/d+1)}}{1-\omega^{dt}}\right|\quad&\le\quad\frac{2q}{\pi t}\sum_{d\mid p-1}\frac{1}{d}\\&\le\quad\frac{4q\log\log p}{\pi t}.\end{aligned}\tag{39}$$

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

Lemma 3.4. (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*

$$\left| \sum_{1\leq t\leq q-1} \chi(t)\psi(t) \right| \leq 2q^{1/2}\log q. \tag{40}$$

3.4 Incomplete And Complete Exponential Sums For Index $r > 1$

Theorem 3.3. *Let $p \geq 2$ be a large prime, and let τ be a primitive root modulo p. If $r \mid p-1$ is a small fixed*
divisor, then

$$\sum_{\gcd(n,(p-1)/r)=1} e^{i2\pi b\tau^{rn}/p} \ll p^{1-\varepsilon} \tag{41}$$

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

Proof. Similar to the proof of Theorem 3.2, mutatis mutandis. ■

Related but weaker upper bound appears in [6, Theorem 6], and related results are given in [3], [8], and [9, Theorem 1].

3.5 Equivalent Exponential Sums For Index $r > 1$

An asymptotic relation for the exponential sums

$$\sum_{\gcd(n,(p-1)/r)=1} e^{i2\pi b\tau^{rn}/p} \quad \text{and} \quad \sum_{\gcd(n,(p-1)/r)=1} e^{i2\pi\tau^{rn}/p}, \tag{42}$$

is provided in Lemma 3.5. This result expresses the first exponential sum in (42) as a sum of simpler exponential sum and an error term.

Lemma 3.5. *Let $p \geq 2$ and $q = p + o(p) \geq p$ be large primes. If τ be a primitive root modulo p, and $r \mid p-1$ is a small integer, then*

$$\sum_{\gcd(n,(p-1)/r)=1} e^{i2\pi b\tau^{rn}/p} = \sum_{\gcd(n,(p-1)/r)=1} e^{i2\pi\tau^{rn}/p} + O(p^{1/2}\log^3 p), \tag{43}$$

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

Proof. Similar to the proof of Lemma 3.1, mutatis mutandis. ■

4 Evaluations Of The Main Terms

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. In addition, many results are expressed in therms of the logarithm integral

$$\mathrm{li}(x) = \int_2^x \frac{1}{\log t}dt = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right). \tag{44}$$

Lemma 4.1. ([23, Lemma 5]) *Let $x \geq 1$ be a large number, and let $\varphi(n)$ be the Euler totient function. If $q \leq \log^c x$, with $c \geq 0$ constant, an integer $1 \leq a < q$ such that $\gcd(a, q) = 1$, then*

$$\sum_{\substack{p\leq x \\ p\equiv a \bmod q}} \frac{\varphi(p-1)}{p-1} = A_q \frac{\mathrm{li}(x)}{\varphi(q)} + O\left(\frac{x}{\log^b x}\right), \tag{45}$$

where $\operatorname{li}(x)$ *is the logarithm integral, and* $b > c + 1$ *is an arbitrary constant, as* $x \to \infty$, *and*

$$A_q = \prod_{p \mid \gcd(a-1,q)} \left(1 - \frac{1}{p}\right) \prod_{p \nmid q} \left(1 - \frac{1}{p(p-1)}\right). \tag{46}$$

Related discussions are given in [30, Lemma 1], [22, p. 16] and, [35]. The generalization to number fields appears in [13].

4.1 Main Term For Index $r = 1$

The case $q = 2$ with $a = 1$ of Lemma 4.1 is ubiquitous in various results in Number Theory.

Lemma 4.2. ([30, Lemma 1]) *Let* $x \geq 1$ *be a large number, let* $\operatorname{li}(x)$ *be the logarithm integral, and let* $\varphi(n)$ *be the Euler totient function. Then*

$$\sum_{p \leq x} \frac{\varphi(p-1)}{p-1} = a_1 \operatorname{li}(x) + O\left(\frac{x}{\log^b x}\right), \tag{47}$$

where $a_1 = 0.3937\ldots$ *is the average density, and* $b > 1$ *is an arbitrary constant, as* $x \to \infty$.

At $a = 1$, and $q = 2$, the constant (46) reduces to the average density

$$a_1 = \prod_{p \geq 2} \left(1 - \frac{1}{p(p-1)}\right) = 0.3739558136\ldots. \tag{48}$$

The average density of primitive roots modulo p was proved in [11] and [30], (the heuristic is due to Artin).

Lemma 4.3. *Let* $x \geq 1$ *be a large number, and let* $\operatorname{li}(x)$ *be the logarithm integral. Then*

$$\sum_{p \leq x} \frac{1}{p} \sum_{\gcd(n,p-1)=1} 1 = a_1 \operatorname{li}(x) + O\left(\frac{x}{\log^b x}\right), \tag{49}$$

where $b > 1$ *is an arbitrary constant,*

Proof. A routine rearrangement gives

$$\begin{aligned} \sum_{p \leq x} \frac{1}{p} \sum_{\gcd(n,p-1)=1} 1 &= \sum_{p \leq x} \frac{\varphi(p-1)}{p} \qquad (50) \\ &= \sum_{p \leq x} \frac{\varphi(p-1)}{p-1} - \sum_{p \leq x} \frac{\varphi(p-1)}{p(p-1)}. \end{aligned}$$

To proceed, apply Lemma 4.2 to reach

$$\sum_{p \leq x} \frac{\varphi(p-1)}{p-1} - \sum_{p \leq x} \frac{\varphi(p-1)}{p(p-1)} = a_1 \operatorname{li}(x) + O\left(\frac{x}{\log^b x}\right), \tag{51}$$

where the second finite sum

$$\sum_{p \leq x} \frac{\varphi(p-1)}{p(p-1)} = O(\log \log x) \tag{52}$$

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

4.2 Main Term For Index $r > 1$

Lemma 4.4. *Let $x \geq 1$ be a large number, let* li(x) *be the logarithm integral, and let $\varphi(n)$ be the Euler totient function. If $q = O(\log^c x)$ and $1 \leq a < q$ are integers such that* $\gcd(a, q) = 1$, *then*

$$\sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \frac{1}{p} \sum_{\gcd(n,p-1)=1} 1 = A_q \frac{\operatorname{li}(x)}{\varphi(q)} + O\left(\frac{x}{\log^b x}\right), \tag{53}$$

where $c \geq 0$, and $b > c + 1$ are arbitrary constants, and A_q is defined in (46)*, as $x \to \infty$.*

Proof. A routine rearrangement gives

$$\begin{aligned} \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \frac{1}{p} \sum_{\gcd(n,p-1)=1} 1 &= \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \frac{\varphi(p-1)}{p} \\ &= \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \frac{\varphi(p-1)}{p-1} - \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \frac{\varphi(p-1)}{p(p-1)}. \end{aligned} \tag{54}$$

To proceed, apply Lemma 4.1 to reach

$$\sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \frac{\varphi(p-1)}{p-1} - \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \frac{\varphi(p-1)}{p(p-1)} = A_q \frac{\operatorname{li}(x)}{\varphi(q)} + O\left(\frac{x}{\log^b x}\right),$$

where the second finite sum

$$\sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \frac{\varphi(p-1)}{p(p-1)} \ll \log \log x \tag{55}$$

is absorbed into the error term, $b > c + 1$ is an arbitrary constant, and A_q is defined in (46). ■

Lemma 4.5. *Let $x \geq 1$ be a large number, and let $r = O(\log^c x)$ be a small integer, $c \geq 0$ constant. Then*

$$\sum_{\substack{x \leq p \leq 2x \\ p \equiv 1 \bmod r}} \frac{1}{p} \sum_{\gcd(n,(p-1)/r)=1} 1 \geq \frac{A_r}{r\varphi(r)} (\operatorname{li}(2x) - \operatorname{li}(x)) + O\left(\frac{x}{r \log^b x}\right), \tag{56}$$

where $b > c + 1$ is an arbitrary constant, and A_q is defined in (46)*.*

Proof. First observe that for any divisor $r \mid p - 1$,

$$\begin{aligned} \sum_{\gcd(n,(p-1)/r)=1} 1 &= \varphi((p-1)/r) \\ &= \frac{p-1}{r} \prod_{q \mid (p-1)/r} \left(1 - \frac{1}{q}\right) \\ &\geq \frac{p-1}{r} \prod_{q \mid p-1} \left(1 - \frac{1}{q}\right) \\ &= \frac{1}{r} \varphi(p-1). \end{aligned} \tag{57}$$

Consequently

$$\sum_{\substack{x \leq p \leq 2x \\ p \equiv 1 \bmod r}} \frac{1}{p} \sum_{\gcd(n,(p-1)/r)=1} 1 \geq \frac{1}{r} \sum_{\substack{x \leq p \leq 2x \\ p \equiv 1 \bmod r}} \frac{\varphi(p-1)}{p}. \tag{58}$$

Apply Lemma 4.4 to the rigth side, (with $q = r = O(\log^c x)$, and $a = 1$), to reach

$$\sum_{\substack{x \leq p \leq 2x \\ p \equiv 1 \bmod r}} \frac{1}{p} \sum_{\gcd(n,(p-1)/r)=1} 1 \geq \frac{1}{r} \left(A_r \frac{\operatorname{li}(2x) - \operatorname{li}(x)}{\varphi(r)} + O\left(\frac{x}{\log^b x}\right)\right), \tag{59}$$

where $c \geq 0$ is a constant, and $b > c + 1$ is an arbitrary constant. ■

This result provides the exact asymptotic order of the primes counting function

$$\begin{aligned} \pi_u(x,r) &= \{p \leq x : \operatorname{ord}_p(u) = (p-1)/r\} \\ &= \delta(u,r)\operatorname{li}(x) + O\left(\frac{x}{\log^b x}\right), \end{aligned} \tag{60}$$

see [19], [37]. The density

$$\delta(u,r) = \lim_{x\to\infty} \frac{\{p \leq x : \operatorname{ord}_p(u) = (p-1)/r\}}{\pi(x)} \tag{61}$$

of the subset of primes $p \geq 2$ with fixed near primitive root $u \neq \pm 1$ of index $r \geq 1$ has various descriptions. For example, Lemma 4.5 suggests

$$\delta(u,r) = \frac{a(u,r)A_r}{r\varphi(r)}, \tag{62}$$

where $a(u,r) \in \mathbb{Q}$ is a rational correction factor. At $r = 1$, it reduces to the standard density formula (86). Other descriptions are given in [37], [28], [25], et cetera. In addition, it decreases approximately as $1/r^2$, and the current form of the prime number theorem for primes in the arithmetic progressions $\{p = rn + a : n \geq 1\}$ with $\gcd(r,a) = 1$ is restricted to $r = O(\log^c x)$. Theses data restrict the index to the small value $r = O(\log^c x)$ for any constant $c \geq 0$.

5 Estimate For The Error Term

The upper bounds for exponential sums over subsets of elements in finite fields $\mathbb{F}_p$ stated in the last section will be used here to estimate the error terms $E(x)$ and $E_r(x)$ arising in the proofs of Theorem 6.1 and Theorem 9.1.

5.1 Error Term For Index $r = 1$

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,*

$$\sum_{x\leq p\leq 2x} \frac{1}{p} \sum_{\gcd(n,p-1)=1,\ 0<m\leq p-1} \psi\left((\tau^n - u)m\right) \ll \frac{x^{1-\varepsilon}}{\log x} \tag{63}$$

for all sufficiently large numbers $x \geq 1$ and an arbitrarily small number $\varepsilon < 1/2$.

Proof. Rearrange the triple finite sum in the form

$$\begin{aligned} E(x) &= \sum_{x\leq p\leq 2x} \frac{1}{p} \sum_{0<m\leq p-1,\ \gcd(n,p-1)=1} \psi((\tau^n - u)m) \\ &= \sum_{x\leq p\leq 2x} \left(\frac{1}{p} \sum_{0<m\leq p-1} e^{-i2\pi\frac{um}{p}}\right) \left(\sum_{\gcd(n,p-1)=1} e^{i2\pi\frac{m\tau^n}{p}}\right). \end{aligned} \tag{64}$$

Applying Lemma 3.1 yields

$$\begin{aligned} E(x) &= \sum_{x\leq p\leq 2x} \left(\frac{1}{p} \sum_{0<m\leq p-1} e^{-i2\pi\frac{um}{p}}\right) \left(\sum_{\gcd(n,p-1)=1} e^{i2\pi\frac{\tau^n}{p}} + O(p^{1/2}\log^3 p)\right) \\ &= \sum_{x\leq p\leq 2x} U_p V_p. \end{aligned} \tag{65}$$

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

$$|U_p| = \left|\frac{1}{p} \sum_{0<m\leq p-1} e^{-i2\pi um/p}\right| = \frac{1}{p}. \tag{66}$$

This follows from the exact value $\sum_{0<m\leq p-1} e^{i2\pi um/p}=-1$ for $u\neq 0$. 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 3.2. A related exponential sum application appears in [26, 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 $\pi(2x)-\pi(x)\leq 2x/\log x$. ■

5.2 Error Term For Index $r>1$

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 near primitive root, and any $r\mid p-1$, then,*

$$\left| \sum_{\substack{x\leq p\leq 2x \\ p\equiv a \bmod q}} \frac{1}{p} \sum_{\gcd(n,(p-1)/r)=1,\, 0<m\leq p-1} \psi\left((\tau^{rn}-u)m\right)\right| \ll \frac{1}{\varphi(q)}\frac{x^{1-\varepsilon}}{\log x}, \tag{69}$$

where $1\leq a<q$, $\gcd(a,q)=1$ and $q=O(\log^c x)$, and $r=O(\log^c x)$, with $c\geq 0$ constant, for all sufficiently large numbers $x\geq 1$ and an arbitrarily small number $\varepsilon<1/2$.

Proof. Rearrange the triple finite sum in the form

$$\begin{aligned} E_r(x) &= \sum_{\substack{x\leq p\leq 2x \\ p\equiv a \bmod q}} \frac{1}{p} \sum_{0<m\leq p-1,\ \gcd(n,(p-1)/r)=1} \psi((\tau^{rn}-u)m) \\ &= \sum_{\substack{x\leq p\leq 2x \\ p\equiv a \bmod q}} \frac{1}{p} \sum_{0<m\leq p-1} e^{-i2\pi um/p} \sum_{\gcd(n,(p-1)/r)=1} e^{i2\pi m\tau^{rn}/p}. \end{aligned} \tag{70}$$

Applying Lemma 3.5 yields

$$\begin{aligned} &E_r(x) \\ &= \sum_{\substack{x\leq p\leq 2x \\ p\equiv a \bmod q}} \left(\frac{1}{p} \sum_{0<m\leq p-1} e^{-i2\pi um/p}\right) \left(\sum_{\gcd(n,(p-1)/r)=1} e^{i2\pi\tau^{rn}/p} + O(p^{1/2}\log^2 p)\right) \\ &= \sum_{\substack{x\leq p\leq 2x \\ p\equiv a \bmod q}} U_p\cdot V_p. \end{aligned} \tag{71}$$

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

$$|U_p| = \left| \frac{1}{p} \sum_{0<m\leq p-1} e^{-i2\pi um/p} \right| = \frac{1}{p}. \tag{72}$$

This follows from $\sum_{0<m\leq p-1} e^{i2\pi um/p} = -1$ for $u \neq 0$ and summation of the geometric series. The absolute value of the second exponential sum V_p has the upper bound

$$\begin{aligned} |V_p| &= \left| \sum_{\gcd(n,(p-1)/r)=1} e^{i2\pi\tau^{rn}} + O\left(p^{1/2}\log^2 p\right) \right| \\ &\ll \left| \sum_{\gcd(n,(p-1)/r)=1} e^{i2\pi\tau^{rn}} \right| + p^{1/2}\log^2 p \\ &\ll p^{1-\varepsilon}, \end{aligned} \tag{73}$$

where $\varepsilon < 1/2$ is an arbitrarily small number, see Theorem 3.3. Now, replace the estimates (72) and (73) into (71), to reach

$$\begin{aligned} \left| \sum_{\substack{x\leq p\leq 2x \\ p\equiv a \bmod q}} U_p V_p \right| &\leq \sum_{\substack{x\leq p\leq 2x \\ p\equiv a \bmod q}} |U_p V_p| \\ &\ll \sum_{\substack{x\leq p\leq 2x \\ p\equiv a \bmod q}} \frac{1}{p} \cdot p^{1-\varepsilon} \\ &\ll \frac{1}{x^{\varepsilon}} \sum_{\substack{x\leq p\leq 2x \\ p\equiv a \bmod q}} 1 \\ &\ll \frac{1}{\varphi(q)} \frac{x^{1-\varepsilon}}{\log x}. \end{aligned} \tag{74}$$

The last finite sum over the primes is estimated using the Brun-Titchmarsh theorem; this result states that the number of primes $p = qn + a$ in the interval $[x, 2x]$ satisfies the inequality

$$\pi(2x, q, a) - \pi(x, q, a) \leq \frac{3}{\varphi(q)} \frac{x}{\log x}, \tag{75}$$

see [16, p. 167], [15, p. 157], [20], et cetera. ■

6 Result For Index $r = 1$

This section is concerned with a general result for the densities of primes with fixed primitive roots and the primes counting function. The leading results on the Artin primitive root conjecture are Hooley conditional proof in [14] for the asymptotic formula

$$\begin{aligned} \pi_u(x) &= \#\{p \leq x : \operatorname{ord}_p(u) = p-1\} \\ &= \delta(u)\operatorname{li}(x) + O\left(\frac{x\log\log x}{\log^2 x)}\right), \end{aligned} \tag{76}$$

and the partial results in [27] and [12].

Theorem 6.1. *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 primes counting function has the asymptotic formula*

$$\pi_u(x) = \delta(u)\operatorname{li}(x) + O\left(\frac{x}{\log^b x}\right), \tag{77}$$

where $\delta(u) \geq 0$ is the density constant depending on the integer $u \neq 0$, and $b > 1$ 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

$$\Psi(u) = \begin{cases} 1 & \text{if } \operatorname{ord}_p(u) = p-1, \\ 0 & \text{if } \operatorname{ord}_p(u) \neq p-1, \end{cases} \tag{78}$$

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

$$0 = \sum_{x \leq p \leq 2x} \Psi(u). \tag{79}$$

Replacing the characteristic function, Lemma 2.1, and expanding the nonexistence equation (79) yield

$$\begin{aligned} 0 &= \sum_{x \leq p \leq 2x} \Psi(u) && (80) \\ &= \sum_{x \leq p \leq 2x} \frac{1}{p} \sum_{\gcd(n,p-1)=1,} \sum_{0 \leq m \leq p-1} \psi\left((\tau^n - u)m\right) \\ &= \sum_{x \leq p \leq 2x} \frac{1}{p} \sum_{\gcd(n,p-1=1} 1 + \sum_{x \leq p \leq 2x} \frac{1}{p} \sum_{\gcd(n,p-1)=1,} \sum_{0 < m \leq p-1} \psi\left((\tau^n - u)m\right) \\ &= M(x) + E(x). \end{aligned}$$

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 4.3 to the main term, and Lemma 5.2 to the error term yield

$$\begin{aligned} \sum_{x \leq p \leq 2x} \Psi(u) &= M(x) + E(x) && (81) \\ &= \delta(u)\left(\operatorname{li}(2x) - \operatorname{li}(x)\right) + O\left(\frac{x}{\log^b x}\right) + O\left(\frac{x^{1-\varepsilon}}{\log x}\right) \\ &= \delta(u)\left(\operatorname{li}(2x) - \operatorname{li}(x)\right) + O\left(\frac{x}{\log^b x}\right) \\ &> 0, \end{aligned}$$

where $b > 1$. However, $\delta(u) > 0$ contradicts the hypothesis (79) for all sufficiently large numbers $x \geq x_0$. Ergo, the short interval $[x, 2x]$ contains primes with the fixed primitive root u. ■

Information on the determination of the density $\delta(u) > 0$ of primes, with a fixed primitive root $u \neq \pm 1, v^2$, is provided in the Section 8, and in [14, p. 220].

7 Primes With Maximal Repeated Decimals

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

$$\frac{1}{p} = \frac{m}{10^w} + \frac{m}{10^{2w}} + \cdots = m \sum_{n \geq 1} \frac{1}{10^{wn}} = \frac{m}{10^w - 1} \tag{82}$$

has the maximal period $w = p - 1$ if and only if 10 has order $\operatorname{ord}_p(10) = p - 1$ modulo p. This follows from the Fermat little theorem and $10^w - 1 = mp$. The exceptions, which are known as Abel-Wieferich primes, satisfy the congruence

$$10^{p-1} - 1 \equiv 0 \bmod p^2, \tag{83}$$

confer [29, p. 333], [4] for other details. Further applications of the digits of the repeated decimals to class numbers of quadratic fields are derived in [38, P. 183], [10], [26] et alii.

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

Proof. (Theorem 1.1) This follows from Theorem 6.1 replacing the base $u = 10$. That is,

$$\pi_{10}(x) = \sum_{p \leq x} \Psi(10) = \delta(10)\,\mathrm{li}(x) + O\left(\frac{x}{\log^b x}\right), \tag{84}$$

where $b > 1$ is a constant. ∎

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

8 Numerical Data For Index $r = 1$

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 [32], and the advanced theory involved in the correction appears in [18] 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 $u \in \{2, 3, 5, 6, 7, 8, 10\}$.

In the case of a decimal base $u = 10$, the the constant $\delta(10)$ is the same as the average density

$$\delta(10) = a_1 = \prod_{p \geq 2}\left(1 - \frac{1}{p(p-1)}\right) = 0.3739558136192022880547280\ldots. \tag{85}$$

This numerical value was computed in [36]. And the corrected densities for other $u \in \{2, 3, 5, 6, 7, 8, 10\}$ were computed with formula proved in [14, 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

$$a_k(u) = \prod_{p \mid k} \frac{1}{p-1} \prod_{p \nmid k}\left(1 - \frac{1}{p(p-1)}\right). \tag{86}$$

1. If $s \not\equiv 1 \bmod 4$, then,
$$\delta(u) = a_k(u). \tag{87}$$

2. If $s \equiv 1 \bmod 4$, then,
$$\delta(u) = \left(1 - \mu(s) \prod_{\substack{p \mid s \\ p \mid k}} \frac{1}{p-2} \prod_{\substack{p \mid s \\ p \nmid k}} \frac{1}{p^2 - p - 1}\right) a_k(u). \tag{88}$$

As illustrated in Table 1, the error rate is within the optimum predicted range

$$R_1(x) = \left|\pi_u(x) - \delta(u)\frac{x}{\log x}\right| = O\left(x^{1/2}\log x\right). \tag{89}$$

Table 1: Statistics For Primes And Primitive Roots, $\pi(x) = 10^6$

Root	Density	Actual	Prediction	Error
u	$\delta(u)$	$\pi_u(x)$	$\delta(u)\frac{x}{\log x}$	$R_1(x)$
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

9 Result For Index $r > 1$

This section is concerned with a general result for the densities of primes with fixed near primitive roots, and the primes counting function. For any index $r > 1$, the leading results are the various forms of the conditional asymptotic formula

$$\begin{aligned} \pi_u(x,r) &= \#\{p \leq x : \operatorname{ord}_p(u) = (p-1)/r\} \\ &= \delta(u,r)\operatorname{li}(x) + O\left(\frac{x}{\log^b x)}\right), \end{aligned} \tag{90}$$

and the density $\delta(u,r)$, proved by [19], [37], and [28].

Theorem 9.1. *Let $x \geq 1$ be a large number, and let $r = O(\log^c x)$. A fixed integer $u \neq \pm 1$ is a near primitive root mod p of index r for infinitely many primes $p \geq 2$. In addition, the primes counting function has the asymptotic formula*

$$\pi_u(x,r) = \delta(u,r)\operatorname{li}(x) + O\left(\frac{x}{\log^b x)}\right), \tag{91}$$

where $b > c+1$ and $c \geq 0$ are constants, $\delta(u,r) \geq 0$ is the density depending on the integer $u \neq 0, \pm 1$, and $r \geq 1$, for all large numbers $x \geq 1$.

Proof. Suppose that $u \neq \pm 1$ is not an element of order $w = \operatorname{ord}_p(u) = (p-1)/r$ modulo p 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 index r characteristic function

$$\Psi_r(u) = \begin{cases} 1 & \text{if } \operatorname{ord}_p(u) = (p-1)/r, \\ 0 & \text{if } \operatorname{ord}_p(u) \neq (p-1)/r, \end{cases} \tag{92}$$

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

$$0 = \sum_{\substack{x \leq p \leq 2x \\ p \equiv 1 \bmod r}} \Psi_r(u). \tag{93}$$

Replacing the characteristic function, Lemma 2.2, and expanding the nonexistence equation (93) yield

$$\begin{aligned} 0 &= \sum_{\substack{x\le p\le 2x \\ p\equiv 1 \bmod r}} \Psi_r(u) \\ &= \sum_{\substack{x\le p\le 2x \\ p\equiv 1 \bmod r}} \frac{1}{p} \sum_{\gcd(n,(p-1)/r)=1,\, 0\le m\le p-1} \sum \psi\left((\tau^{rn}-u)m\right) \qquad (94) \\ &= \sum_{\substack{x\le p\le 2x \\ p\equiv 1 \bmod r}} \frac{1}{p} \sum_{\gcd(n,(p-1)/r)=1} 1 \\ &\qquad + \sum_{\substack{x\le p\le 2x \\ p\equiv 1 \bmod r}} \frac{1}{p} \sum_{\gcd(n,(p-1)/r)=1,\, 0< m\le p-1} \sum \psi\left((\tau^{rn}-u)m\right) \\ &= M_r(x)+E_r(x). \end{aligned}$$

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

Applying Lemma 4.5 to the main term, and Lemma 5.2 (with $a = 1$ and $q = r$), to the error term yield

$$\begin{aligned} \sum_{\substack{x\le p\le 2x \\ p\equiv 1 \bmod r}} \Psi_w(u) &= M_r(x)+E_r(x) \qquad (95) \\ &\geq \frac{1}{r}\left(A_r \frac{\operatorname{li}(2x)-\operatorname{li}(x)}{\varphi(r)} + O\left(\frac{x}{\log^b x}\right)\right) + O\left(\frac{1}{\varphi(r)}\frac{x^{1-\varepsilon}}{\log x}\right) \\ &\geq \frac{A_r}{r\varphi(r)}\left(\operatorname{li}(2x)-\operatorname{li}(x)\right) + O\left(\frac{x}{r\log^b x}\right) \\ &> 0. \end{aligned}$$

Since $\delta(u,r) \geq A_r/r\varphi(r) > 0$ for almost every fixed pair u and $r \geq 1$, this contradicts the hypothesis (93) for any $\delta(u,r) > 0$, and all sufficiently large numbers $x \geq x_0$. Ergo, the short interval $[x, 2x]$ contains primes such that the fixed element u has order $w = \operatorname{ord}_p(u) = (p-1)/r$ modulo p ■

For example, $\delta(10,r) > 0$ for all $r \geq 1$, see Section 9 for the actual calculations. The only exception is $\delta(u,r) = 0$ for any pair $r = 2a+1 \geq 1$ and $u = 4b+2 \geq 2$, see [19], [37], [28, Table 1], and [24].

10 Primes With Near Maximal Repeated Decimals

Let $p \geq 2$ be a prime, and let $r \mid p-1$ be a proper divisor. The repeating decimal fractions of near maximal period $w = (p-1)/r$ over the squarefree base $u = 10$ has the decimal fraction representation

$$\frac{1}{p} = \frac{m}{10^w} + \frac{m}{10^{2w}} + \cdots = m\sum_{n\geq 1}\frac{1}{10^{wn}} = \frac{m}{10^w-1}. \qquad (96)$$

Clearly, the near maximal period $w = (p-1)/r$ occur if and only if 10 has order $\operatorname{ord}_p(10) = (p-1)/r$ modulo p. This follows from the Fermat little theorem and $10^w - 1 = mp$. The result for repeating decimal of near maximal period is a simple corollary of the previous result.

Proof. (Theorem 1.2) This follows from Theorem 9.1 replacing the base $u = 10$. That is,

$$\pi_{10}(x,r) = \sum_{\substack{p\le x \\ p\equiv 1 \bmod r}} \Psi(10) = \delta(10,r)\operatorname{li}(x) + O\left(\frac{x}{\log^b x}\right), \qquad (97)$$

where $b > c + 1$ and $c \geq 0$ are constants for all large number $x \geq 1$. ■

11 Numerical Data For Index $r > 1$

There are very few numerical results for the density of primes with fixed near primitive roots, the data in Table 1 in [37] for $\delta(2, r)$, where $r \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, and $\pi(x) = 9592$, is the only one available in the literature. A numerical experiment was conducted to extend this calculation to $\delta(10, r)$. The numerical experiment employed $\pi(x) = 1000000$ primes for the near primitive root $u = 10$ and index $r \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

For the integer $u = 10$, and $r \geq 1$, the density has the precise form

$$\delta(u, r) = \begin{cases} E(r)a_1 & \text{if } 4 \nmid r, \\ (1 - B(r)/3)E(r)a_1 & \text{if } 4 \mid\mid r, \\ (1 + B(r))E(r)a_1 & \text{if } 8 \mid r, \end{cases} \tag{98}$$

where $a_1 = 0.3739558136\ldots$, see (48), and (85), and

$$E(r) = \frac{1}{r^2}\prod_{p \mid r}\frac{p^2 - 1}{p^2 - p - 1}, \quad A(r) = \frac{u}{\gcd(u, r)}, \quad B(r) = \prod_{p \mid A(r)}\frac{-1}{p^2 - p - 1}. \tag{99}$$

Furthermore, in the case $u = 10$, the average density is

$$\overline{\delta(10, r)} = \frac{a_1}{r^2}\prod_{p \mid r}\frac{p^2 - 1}{p^2 - p - 1}, \tag{100}$$

and the rational correction factor $a(u, r) \in \mathbb{Q}$ is not random, see (98). The density $\delta(u, r) = a(u, r)A_r/(r\varphi(r)) \geq 0$, where $a(u, r) \in \mathbb{Q}$ is rational, of primes with a fixed near primitive root $u \neq \pm 1$ has a complicated structure depending on both integers $u \neq \pm 1$ and $r \geq 1$. The properties of these constants were investigated by [19], [37], [28], [24], and [25].

As illustrated in Table 2, the error rate is within the optimum predicted range

$$R_r(x) = \left|\pi_u(x, r) - \delta(u, r)\frac{x}{\log x}\right| = O\left(x^{1/2}\log x\right). \tag{101}$$

12 The Analytic Properties of the Index

Given a large number $x \geq 1$, a prime $p \leq x$, and an integer $u \neq 0, \pm 1$, the average index $r = [(\mathbb{Z}/p\mathbb{Z})^{\times} : \langle u \mod p\rangle]$ is expected to satisfies

$$r = c_u \log x + o(\log x), \tag{102}$$

where $c_u > 0$ is a constant depending on the integer u. Currently, this is an open problem. An earlier closely related result, conditional on the GRH, states that

$$\sum_{p \leq x}\frac{1}{\operatorname{ind}_p(u)} = a_u\frac{x}{\log x} + O\left(\frac{x \log\log}{\log^2 x}\right), \tag{103}$$

where a_u is a density constant, see [31, Theorem 1]. Some of the recent analytic results for the index $r \geq 1$ are investigated in [5], [1], et alii.

Table 2: Statistics For Primes And Near Primitive Roots, $\pi(x) = 10^6$

Index r	Density $\delta(u,r)$	Actual $\pi_u(x,r)$	Prediction $\delta(u,r)\frac{x}{\log x}$	Error $R_r(x)$
1	a_1	374125	373955.8	169.2
2	$\frac{3a_1}{4}$	280267	280467.00	-199.86
3	$\frac{8a_1}{45}$	66487	66481.00	5.97
4	$\frac{29a_1}{52}$	71297	70116.7	-49.83
5	$\frac{24a_1}{475}$	18879	18894.60	-15.61
6	$\frac{2a_1}{15}$	49894	49860.80	33.22
7	$\frac{48a_1}{2009}$	8827	8934.73	-107.73
8	$\frac{27a_1}{608}$	16761	16606.6	154.41
9	$\frac{8a_1}{405}$	7409	7386.78	22.22
10	$\frac{18a_1}{475}$	14305	14171.00	134.04

References

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

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

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

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

[5] Felix, Adam Tyler. The index of a modulo p. SCHOLAR- 83-96, Contemp. Math., 655, Centre Rech. Math. Proc., Amer. Math. Soc., Providence, RI, 2015.

[6] Friedlander, John B.; Hansen, Jan; Shparlinski, Igor E. Character sums with exponential functions. Mathematika 47 (2000), no. 1-2, 75 -85 (2002).

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

[8] Garaev, M. Z. Double exponential sums related to Diffie-Hellman distributions. Int. Math. Res. Not. 2005, no. 17, 1005-1014.

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

[10] Girstmair, Kurt. A "popular" class number formula. Amer. Math. Monthly 101 (1994), no. 10, 997-1001.

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

[12] Heath-Brown, D. R. Artins conjecture for primitive roots. Quart. J. Math. Oxford Ser. (2) 37 (1986), no. 145, 27-38.

[13] Hinz, Jurgen G. Some applications of sieve methods in algebraic number fields. Manuscripta Math. 48 (1984), no. 1-3, 117-137.

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

[15] Harman, Glyn. Prime-detecting sieves. London Mathematical Society Monographs Series, 33. Princeton University Press, Princeton, NJ, 2007.

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

[17] 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.

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

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

[20] Maynard, James. On the Brun-Titchmarsh theorem. Acta Arith. 157 (2013), no. 3, 249-296.

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

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

[23] Moree, Pieter. On primes in arithmetic progression having a prescribed primitive root. J. Number Theory 78 (1999), no. 1, 85-98.

[24] Moree, Pieter. Asymptotically exact heuristics for (near) primitive roots. J. Number Theory 83 (2000), no. 1, 155-181.

[25] Moree, Pieter. Near-primitive roots. Funct. Approx. Comment. Math. 48 (2013), part 1, 133-145.

[26] Murty, M. Ram; Thangadurai, R. The class number of $Q(\sqrt{-p})$ and digits of $1/p$. Proc. Amer. Math. Soc. 139 (2011), no. 4, 1277-1289.

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

[28] Murata, Leo. A problem analogous to Artin's conjecture for primitive roots and its applications. Arch. Math. (Basel) 57 (1991), no. 6, 555-565.

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

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

[31] Stephens, P. J. Prime divisors of second-order linear recurrences. I. J. Number Theory 8 (1976), no. 3, 313-332.

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

[34] Tenenbaum, Gerald. Introduction to analytic and probabilistic number theory. Translated from the Third French edition. American Mathematical Society, Rhode Island, 2015.

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

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

[37] Wagstaff, Samuel S., Jr. Pseudoprimes and a generalization of Artin's conjecture. Acta Arith. 41 (1982), no. 2, 141-150.

[38] Zagier, Don. A Kronecker limit formula for real quadratic fields. Math. Ann. 213 (1975), 153-184.