Primitive Roots In Short Intervals

N. A. Carella

Abstract: Let \( p \geq 2 \) be a large prime, and let \( N \gg (\log p)^{1+\varepsilon} \). This note proves the existence of primitive roots in the short interval \([M, M+N]\), where \( M \geq 2 \) is a fixed number, and \( \varepsilon > 0 \) is a small number. In particular, the least primitive root \( g(p) = O ((\log p)^{1+\varepsilon}) \), and the least prime primitive root \( g^*(p) = O ((\log p)^{2+\varepsilon}) \) unconditionally.

Mathematics Subject Classifications: Primary 11A07, Secondary 11N37.

Keywords: Least primitive root; Least prime primitive root; Primitive root in short interval.

1 Introduction

Given a large prime \( p \geq 2 \), and a number \( N \leq p \). The standard analytic methods demonstrate the existence of primitive roots in any short interval

\[
[M, M+N]
\]

(1)

for any number \( N \gg p^{1/2+\varepsilon} \), where \( M \geq 2 \) is a fixed number, and \( \varepsilon > 0 \) is a small number, see [10], [12], [8], [35]. More elaborate exponential sums methods can reduce the size of the interval to \( N \gg p^{1/4+\varepsilon} \), see [2]. And recently, it was proved that the least prime primitive root \( g^*(p) = O (p^\varepsilon) \), unconditionally, see [9]. Further, the explicit upper bound claims that the least primitive root \( g(p) \geq 2 \) satisfies the inequality

\[
g(p) < \sqrt{p} - 2
\]

(2)

for all primes \( p > 409 \), see [10], and [30]. Assuming standard conjectures, the least primitive root is expected to be \( g(p) = O ((\log \log p)^2) \), and the average value is expected to be \( g(p) = O ((\log \log p)^2) \), see [10] and [9] respectively.

Almost all these results are based on standard indicator function in Lemma 2.1. This note introduces a new technique based on indicator function in Lemma 2.2 to improve the results for primitive roots in short intervals.

Theorem 1.1. Given a small number \( \varepsilon > 0 \), and a sufficiently large prime \( p \geq 2 \), let \( N \gg (\log p)^{1+\varepsilon} \). Then, the short interval

\[
[M, M+N]
\]

(3)

contains a primitive root for any fixed \( M \geq 2 \). In particular, the least primitive root \( g(p) = O ((\log p)^{1+\varepsilon}) \) unconditionally.
As the probability of a primitive root modulo $p$ is $O(1/\log \log p)$, this result is nearly optimal, see Section 4 for a discussion. The existence of prime primitive roots requires information about primes in short intervals such that $N < p^{1/2}$, and $M \geq 2$ is any fixed number, which is not available in the literature. But, for the long interval $[2, x]$, it is feasible.

**Theorem 1.2.** If $p \geq 2$ is a sufficiently large prime, then, the least prime primitive root satisfies

$$g^*(p) = O \left( (\log p)^{2+\varepsilon} \right)$$

for any small number $\varepsilon > 0$, unconditionally.

**Theorem 1.3.** Let $p \geq 2$ be a sufficiently large prime, and let $N \gg p^{525}$. Then, the short interval $[M, M+N]$ contains a prime primitive root for any fixed $M \geq 2$ unconditionally.

The fundamental background materials are discussed in the earlier sections. Section 8 presents a proof of Theorem 1.1, the penultimate section presents a proof of Theorem 1.2, and the last section presents a proof of Theorem 1.3.

### 2 Representations of the Characteristic Functions

The characteristic function $\Psi : G \rightarrow \{0, 1\}$ 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 $\Psi$ of primitive elements are possible. Several of these representations are studied in this section.

#### 2.1 Divisors Dependent Characteristic Function

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

**Definition 2.1.** The order of an element in the cyclic group $\mathbb{F}_p^\times$ is defined by $\operatorname{ord}_p(v) = \min\{k : v^k \equiv 1 \mod p\}$. Primitive elements in this cyclic group have order $p - 1 = \#G$.

**Lemma 2.1.** Let $G$ be a finite cyclic group of order $p - 1 = \#G$, and let $0 \neq u \in G$ be an invertible element of the group. Then

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

The works in [12], and [41] attribute this formula to Vinogradov. The proof and other details on the characteristic function are given in [16, p. 863], [26, p. 258], [28, p. 18]. The characteristic function for multiple primitive roots is used in [11, p. 146] to study consecutive primitive roots. In [14] it is used to study the gap between primitive roots with respect to the Hamming metric. And in [11] it is used to prove the existence of primitive roots in certain small subsets $A \subset \mathbb{F}_p$. In [12] it is used to prove that some finite fields do not have primitive roots of the form $a\tau + b$, with $\tau$ primitive and $a, b \in \mathbb{F}_p$ constants. In addition, the Artin primitive root conjecture for polynomials over finite fields was proved in [34] using this formula.
2.2 Divisors Free Characteristic Function

It often difficult to derive any meaningful result using the usual divisors dependent characteristic function of primitive elements given in Lemma 2.1. 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 [16], [14] for typical applications and [27] 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 2.1, detects the order \( \text{ord}_p(u) \) 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 2.2, detects the order \( \text{ord}_p(u) \geq 1 \) 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 \( u, \tau \) are constants, and \( 1 \leq n < p - 1, \gcd(n, p - 1) = 1 \), is a variable.

**Lemma 2.2.** Let \( p \geq 2 \) be a prime, and let \( \tau \) be a primitive root mod \( p \). If \( u \in \mathbb{F}_p \) is a nonzero element, and \( \psi \neq 1 \) is a nonprincipal additive character of order \( \text{ord}_p(\psi) = p \), then

\[
\Psi(u) = \sum_{\gcd(n, p - 1) = 1} \frac{1}{p} \sum_{0 \leq m \leq p - 1} \psi((\tau^n - u)m) = \begin{cases} 1 & \text{if } \text{ord}_p(u) = p - 1, \\ 0 & \text{if } \text{ord}_p(u) \neq p - 1. \end{cases}
\]

(7)

**Proof.** 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

\[
\tau^n - u = 0
\]

(8)

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

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

(9)

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

3 Primes Numbers Results

Some prime numbers results focusing on the local minima of the ratio

\[
\frac{\varphi(n)}{n} = \prod_{p \mid n} \left(1 - \frac{1}{p}\right) > \frac{1}{e^{\gamma} \log \log n + 5/(2 \log \log n)}
\]

(10)

are recorded in this section. The conditional results are studied in [32], and the unconditional results are proved by various authors as [37] Theorem 7 and Theorem 15, and [31] Theorem 2.9.

**Lemma 3.1.** Let \( n \geq 1 \) be a large integer, then

(i) The average number \( \omega(n) \) of prime divisors \( p \mid n \) satisfies

\[
\omega(n) \ll \log \log n.
\]
(ii) The maximal number $\omega(n)$ of prime divisors $p \mid n$ satisfies

$$\omega(n) \ll \log n / \log \log n.$$ 

Proof. A standard in analytic number theory, see [31, Theorem 2.6].

Lemma 3.2. Let $x \geq 2$ be a large number, then

(i) Unconditionally,

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \frac{1}{e^{\gamma} \log x} + O \left( e^{-c_0 \sqrt{\log x}} \right).$$

(ii) Unconditional oscillation,

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \frac{1}{e^{\gamma} \log x} + \Omega_{\pm} \left( \frac{\log \log x}{x^{1/2}} \right).$$

(iii) Conditional on the RH,

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \frac{1}{e^{\gamma} \log x} + O \left( \frac{\log x}{x^{1/2}} \right).$$

where $\gamma$ is Euler constant, and $c_0 > 0$ is an absolute constant.

The explicit estimates are given in [37, Theorem 7], and the results for products over arithmetic progression are proved in [25], et alii. The nonquantitative unconditional oscillations of the error of the product of primes is implied by the work of Phragmen, refer to equation (14), and [33, p. 182]. Since then, various authors have developed quantitative versions, see [37], [13], et alii.

4 Basic Statistics For Primitive roots

The probability of primitive roots in a finite field $F_p$ has the closed form $\varphi(p-1)/p \leq 1/2$. The maximal probability $\varphi(p-1)/p = 1/2$ occurs on the subset of Fermat primes

$$F = \{ p = 2^{2^n} + 1 : n \geq 0 \} = \{3, 5, 17, 257, 65537, \ldots\}.$$  

(11)

This is followed by the subset of Germain primes

$$S = \{ p = 2^a q + 1 : q \geq 2 \text{ is prime, and } a \geq 1 \} = \{5, 7, 11, 13, 23, 29, \ldots\},$$  

(12)

which has $\varphi(p-1)/p = (1/2)(1 - 1/q)$, et cetera. Some basic questions such as the sizes of these subsets of primes are open problems. In contrast, the minimal probabilities occur on the various subsets of primes with highly composite totients $p - 1$. For example, the subset

$$R = \{ p \geq 2 : p - 1 = 2^{v_2} \cdot 3^{v_3} \cdot 5^{v_5} \cdots q^{v_q}, \text{ and } v_i \geq 1 \} = \{3, 7, 31, 191, \ldots\}.$$  

(13)

In these cases, the probability function can have a complicated expression such as

$$\varphi(p-1)/p = \prod_{q \mid \log p} \left(1 - \frac{1}{q}\right) = \frac{1}{e^{\gamma} \log \log \log p} + \Omega_{\pm} \left( \frac{\log \log \log \log p}{(\log p)^{1/2}} \right).$$  

(14)
This is derived from the standard results in Lemma 3.1 and in Lemma 3.2. Further, the average probability over all the primes \( p \leq x \) is a well known constant
\[
a_0 = \frac{1}{\pi(x)} \sum_{p \leq x} \frac{\varphi(p-1)}{p} = \prod_{p > 2} \left( 1 - \frac{1}{p(p-1)} \right) = 0.3739558136 \ldots \tag{15}\]

The analysis of the average appears in [20], [38], and the numerical calculations in [42]. The distribution of primitive root for highly composite totients \( p - 1 \) is approximately a Poisson distribution with parameter \( \lambda > 0 \). For \( k \geq 0 \), and \( 1 \leq t \leq \delta \log \log p \), with \( \delta > 0 \), the probability function has the asymptotic formula
\[
P_k(t) \sim e^{-\lambda} \frac{\lambda^k}{k!}, \tag{16}\]
confer [11, Theorem 2] for the finer details.

## 5 Estimates Of Exponential Sums

This section provides results for the exponential sums of interest in this analysis. The upper bound in Lemma 5.1, and the equivalence relation
\[
\sum_{\gcd(n,p-1)=1} e^{i2\pi s \tau^n/p} = \sum_{\gcd(n,p-1)=1} e^{i2\pi \tau^n/p} + E(p), \tag{17}\]
where \( E(p) \) is an error term, in Lemma 5.2 are considered here.

### 5.1 Upper Bound of Exponential Sums

The estimates of interest in this work can also be derived from any of the double exponential sums proved in [18], and [21]. A different proof of this result appears in [19, Theorem 6].

**Lemma 5.1.** Let \( p \geq 2 \) be a large prime, and let \( \tau \) be a primitive root modulo \( p \). Then,
\[
\max_{\gcd(s,p-1)=1} \left| \sum_{\gcd(n,p-1)=1} e^{i2\pi s \tau^n/p} \right| \ll p^{1-\varepsilon} \tag{18}\]
for any arbitrary small number \( \varepsilon < 1/16 \).

### 5.2 Equivalent Exponential Sums

For any fixed \( 0 \neq s \in \mathbb{F}_p \), the map \( \tau^n \rightarrow s \tau^n \) is one-to-one in \( \mathbb{F}_p \). Consequently, the subsets
\[
\{ \tau^n : \gcd(n,p - 1) = 1 \} \quad \text{and} \quad \{ s \tau^n : \gcd(n,p - 1) = 1 \} \subset \mathbb{F}_p\tag{19}\]
have the same cardinalities. As a direct consequence the exponential sums
\[
\sum_{\gcd(n,p-1)=1} e^{i2\pi s \tau^n/p} \quad \text{and} \quad \sum_{\gcd(n,p-1)=1} e^{i2\pi \tau^n/p}, \tag{20}\]
have the same upper bound up to an error term. An asymptotic relation for the exponential sums [20] is provided in Lemma 5.2. This result expresses the first exponential sum in [20]
as a sum of simpler exponential sum and an error term. The proof is based on Lagrange resolvent
\[(\omega^t, \zeta^s) = \zeta^s + \omega^{-t} \zeta^{st} + \omega^{-2t} \zeta^{st^2} + \cdots + \omega^{-((q-1)t)} \zeta^{st^{q-1}}, \quad (21)\]
where \(\omega = e^{i2\pi/q}\), \(\zeta = e^{i2\pi/p}\), and \(0 \neq s, t \in \mathbb{F}_p\). This is a more general version of the resolvent based on the two large primes \(p \geq 2\) and \(q = p + o(p) > p\).

**Lemma 5.2.** Let \(p \geq 2\) and \(q = p + o(p) > p\) be large primes. If \(\tau\) be a primitive root modulo \(p\), then,
\[
\sum_{\gcd(n,p-1)=1} e^{i2\pi sn^p} = \sum_{\gcd(n,p-1)=1} e^{i2\pi \tau^n/p} + O(p^{1/2} \log^3 p), \quad (22)
\]
for any \(s \in [1, p - 1]\).

**Proof.** Summing \((21)\) times \(\omega^{ln}\) over the variable \(t \in \mathbb{Z}/q\mathbb{Z}\) yields
\[
q \cdot e^{i2\pi sn^p/p} = \sum_{0 \leq t \leq q-1} (\omega^t, \zeta^{st})\omega^{ln}. \quad (23)
\]
Summing \((23)\) over the relatively prime variable \(n < p - 1 < q - 1\) yields
\[
q \cdot \sum_{\gcd(n,p-1)=1} e^{i2\pi sn^p/p} = \sum_{\gcd(n,p-1)=1, 0 \leq t \leq q-1} \sum_{1 \leq t \leq q-1} (\omega^t, \zeta^{st})\sum_{\gcd(n,p-1)=1} \omega^{ln} - \varphi(q). \quad (24)
\]
The first index \(t = 0\) contributes \(\varphi(q)\), see [29, Equation (5)] for similar calculations. Likewise, the basic exponential sum for \(s = 1\) can be written as
\[
q \cdot \sum_{\gcd(n,p-1)=1} e^{i2\pi n^p/p} = \sum_{0 \leq t \leq p-1} (\omega^t, \zeta^t) \sum_{\gcd(n,p-1)=1} \omega^{ln} - \varphi(q), \quad (25)
\]
Differencing \((24)\) and \((25)\) produces
\[
S = q \cdot \left( \sum_{\gcd(n,p-1)=1} e^{i2\pi sn^p/p} - \sum_{\gcd(n,p-1)=1} e^{i2\pi \tau^n/p} \right) = \sum_{1 \leq t \leq q-1} ((\omega^t, \zeta^{st}) - (\omega^t, \zeta^t)) \sum_{\gcd(n,p-1)=1} \omega^{ln}. \quad (26)
\]
The right side of the sum \(S\) can be rewritten as
\[
S = \sum_{1 \leq t \leq q-1} ((\omega^t, \zeta^{st^n}) - (\omega^t, \zeta^{tn})) \sum_{\gcd(n,p-1)=1} \omega^{ln} = \sum_{1 \leq t \leq q-1} \sum_{d \leq p-1} ((\omega^t, \zeta^{st^n}) - (\omega^t, \zeta^{tn})) \mu(d) \frac{\omega^{dt} - \omega^{dtp}}{1 - \omega^{dt}}.
\]
The second line follows from Lemma 5.3. The upper bound

\[ |S| \leq \sum_{1 \leq t \leq q-1} \sum_{d \leq p-1} \left| (\omega^t, \zeta^{s^{tn}} - (\omega^t, \zeta^{s^{tn}}) \right| \mu(d) \frac{\omega^{dt} - \omega^{dtp}}{1 - \omega^{dt}} \]

\[ \leq \sum_{1 \leq t \leq q-1} \sum_{d \leq p-1} \left| (\omega^t, \zeta^{s^{tn}} - (\omega^t, \zeta^{s^{tn}}) \right| \mu(d) \frac{\omega^{dt} - \omega^{dtp}}{1 - \omega^{dt}} \]

\[ \leq \sum_{1 \leq t \leq q-1} \sum_{d \leq p-1} \left( 4q^{1/2} \log q \right) \mu(d) \frac{\omega^{dt} - \omega^{dtp}}{1 - \omega^{dt}} \]

\[ \leq \left( 4q^{3/2} \log q \log p \right) \sum_{1 \leq t \leq q-1} \frac{1}{t} \]

\[ \leq 8q^{3/2} \log^2 q \log p. \] (27)

The third line in (27) follows the upper bound for Lagrange resolvents in (28), and the fourth line follows from Lemma 5.3.ii. Here, the difference of two Lagrange resolvents, (Gauss sums), has the upper bound

\[ \left| (\omega^t, \zeta^{s^{tn}} - (\omega^t, \zeta^{s^{tn}}) \right| \leq 2 \sum_{1 \leq t \leq q-1} \chi(t) e^{i2\pi t/q} \leq 2q^{1/2} \log q, \] (28)

where \( |\chi(t)| = 1 \) is a root of unity. Taking absolute value in (29) and using (27) return

\[ q \cdot \sum_{\gcd(n,p-1)=1} e^{i2\pi s^{tn}/p} - \sum_{\gcd(n,p-1)=1} e^{i2\pi r^n/p} \leq |S| \]

\[ \leq 16q^{3/2} \log q \log p, \] (29)

where \( q = p + o(p) \). The last inequality implies the claim.

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

\[ \sum_{n \in A} e^{i2\pi s^{tn}/p} = \sum_{n \in A} e^{i2\pi r^n/p} + O(p^{1/2} \log c \cdot p), \] (30)

for some constant \( c > 0 \).

**Lemma 5.3.** Let \( p \geq 2 \) and \( q = p + o(p) > p \) be large primes, and let \( \omega = e^{i2\pi/q} \) be a qth root of unity. Then,

(i)

\[ \sum_{\gcd(n,p-1)=1} \omega^{tn} = \sum_{d \leq p-1} \mu(d) \frac{\omega^{dt} - \omega^{dtp}}{1 - \omega^{dt}}, \]

(ii)

\[ \sum_{\gcd(n,p-1)=1} \omega^{tn} \leq \frac{2q \log p}{\pi t}, \]

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

\[ \sum_{\gcd(n, p-1)=1} \omega^{tn} = \sum_{d \leq p-1} \mu(d) \sum_{d|n} \omega^{tn} \]

\[ = \sum_{d \leq p-1} \mu(d) \sum_{n \leq p-1} \omega^{tn} \]

\[ = \sum_{d \leq p-1} \mu(d) \sum_{m \leq (p-1)/d} \omega^{dtm} \]

\[ \leq \sum_{d \leq p-1} \mu(d) \frac{\omega^{dt} - \omega^{dt p}}{1 - \omega^{dt}}. \]

(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

\[ \left| \frac{\omega^{dt} - \omega^{dt p}}{1 - \omega^{dt}} \right| \leq \frac{2q}{\sin(\pi dt/q)} \leq \frac{2q}{\pi dt} \]

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

\[ \left| \sum_{d \leq p-1} \mu(d) \frac{\omega^{dt} - \omega^{dt p}}{1 - \omega^{dt}} \right| \leq \frac{2q}{\pi t} \sum_{d \leq p-1} \frac{1}{d} \]

\[ \leq \frac{2q \log p}{\pi t}. \]

6 Maximal Error Term

The upper bounds for exponential sums over subsets of elements in finite fields \( \mathbb{F}_p \) studied in Section 5 are used to estimate the error terms \( E(x, y) \) and \( E(x, \Lambda) \) in the proofs of Theorem 1.1 and Theorem 1.2 respectively.

6.1 Short Intervals

Lemma 6.1. Let \( p \geq 2 \) be a large prime, let \( \psi \neq 1 \) be an additive character, and let \( \tau \) be a primitive root mod \( p \). If the element \( u \neq 0 \) is not a primitive root, then,

\[ \frac{1}{p} \sum_{x \leq u \leq y, \gcd(n, p-1)=1} \sum_{0 < m \leq p-1} \psi ((\tau^n - u)m) \ll \frac{y-x}{p} \]

for all sufficiently large numbers \( 1 \leq x < y \leq p \), and an arbitrarily small number \( \varepsilon > 0 \).

Proof. By hypothesis \( \tau^n - u \neq 0 \), so \( \sum_{0 < m \leq p-1} \psi ((\tau^n - u)m) = -1 \). Since \( \varphi(p-1)/p \leq 1/2 \), a nontrivial error term

\[ |E(x, y)| < \left| \frac{\varphi(p-1)}{p} (y-x) \right| \leq \frac{y-x}{2} \]
can be computed. Toward this end let $\psi(z) = e^{i2\pi z/p}$, and rearrange the triple finite sum in the form

$$E(x, y) = \frac{1}{p} \sum_{x \leq u \leq y, 0 < m \leq p-1, \gcd(n, p-1) = 1} \psi((\tau^m - u)m)$$

(36)

$$= \frac{1}{p} \sum_{x \leq u \leq y} \left( \sum_{0 < m \leq p-1} e^{-i2\pi um/p} \right) \left( \sum_{\gcd(n, p-1) = 1} e^{i2\pi m\tau^m/p} \right)$$

$$= \frac{1}{p} \sum_{x \leq u \leq y} \left( \sum_{0 < m \leq p-1} e^{-i2\pi um/p} \right) \left( \sum_{\gcd(n, p-1) = 1} e^{i2\pi \tau^m/p} + O(p^{1/2} \log^3 p) \right)$$

$$= \frac{1}{p} \sum_{x \leq u \leq y} \left( \sum_{0 < m \leq p-1} e^{-i2\pi um/p} \right) \left( \sum_{\gcd(n, p-1) = 1} e^{i2\pi \tau^m/p} \right)$$

$$+ O \left( \frac{p^{1/2} \log^3 p}{p} \sum_{x \leq u \leq y, 0 < m \leq p-1} e^{-i2\pi um/p} \right)$$

$$= T_1 + T_2.$$

The third line in equation (36) follows from Lemma 5.2. The first exponential sum $T_1$ has the upper bound

$$|T_1| \leq \frac{1}{p} \sum_{x \leq u \leq y} \left| \sum_{0 < m \leq p-1} e^{-i2\pi um/p} \right| \left| \sum_{\gcd(n, p-1) = 1} e^{i2\pi \tau^m/p} \right|$$

(37)

$$\ll \frac{1}{p} \sum_{x \leq u \leq y} (1) \cdot (p^{1-\epsilon})$$

$$\ll \frac{y - x}{p^{\epsilon}},$$

where $\sum_{0 < m \leq p-1} e^{i2\pi um/p} = -1$ for any $u \in [x, y]$, with $1 \leq x < y < p$. And an application of Lemma 5.1. The second exponential sum $T_2$ has the upper bound

$$|T_2| = O \left( \frac{p^{1/2} \log^3 p}{p} \sum_{x \leq u \leq y} \left| \sum_{0 < m \leq p-1} e^{-i2\pi um/p} \right| \right)$$

(38)

$$= O \left( \frac{p^{1/2} \log^3 p}{p} \sum_{x \leq u \leq y} 1 \right)$$

$$= O \left( \frac{(y - x) \log^3 p}{p^{1/2}} \right).$$

Collecting (37) and (38) into one term returns

$$|E(x, y)| \leq |T_1| + |T_2| \ll \frac{y - x}{p^{\epsilon}}.$$

(39)

These complete the verification.

\[ \blacksquare \]
6.2 Long Intervals

The results available in the literature for primes in small intervals of the forms \([x, x + y]\) with \(y < x^{1/2}\) are not uniform. In light of this fact, only the error term for the simpler intervals \([2, x]\) can be computed effectively.

**Lemma 6.2.** Let \(p \geq 2\) be a large prime, let \(\psi \neq 1\) be an additive character, and let \(\tau\) be a primitive root mod \(p\). If the element \(u \neq 0\) is not a primitive root, then,

\[
\frac{1}{p} \sum_{u \leq x, \gcd(n, p-1)=1} \sum_{0 < m \leq p-1} \psi((\tau^n - u)m) \Lambda(u) \ll \frac{x}{p^e} \tag{40}
\]

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

**Proof.** Same as the previous one.

\[ \blacksquare \]

7 Asymptotics For The Main Terms

The notation \(f(x) \asymp g(x)\) is defined by \(a f(x) < g(x) < b f(x)\) for some constants \(a, b > 0\).

7.1 Short Intervals For Primitive Root

**Lemma 7.1.** Let \(p \geq 2\) be a large prime, and let \(1 \leq x < y < p\) be a pair of numbers. Then,

\[
\sum_{x \leq u \leq y} \frac{1}{p} \sum_{\gcd(n, p-1)=1} 1 \gg \frac{y - x}{\log \log p} \left(1 + O \left((\log \log p)e^{-c_0 \sqrt{\log \log p}}\right)\right). \tag{41}
\]

**Proof.** The maximal number \(\omega(p - 1)\) of prime divisors of highly composite totients \(p - 1\) satisfies \(\omega(p - 1) \gg \log p/\log \log p\). This implies that \(z \asymp \log p\). An application of Lemma 3.2 to the ratio returns

\[
\frac{\varphi(p - 1)}{p} = \prod_{q \leq z} \left(1 - \frac{1}{q}\right)
\]

\[
= \frac{1}{e^{\gamma} \log z} + O \left(e^{-c_0 \sqrt{\log z}}\right) \tag{42}
\]

\[
\gg \frac{1}{e^{\gamma} \log \log p} + O \left(e^{-c_0 \sqrt{\log \log p}}\right).
\]

Substituting this, the main term reduces to

\[
M(x, y) = \sum_{x \leq u \leq y} \frac{1}{p} \sum_{\gcd(n, p-1)=1} 1
\]

\[
= \frac{\varphi(p - 1)}{p} (y - x)
\]

\[
\gg \left(\frac{1}{e^{\gamma} \log \log p} + O \left(e^{-c_0 \sqrt{\log \log p}}\right)\right) (y - x). \tag{43}
\]

The proves the claim.

\[ \blacksquare \]
7.2 Long Intervals For Prime Primitive Root

Lemma 7.2. Let \( p \geq 2 \) be a large prime, and let \( x < p \) be a number. Then,

\[
\sum_{u \leq x} \frac{1}{p} \sum_{\gcd(n,p-1)=1} \Lambda(u) \gg \frac{x}{\log \log p} \left(1 + O\left(\frac{e^{\gamma} \log \log p}{e^{c_0 \sqrt{\log \log p}}}\right)\right)
\]

for some constant \( c_0 > 0 \).

Proof. The maximal number \( \omega(p-1) \) of prime divisors of highly composite totients \( p-1 \) satisfies \( \omega(p-1) \gg \log p / \log \log p \). This implies that \( z \asymp \log p \). An application of Lemma 3.2 to the ratio returns

\[
\frac{\varphi(p-1)}{p} = \prod_{q \leq z} \left(1 - \frac{1}{q}\right) = \frac{1}{e^{\gamma} \log z} + O\left(e^{-c_0 \sqrt{\log z}}\right)
\]

which implies

\[
\gg \frac{1}{e^{\gamma} \log \log p} + O\left(e^{-c_0 \sqrt{\log \log p}}\right).
\]

In addition, using the prime number theorem in the form

\[
\sum_{n \leq x} \Lambda(n) = x + O\left(x e^{-c_0 \sqrt{\log x}}\right),
\]

the main term reduces to

\[
M(x, \Lambda) = \sum_{u \leq x} \frac{1}{p} \sum_{\gcd(n,p-1)=1} \Lambda(u) = \frac{\varphi(p-1)}{p} \left(x + O\left(x e^{-c_0 \sqrt{\log x}}\right)\right)
\]

\[
\gg \left(\frac{1}{e^{\gamma} \log p} + O\left(e^{-c_0 \sqrt{\log \log p}}\right)\right) \left(x + O\left(x e^{-c_0 \sqrt{\log x}}\right)\right)
\]

\[
\gg \frac{x}{\log \log p} \left(1 + O\left((\log \log p) e^{-c_0 \sqrt{\log \log p}}\right)\right) \left(1 + O\left(e^{-c_0 \sqrt{\log x}}\right)\right)
\]

This proves the claim. 

7.3 Short Intervals For Prime Primitive Root

Lemma 7.3. Let \( p \geq 2 \) be a large prime, and let \( 1 \leq p^{525} < N < p \) be a pair of numbers. Then, for any number \( M < p \),

\[
\sum_{M \leq u \leq M+N} \frac{1}{p} \sum_{\gcd(n,p-1)=1} \Lambda(u) \gg \frac{N}{e^{\gamma} \log \log p} \left(1 + O\left(\frac{e^{\gamma} \log \log p}{e^{c_0 \sqrt{\log \log p}}}\right)\right).
\]

Proof. The maximal number \( \omega(p-1) \) of prime divisors of highly composite totients \( p-1 \) satisfies \( \omega(p-1) \gg \log p / \log \log p \). This implies that \( z \asymp \log p \). An application of Lemma 3.2 to the ratio returns

\[
\frac{\varphi(p-1)}{p} = \prod_{q \leq z} \left(1 - \frac{1}{q}\right) = \frac{1}{e^{\gamma} \log z} + O\left(e^{-c_0 \sqrt{\log z}}\right)
\]

which implies

\[
\gg \frac{1}{e^{\gamma} \log \log p} + O\left(e^{-c_0 \sqrt{\log \log p}}\right).
\]
Let \( x = M \), and \( y = M + N \). Substituting this, the main term reduces to

\[
M(x, y, \Lambda) = \sum_{x \leq u \leq y} \frac{1}{p} \sum_{\gcd(n, p-1) = 1} \Lambda(u)
\]

\[
= \frac{\varphi(p-1)}{p} \sum_{x \leq u \leq y} \Lambda(u)
\]

\[
\gg \left( \frac{1}{e^\gamma \log \log p} + O \left( e^{-c_0 \sqrt{\log \log p}} \right) \right) \sum_{x \leq u \leq y} \Lambda(u).
\] (49)

Applying the prime number theorem in short intervals \( \sum_{x \leq n \leq y} \Lambda(n) \gg y - x = N \), see [5], to the last inequality yields

\[
M(x, y, \Lambda) \gg \left( \frac{1}{e^\gamma \log \log p} + O \left( e^{-c_0 \sqrt{\log \log p}} \right) \right) (y - x) \] (50)

\[
\gg \frac{N}{e^\gamma \log \log p} \left( 1 + O \left( \frac{e^\gamma \log \log p}{e^{c_0 \sqrt{\log \log p}}} \right) \right).
\]

The proves the claim. \[\blacksquare\]

8 **Primitive Roots In Short Intervals**

The previous sections provide sufficient background materials to assemble the proof of the existence of primitive roots in a short interval \([M, M + N]\) for any sufficiently large prime \( p \geq 2 \), a number \( N \gg (\log p)^{1+\varepsilon} \), and the fixed parameters \( M \geq 2 \) and \( \varepsilon > 0 \).

The analysis below indicates that the local minima of the ratio \( \varphi(p-1)/p \) at the highly composite totients \( p - 1 \) are the primary factor determining the size of the short interval.

**Proof.** (Theorem 1.1) Suppose that the short interval \([x, y]\), with \( 1 \leq x < y < p \), does not contain a primitive root modulo a large primes \( p \geq 2 \), and consider the sum of the characteristic function over the short interval, that is,

\[
0 = \sum_{x \leq u \leq y} \Psi(u).
\] (51)

Replacing the characteristic function, Lemma [2.2] and expanding the nonexistence equation (51) yield

\[
0 = \sum_{x \leq u \leq y} \Psi(u)
\]

\[
= \sum_{x \leq u \leq y} \left( \frac{1}{p} \sum_{\gcd(n, p-1) = 1, \ 0 \leq m \leq p-1} \psi((\tau^m - u)m) \right)
\]

\[
= \frac{c_p}{p} \sum_{x \leq u \leq y, \gcd(n, p-1) = 1} \sum_{1}^{p-1} \frac{1}{p} \sum_{x \leq u \leq y, \gcd(n, p-1) = 1, \ 0 < m \leq p-1} \psi((\tau^m - u)m)
\]

\[
= M(x, y) + E(x, y),
\]
where \( c_p \geq 0 \) is a local correction constant depending on the fixed prime \( p \geq 2 \). The main term \( M(x, y) \) is determined by a finite sum over the trivial additive character \( \psi = 1 \), and the error term \( E(x, y) \) is determined by a finite sum over the nontrivial additive characters \( \psi(t) = e^{i2\pi t/p} \neq 1 \).

An application of Lemma 7.1 to the main term, and an application of Lemma 6.1 to the error term yield

\[
\sum_{x \leq u \leq y} \Psi(u) = M(x, y) + E(x, y) \\
\gg \left( \frac{1}{e^\gamma \log \log p} + O \left( e^{-c_0 \sqrt{\log \log p}} \right) \right) (y - x) + O \left( \frac{y - x}{p^\varepsilon} \right) \\
\gg \frac{y - x}{\log \log p} \left( 1 + O \left( \frac{e^\gamma \log \log p}{e^{c_0 \sqrt{\log \log p}}} \right) \right)
\]

where the implied constant \( d_p = e^{-\gamma} a_p c_p \geq 0 \) depends on local information and the fixed prime \( p \geq 2 \). However, a short interval \([x, y]\) of length \( y - x = N \gg (\log p)^{1+\varepsilon} > 0\) contradicts the hypothesis (51) for all sufficiently large primes \( p \geq 2 \). Ergo, the short interval \([M, M + N]\) contains a primitive root for any sufficiently large prime \( p \geq 2 \) and the fixed parameters \( M \geq 2 \) and \( \varepsilon > 0 \).

**9 Least Prime Primitive Roots**

A modified version of the previous result demonstrate the existence of prime primitive roots in an interval \([2, x]\) for any sufficiently large prime \( p \geq 2 \). The analysis below indicates that the local minima of the ratio \( \varphi(p - 1)/p \) at the highly composite totients \( p - 1 \), and the number of primes \( \sum_{p \leq x} \Lambda(n) \) are the primary factors determining the size of the interval \([2, x]\).

**Proof.** (Theorem 1.2) Suppose that the interval \([2, x]\), with \( 1 \leq x < p \), does not contain a prime primitive root modulo a large primes \( p \geq 2 \), and consider the sum of the weighted characteristic function over the integers \( u \leq x \), that is,

\[
0 = \sum_{u \leq x} \Psi(u) \Lambda(u). \tag{53}
\]

Replacing the characteristic function, Lemma 2.2, and expanding the nonexistence equation (51) yield

\[
0 = \sum_{u \leq x} \Psi(u) \Lambda(u) \\
= \sum_{u \leq x} \left( \frac{1}{p} \sum_{\gcd(n, p-1) = 1, 0 \leq m \leq p-1} \psi \left( (\tau^n - u)m \right) \right) \Lambda(u) \\
= \frac{c_p}{p} \sum_{u \leq x} \Lambda(u) \sum_{\gcd(n, p-1) = 1} 1 + \frac{1}{p} \sum_{u \leq x} \Lambda(u) \sum_{\gcd(n, p-1) = 1, 0 < m \leq p-1} \psi \left( (\tau^n - u)m \right) \\
= M(x, \Lambda) + E(x, \Lambda),
\]
where \( c_p \geq 0 \) is a local correction constant depending on the fixed prime \( p \geq 2 \). The main term \( M(x, \Lambda) \) is determined by a finite sum over the trivial additive character \( \psi = 1 \), and the error term \( E(x, \Lambda) \) is determined by a finite sum over the nontrivial additive characters \( \psi(t) = e^{i2\pi t/p} \neq 1 \).

An application of Lemma 7.2 to the main term, and an application of Lemma 6.2 to the error term yield

\[
\sum_{u \leq y} \Psi(u)\Lambda(u) = M(x, \Lambda) + E(x, \Lambda) \\
\gg \frac{x}{\log \log p} \left( 1 + O \left( \frac{\log \log p e^c_0 \sqrt{\log \log p}}{1 + O(e^c_0 \log \log p)} \right) \right)
\]

where the implied constant \( d_p = e^{-c_p}a_pc_p \geq 0 \) depends on local information and the fixed prime \( p \geq 2 \). But, an interval \([2, x]\) of length \( x - 2 \gg (\log p)^{2+\varepsilon} > 0 \) contradicts the hypothesis (53) for all sufficiently large primes \( p \geq 2 \). Ergo, the short interval \([2, x]\) contains a prime primitive root for any sufficiently large prime \( p \geq 2 \) and a fixed parameter \( \varepsilon > 0 \).

\section{Prime Primitive Roots In Short Intervals}

The prime number theorem in short intervals \( \sum_{M \leq n \leq M+N} \Lambda(n) \gg N \), see [5]. A modified version of the previous result will prove the existence of prime primitive roots in short interval \([M, M+N]\) for any sufficiently large prime \( p \geq 2 \), \( N \gg p^{2+\varepsilon} \) and any \( M < p \). The analysis below indicates that the number of primes \( \sum_{M \leq n \leq M+N} \Lambda(n) \) in a short interval \([M, M+N]\) is the primary factor determining the size of the interval \( N \). The local minima of the ratio \( \varphi(p-1)/p \) at the highly composite totients \( p-1 \) have a minor impact on the analysis.

\textbf{Proof.} (Theorem 1.3) Suppose that the interval \([2, x]\), with \( 1 \leq x < p \), does not contain a prime primitive root modulo a large primes \( p \geq 2 \), and consider the sum of the weighted characteristic function over the integers \( u \leq x \), that is,

\[
0 = \sum_{M \leq u \leq M+N} \Psi(u)\Lambda(u).
\]

Replacing the characteristic function, Lemma 2.2 and expanding the nonexistence equation 51 yield
0 = \sum_{M \leq u \leq M+N} \Psi(u)\Lambda(u) \\
= \sum_{M \leq u \leq M+N} \left( \frac{1}{p} \sum_{\text{gcd}(n,p-1)=1, 0 \leq m \leq p-1} \psi((\tau^n - u)m) \right) \Lambda(u) \\
= \frac{c_p}{p} \sum_{M \leq u \leq M+N} \Lambda(u) \sum_{\text{gcd}(n,p-1)=1} 1 + \frac{1}{p} \sum_{M \leq u \leq M+N} \Lambda(u) \sum_{\text{gcd}(n,p-1)=1, 0 \leq m \leq p-1} \psi((\tau^n - u)m) \\
= M(N, \Lambda) + E(N, \Lambda),

where \( c_p \geq 0 \) is a local correction constant depending on the fixed prime \( p \geq 2 \). The main term \( M(N, \Lambda) \) is determined by a finite sum over the trivial additive character \( \psi = 1 \), and the error term \( E(N, \Lambda) \) is determined by a finite sum over the nontrivial additive characters \( \psi(t) = e^{i2\pi t/p} \neq 1 \).

An application of Lemma 11.3 to the main term, and an application of Lemma 6.2 to the error term yield

\[ \sum_{M \leq u \leq M+N} \Psi(u)\Lambda(u) = M(N, \Lambda) + E(N, \Lambda) \]

\[ \gg \frac{N}{\log \log p} \left( 1 + O \left( (\log \log p)e^{-c\sqrt{\log \log p}} \right) \right) + O \left( \frac{x}{p^2} \right) \]

\[ \gg \frac{N}{\log \log p} \left( 1 + O \left( \frac{e^\gamma \log \log p}{e^{c \sqrt{\log \log p}}} \right) \right) \]

\[ > 0, \]

where the implied constant \( d_p = e^{-\gamma}a_p c_p \geq 0 \) depends on local information and the fixed prime \( p \geq 2 \). But, an interval \([M, M+N]\) of length \( N \gg p^{525} > 0 \) contradicts the hypothesis \( \lbrack 43 \rbrack \) for all sufficiently large primes \( p \geq 2 \). Ergo, the short interval \([M, M+N]\) contains a prime primitive root for any sufficiently large prime \( p \geq 2 \) and a fixed parameter \( M \geq 0 \).

\[ \]
Exercise 11.4. Estimate the number of highly composite totients $p-1$ in a short interval, that is,

$$\sum_{x \leq p \leq x+y} 1, \quad \omega(p-1) \gg \log p / \log \log p$$

where $x \geq 1$ is a large number, and $1 < y < x$.

References

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

[2] Burgess, D. A. Character sums and primitive roots in finite fields. Proc. London Math. Soc. (3) 17 1967 11-25.

[3] Bach, Eric; Huelsbergen, Lorenz. Statistical evidence for small generating sets. Math. Comp. 61 (1993), no. 203, 69-82.

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

[5] Baker, R. C.; Harman, G.; Pintz, J. The difference between consecutive primes. II. Proc. London Math. Soc. (3) 83 (2001), no. 3, 532-562.

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

[7] Carlitz, L. Primitive roots in a finite field. Trans. Amer. Math. Soc. 73, (1952). 373-382.

[8] Carlitz, L. Distribution of primitive roots in a finite field. Quart. J. Math., Oxford Ser. (2) 4, (1953). 4-10.

[9] N. A. Carella, Least Prime Primitive Roots, arXiv:1709.01172.

[10] Stephen D. Cohen, Tomas Oliveira e Silva, Tim Trudgian. On Grosswald’s conjecture on primitive roots, arXiv:1503.04519.

[11] Cobeli, Cristian; Zaharescu, Alexandru. On the distribution of primitive roots mod $p$. Acta Arith. 83, (1998), no. 2, 143-153.

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

[13] H. G. Diamond and J. Pintz. Oscillation of Mertens product formula. J. Theor. Nombres Bordeaux 21 (2009), no. 3, 523-533.

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

[15] Ellison, William; Ellison, Fern. Prime numbers. Wiley-Interscience Publication. New York; Hermann, Paris, 1985.

[16] Paul Erdős, Harold N. Shapiro. On The Least Primitive Root Of A Prime, 1957, euclidproject.org.
17 Friedlander, John B.; Konyagin, Sergei; Shparlinski, Igor E. Some doubly exponential sums over $\mathbb{Z}_m$. Acta Arith. 105, (2002), no. 4, 349-370.

18 Friedlander, John B.; Shparlinski, Igor E. Double exponential sums over thin sets. Proc. Amer. Math. Soc. 129 (2001), no. 6, 1617-1621.

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

20 Goldfeld, Morris. Artin conjecture on the average. Mathematika 15, 1968, 223-226.

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

22 Garaev, M. Z. A. A. Karatsuba. New estimates of double trigonometric sums with exponential functions, \texttt{arXiv:math/0504026}.

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

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

25 Alessandro, Languasco, Alessandro, Zaccagnini. On the constant in the Mertens product for arithmetic progressions. I., \texttt{arXiv:0706.2807}.

26 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.

27 Moree, Pieter. Artin’s primitive root conjecture -a survey. \texttt{arXiv:math/0412262}.

28 Moree, P. Artin prime producing quadratics. Abh. Math. Sem. Univ. Hamburg 77 (2007), 109-127.

29 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.

30 Kevin McGown, Enrique Trevino, Tim Trudgian, Resolving Grosswald’s conjecture on GRH, \texttt{arXiv:1508.05182}.

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

32 Jean-Louis Nicolas. Small values of the Euler function and the Riemann hypothesis, \texttt{arXiv:1202.0729}, or Acta Arithmetica, 155.3, 2012, 311-321.

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

34 Pappalardi, Francesco; Shparlinski, Igor. On Artin’s conjecture over function fields. Finite Fields Appl. 1 (1995), no. 4, 399-404.

35 Perelmuter, G. I.; Shparlinski, I. E. Distribution of primitive roots in finite fields. Uspekhi Mat. Nauk 45 (1990), no. 1(271), 185–186; translation in Surveys 45 (1990), no. 1, 223-224.
[36] Ribenboim, Paulo. The new book of prime number records, Berlin, New York: Springer-Verlag, 1996.

[37] J.B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, Illinois J. Math. 6 (1962) 64-94.

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

[39] 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.

[40] Shoup, Victor Searching for primitive roots in finite fields. Math. Comp. 58 (1992), no. 197, 369-380.

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

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