Configurations Of Consecutive Primitive Roots

N. A. Carella

***Abstract*:** Let $p \geq 2$ be a large prime, and let $k \ll \log p$ be a small integer. This note proves the existence of various configurations of $(k+1)$-tuples of consecutive and quasi consecutive primitive roots $n+a_0, n+a_1, n+a_2, \ldots, n+a_k$ in the finite field $\mathbb{F}_p$, where $a_0, a_1, \ldots, a_k$ is a fixed $(k+1)$-tuples of distinct integers.

Contents

October 8, 2019
Mathematics Subject Classifications: Primary 11A07, Secondary 11N37.
Keywords: Primitive root; Consecutive primitive root; Consecutive squarefree primitive root; Relative prime primitive root.

1 Introduction

Let $p \geq 2$ be a large prime, and let $\mathbb{F}_p$ be a finite field. The order $\operatorname{ord}_p \alpha = d$ of an element $\alpha \in \mathbb{F}_p$ is the smallest divisor $d \mid p-1$ for which $\alpha^d \equiv 1 \bmod p$. An element of maximal order $\operatorname{ord}_p(\alpha) = p-1$ is called a primitive root. This note is concerned with the configurations of subsets of primitive roots in finite fields. A configuration deals with the existence of $(k+1)$-tuples of quasi consecutive primitive roots

$$n + a_0, \quad n + a_1, \quad n + a_2, \quad \ldots, \quad n + a_k, \tag{1}$$

where $a_0, a_1, \ldots, a_k$ is a fixed $(k+1)$-tuples of distinct integers, in a finite field $\mathbb{F}_p$, or in large subsets $\mathcal{A} \subset \mathbb{F}_p$. The corresponding counting functions have the forms

$$\sum_{n \in \mathbb{F}_p} \Psi(n+a_0)\, \Psi(n+a_1) \cdots \Psi(n+a_k)\, f(n+a_0)\, f(n+a_1) \cdots f(n+a_k), \tag{2}$$

and

$$\sum_{n \in \mathcal{A}} \Psi(n+a_0)\, \Psi(n+a_1) \cdots \Psi(n+a_k)\, f(n+a_0)\, f(n+a_1) \cdots f(n+a_k), \tag{3}$$

respectively, where $\Psi : \mathbb{N} \longrightarrow \{0, 1\}$ is the characteristic function of primitive roots modulo p, see Section 9, and $f : \mathbb{N} \longrightarrow \mathbb{Z}$ is an arithmetic function. The function f restricts the sequence of $(k+1)$-tuples of quasi consecutive primitive roots to certain subsequence of integers. There are many possible classes of clusters and constellations of primitive roots generated by the different classes of $(k+1)$-tuples. The precise results for some of the various restricted $(k+1)$-tuples of configurations of quasi consecutive primitive roots are detailed below.

1.1 Consecutive Primitive Roots

The earliest works on consecutive primitive roots seems to be that in [6] or before. The author proved a general result for the existence of consecutive primitive roots. The proof is based on the divisors dependent characteristic function for primitive roots, see Lemma 9.1. Later, a qualitative result for the existence of some consecutive primitive roots was proved in [56]. A quantitative and weaker result for two consecutive primitive roots is proved in [50], the same result, but emphasizing the numerical aspects, is also proved in [10]. More recently, some partial result but no proof for k-consecutive primitive roots appears in [55].

Theorem 1.1. *Let $p \geq 2$ be a large prime, and let $k \ll \log p$ be an integer. Then, the finite field $\mathbb{F}_p$ contains $(k+1)$-tuples of consecutive primitive roots. Furthermore, the number of $(k+1)$-tuples has the asymptotic formula*

$$N(k, p) = \left(\frac{\varphi(p-1)}{p-1} \right)^{k+1} p + O(p^{1-\varepsilon}), \tag{4}$$

where $\varepsilon > 0$ is an arbitrary small number.

The complete proof for this case is given in Section 15.

Theorem 1.2. *Let $p \geq 2$ be a large prime, and let $k \ll \log p$ be an integer. Then, any large subset of elements $\mathcal{A} \subset \mathbb{F}_p$ of cardinality $p^{1-\varepsilon/2} \ll \#\mathcal{A}$ contains $(k+1)$-tuples of consecutive primitive roots. Furthermore, the number of $(k+1)$-tuples has the asymptotic formula*

$$N(k, p, \mathcal{A}) = \left(\frac{\varphi(p-1)}{p-1} \right)^{k+1} \#\mathcal{A} + O(p^{1-\varepsilon}), \tag{5}$$

where $\varepsilon > 0$ is an arbitrary small number.

The average length of $(k+1)$-tuples is $k \ll \log p / \log \log \log p$. This statistic is dependent on the primes decomposition of the average totient $p-1$. Asymptotically, highly composite totients $p-1$ have slightly shorter lengths $k \ll \log p / \log \log p$. The Fermat and Germain totients have the longest lengths, namely, $k \ll \log p$, the details appears in Lemma 14.1. The distribution of $(k+1)$-tuples of consecutive primitive roots is a very interesting research problem. The numerical data is not adequate to make any strong heuristic, but it suggests that the $(k+1)$-tuples of consecutive primitive roots are not uniformly distributed.

1.2 Consecutive Squarefree Primitive Roots

The result for a single squarefree primitive root n in a finite field $\mathbb{F}_p$, which is a special case of Theorem 1.4, is proved in Theorem 17.1. A result for two consecutive squarefree primitive roots n and $n+1$ in a finite field $\mathbb{F}_p$ is given in Theorem 17.2 and a result for three consecutive squarefree primitive roots n, $n+1$ and $n+2$ is given in Theorem 17.3. The next case for four squarefree primitive roots n, $n+1$, $n+2$ and $n+3$ is not feasible, see (15). However, there are other sequences of integers that support long strings of quasi consecutive squarefree primitive roots.

Theorem 1.3. *Let $p \geq 2$ be a large prime, and let $k \ll \log p$ be an integer. For any admissible $(k+1)$-tuples $a_0 < a_1 < \cdots < a_k$, the finite field $\mathbb{F}_p$ contains $(k+1)$-tuples of consecutive squarefree primitive roots*

$$n+a_0, \quad n+a_1, \quad n+a_2, \quad \ldots, \quad n+a_k. \tag{6}$$

Furthermore, the number of $(k+1)$-tuples has the asymptotic formula

$$N(k,p) = \prod_{q \geq 2}\left(1 - \frac{\omega(q)}{q^2}\right)\left(\frac{\varphi(p-1)}{p-1}\right)^{k+1} p + O(p^{1-\varepsilon}), \tag{7}$$

where $\varepsilon > 0$ is an arbitrary small number.

The complete proof for this case is given in Section 17.

1.3 Consecutive s-Power Free Primitive Roots

Let $s \geq 2$ be a small integer. A primitive root $n \in \mathbb{F}_p$ is s-power free if and only if it is not divisible by an s-power, exempli gratia, $r^s \nmid n$ for all prime $r \geq 2$. This idea generalizes the idea of squarefree primitive roots.

Theorem 1.4. *Let $p \geq 2$ be a large prime, and let $s \geq 2$ be a small integer. Then, the finite field $\mathbb{F}_p$ contains s-power free primitive roots. Furthermore, the number of such elements has the asymptotic formula*

$$N_s(p) = \frac{1}{\zeta(s)}\frac{\varphi(p-1)}{p-1}p + O(p^{1-\varepsilon}), \tag{8}$$

where $\zeta(s)$ is the zeta function, and $\varepsilon > 0$ is an arbitrary small number.

Theorem 1.5. *Let $p \geq 2$ be a large prime, and let $a_0 \neq a_1$ and $s \geq 2$ be small integers. Then, the finite field $\mathbb{F}_p$ contains a pair of consecutive s-power free primitive roots $n+a_0$ and $n+a_1$. Furthermore, the number of such pairs has the asymptotic formula*

$$N_s(2,p) = \prod_{q \geq 2}\left(1 - \frac{\rho(q)}{q^s}\right)\left(\frac{\varphi(p-1)}{p-1}\right)^{2} p + O(p^{1-\varepsilon}), \tag{9}$$

where $\rho(s) = 1, 2$, and $\varepsilon > 0$ is an arbitrary small number.

The complete proofs for these cases are given in Section 18.

1.4 Consecutive Primitive Roots And Relatively Prime

The earliest work considered the existence of primitive roots relatively prime to $p-1$. In other words, the case $q = p-1$ was proved in [27] using the divisors dependent characteristic function in Lemma 9.1. A generalized version for $q \leq p-1$, using the divisors free characteristic function in Lemma 9.2, is realized in Theorem 1.6. In addition, for $a \geq 1$, a result for two consecutive primitive roots n, $n+a$, and relative prime to $q = q(a)$ is proved in Theorem 1.7. Both of these results are appear to be new in the literature.

Theorem 1.6. *Let $p \geq 2$ be a large prime, and let $q < p$ be an integer. Then, the finite field $\mathbb{F}_p$ contains primitive roots relatively prime to q. Furthermore, the number of such elements has the asymptotic formula*

$$N_r(p,q) = \frac{\varphi(q)}{q}\frac{\varphi(p-1)}{p-1}p + O(p^{1-\varepsilon}), \tag{10}$$

where $\varepsilon > 0$ is an arbitrary small number.

Theorem 1.7. *Let $p \geq 2$ be a large prime, let $q < p$ be an integer, and let $a \geq 1$ be a fixed integer. Then, the finite field $\mathbb{F}_p$ contains a pair of quasi consecutive primitive roots n, $n+a$, relatively prime to $q = q(a)$. Furthermore, the number of such pairs has the asymptotic formula*

$$N_r(2,p,q) = c_2(q,a) \left(\frac{\varphi(q)}{q} \right)^2 \frac{\varphi(p-1)}{p-1} p + O(p^{1-\varepsilon}), \tag{11}$$

where $c_2(q,a) \geq 0$ is a dependence correction factor, and $\varepsilon > 0$ is an arbitrary small number.

Both parameters $c_2(q,a) \geq 0$ and $q = q(a)$ depend on $a \geq 1$. For instance, for $a = 2b+1$ odd, the value $q = q(a)$ must be odd, and $c_2(q,a) > 0$, otherwise $c_2(q,a) = 0$ for even q. The complete proof for both of these cases are given in Section 19.

2 Results For Arithmetic Functions

Several results for some arithmetic functions required in later sections are recorded here.

2.1 Prime Divisors Counting Function

Let $p_i \geq 2$ denotes the ith prime in increasing order, and let $n \in \mathbb{N}$ be an integer. An integer has a unique prime decomposition $n = p_1^{v_1} \cdot p_2^{v_2} \cdots p_t^{v_t}$, where $v_i \geq 1$.

Definition 2.1. The prime divisors counting function $\omega : \mathbb{N} \longrightarrow \mathbb{N}$ is defined by $\omega(n) = t$.

The number of prime divisors $\omega(n)$ of a random integer $n \in \mathbb{N}$ is a normal random variable with mean $\log\log n$, and standard error $\sqrt{\log\log n}$, as verified below.

Theorem 2.1. *Let $x \geq 1$ be a large number, and $a \leq q = o(\log x)$ be a pair of integers. Then, $\omega(n)$ has the followings average orders in an arithmetic progression.*

(i) $$\sum_{\substack{n \leq x \\ n \equiv a \bmod q}} \omega(n) = \frac{1}{\varphi(q)} x \log\log x + x\beta(q,a) + O\left(\frac{x}{\log x} \right),$$

(ii) $$\sum_{\substack{n \leq x \\ n \equiv a \bmod q}} (\omega(n) - \log\log n)^2 \leq \frac{C(q,a)}{\varphi(q)} x \log\log x,$$

where $\beta(q,a) \neq 0$ and $C(q,a)$ are constants.

Proof. (i) Let $\{x\} \in (0,1)$ be the fractional function. The finite sum $\sum_{k \leq x/p} 1$ tallies the number of integers $n \leq x$ divisible by a prime $p \leq x$. Thus,

$$\begin{aligned} \sum_{\substack{n \leq x \\ n \equiv a \bmod q}} \omega(n) &= \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \sum_{k \leq x/p} 1 \\ &= x \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \frac{1}{p} - \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \left\{ \frac{x}{p} \right\}. \end{aligned} \tag{12}$$

Apply Mertens theorem in arithmetic progression to the first finite sum, and estimate the second finite sum to obtain this:

$$\sum_{\substack{n \leq x \\ n \equiv a \bmod q}} \omega(n) = x \left(\frac{1}{\varphi(q)} \log\log x + \beta(q,a) + O\left(\frac{1}{\log x} \right) \right) + O\left(\frac{x}{\varphi(q) \log x} \right), \tag{13}$$

where $\beta(q,a) \neq 0$ is a constant. ∎

Observe that there are a few versions of Mertens theorem in arithmetic progression, see [13, Theorem 15.4], [32], et alii. The basic case $q = 2$ of Theorem 2.1 is proved in [13, Theorem 7.2], [43, Proposition 2.6], et cetera. The more general concept of the Erdos-Kac theorem provides finer details on the distribution of the random variable $\omega(n) \in \mathbb{N}$.

Lemma 2.1. *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. (i) Set $a = 1$ and $q = 2$ in Theorem 2.1-i. (ii) Set $n = \prod_{p \leq x} p$, and employ routine calculations. ■

Both of these results are standard results in analytic number theory, see [40, Theorem 2.6].

2.2 Mobius Function

Definition 2.2. The Mobius function $\mu : \mathbb{N} \longrightarrow \{-1, 0, 1\}$ is defined by

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & n = p_1 p_2 \cdots p_v \\ 0 & n \neq p_1 p_2 \cdots p_v, \end{cases} \tag{14}$$

where the $p_i \geq 2$ are primes.

The function μ is quasiperiodic. It has a period of 4, that is, $\mu(4) = \cdots = \mu(4m) = 0$ for any integer $m \in \mathbb{Z}$. But, its interperiods values are pseudorandom, that is, the values

$$\mu(n), \quad \mu(n+4), \quad \cdots, \quad \mu(n+4m) \tag{15}$$

are not periodic as $n \to \infty$.

Definition 2.3. An integer $n \in \mathbb{N}$ is said to be s-power free if for each prime $p \mid n$, the maximal prime power divisor is $p^{s-1} \mid\mid n$. Equivalently, the *p-adic* valuation $v_p(n) = s - 1$ for any $s \geq 2$.

The 2-free integers are usually called squarefree integers.

Definition 2.4. The characteristic function for s-power free integers is defined by

$$\mu_s(n) = \begin{cases} 1 & \text{if } p^s \nmid n \text{ for any prime } p \mid n, \\ 0 & \text{if } p^s \mid n \text{ for any prime } p \mid n. \end{cases} \tag{16}$$

The characteristic function for s-power free integers is closely linked to the Mobius function.

Lemma 2.2. *For any integer $n \geq 1$, the characteristic function for squarefree integers has the expansion*

$$\mu(n)^2 = \sum_{d^2 \mid n} \mu(d). \tag{17}$$

More generally, the characteristic function for s-power free integers has the expansion

$$\mu_s(n) = \sum_{d^s \mid n} \mu(d). \tag{18}$$

The case $s = 2$ for squarefree integers is usually denoted by $\mu^2(n) = \mu_2(n)$. Some early works on this topic appear in [7] and [36].

Definition 2.5. A pair of integers a and q are relatively prime if and only if $\gcd(a,q)=1$. The characteristic function for relatively prime integers is defined by

$$\sum_{\substack{d\mid a\\ d\mid q}}\mu(d)=\begin{cases}1 & \text{if and only if } \gcd(a,q)=1,\\ 0 & \text{if and only if } \gcd(a,q)\neq 1.\end{cases} \tag{19}$$

Lemma 2.3. *Let $n\geq 1$ be an integer. Then,*

(i) $\displaystyle\sum_{d\mid n}\mu(n)=\begin{cases}1 & \text{if } n=1,\\ 0 & \text{if } n\neq 1.\end{cases}$

(ii) $\displaystyle\sum_{d\mid n}\mu^2(n)=2^{\omega(n)}$.

2.3 Extreme Values Of The Totient Function

Some estimates for the extreme values of the Euler totient function are stated in this subsection. The Euler totient function counts the number of relatively prime integers $\varphi(n)=\#\{k:\gcd(k,n)=1\}$. For each $n\in\mathbb{N}$, this counting function is compactly expressed by the analytic formula

$$\varphi(n)=n\sum_{d\mid n}\frac{\mu(d)}{d}=n\prod_{p\mid n}\left(1-\frac{1}{p}\right). \tag{20}$$

The explicit lower bound

$$\frac{\varphi(n)}{n}>\frac{1}{e^{\gamma}\log\log n+5/(2\log\log n)} \tag{21}$$

and other estimates are given in [48, Theorem 7]. The maximal values of the Euler function occurs at the prime arguments. Id est, $\varphi(p)=p-1<p$. There are other subsets of integers that have nearly maximal values. In fact, asymptotically, these integers and the primes number have the same order of magnitudes.

Lemma 2.4. *Let $x\geq 1$ be a large number, and let $n=1+\prod_{p\leq\log x}p$. Then*

(i) $\varphi(n)=n+O\left(n/\log\log n\right)$,

(ii) $\varphi(n+1)=n/2+O\left(n/\log n\right)$.

Proof. (i) Observe that $\log n\geq\sum_{p\leq\log x}\log p$, so that $p\leq\log x\leq 2\log n$. Hence, a prime divisor $q\mid n=1+\prod_{p\leq\log x}p$ implies that $q>\log n$. Consequently, there is the upper bound

$$\begin{aligned}\varphi(n) &= n\prod_{p\mid n}\left(1-\frac{1}{p}\right) \\ &\leq n\left(1-\frac{1}{\log n}\right) \\ &= n+O\left(\frac{1}{\log n}\right).\end{aligned} \tag{22}$$

In the other direction, there is the lower bound

$$\begin{aligned}\varphi(n) &= n\prod_{p\mid n}\left(1-\frac{1}{p}\right) \\ &\geq n\prod_{\log n<p\leq 2\log n}\left(1-\frac{1}{p}\right) \\ &= n+O\left(\frac{n}{\log\log n}\right).\end{aligned} \tag{23}$$

Both relations (22) and (23) confirm the claim. (ii) The prime divisors of $n+1$ are $q=2$ and some prime $q>\log n$, so the claim follows from

$$\varphi(n+1)=(n+1)\prod_{p\mid(n+1)}\left(1-\frac{1}{p}\right)\leq\frac{n}{2}\left(1-\frac{1}{\log n}\right)=\frac{n}{2}+O\left(\frac{n}{\log n}\right). \tag{24}$$

■

Theorem 2.2. *Let $p\geq 2$ be a large prime. Then, the followings extreme values hold.*

(i) $\dfrac{\varphi(n)}{n}\leq n-1,$ *if $n\geq 2$ is an integer.*

(ii) $\dfrac{\varphi(n)}{n}\geq\dfrac{e^{-\gamma}}{4\log\log n},$ *if $n\geq 2$ is a highly composite integer.*

(iii) $\dfrac{\varphi(n)}{n}\approx\dfrac{e^{-\gamma}}{\log\log\log n},$ *if $n\geq 2$ is an average integer.*

The totient function have a wide range of values, as confirmed by Lemma 2.4, and this accounts for the wide range and large gaps in the sequence of totient gaps

$$\varphi(2)-\varphi(1),\ \ \varphi(3)-\varphi(2),\ \ \varphi(4)-\varphi(3),\ \ \ldots,\ \ \varphi(n+1)-\varphi(n),\ \ \ldots. \tag{25}$$

The gap can be as small as $\varphi(n+1)-\varphi(n)=0$, and it can be as large as $\varphi(n+1)-\varphi(n)=n/2+O\left(n/\log n\right)$. For example, $\varphi(4)-\varphi(3)=0$, and $\varphi(2\cdot3\cdot5+1)-\varphi(2\cdot3\cdot5+2)=14$.

3 Summatory Functions For Squarefree Integers

The subset of 2-power free integers are usually called squarefree integers, and denoted by

$$\mathcal{Q}_2=\{n\in\mathbb{Z}:\mu^2(n)\neq 0\} \tag{26}$$

and the complementary subset of non squarefree integers is denoted by

$$\overline{\mathcal{Q}_2}=\{n\in\mathbb{Z}:\mu^2(n)=0\}. \tag{27}$$

The number of squarefree integers have the following asymptotic formulas.

Lemma 3.1. *Let $\mu:\mathbb{Z}\longrightarrow\{-1,0,1\}$ be the Mobius function. Then, for any sufficiently large number $x\geq 1$,*

$$\sum_{n\leq x}\mu^2(n)=\frac{6}{\pi^2}x+O\left(x^{1/2}\right). \tag{28}$$

Proof. Use Lemma 2.2 or confer to the literature. ■

The constant coincides with the density of squarefree integers. Its approximate numerical value is

$$\frac{6}{\pi^2}=\prod_{q\geq 2}\left(1-\frac{1}{q^2}\right)=0.607988295164627617135754\ldots, \tag{29}$$

where $q\geq 2$ ranges over the primes. The remainder term

$$R(x)=\sum_{n\leq x}\mu^2(n)-\frac{6}{\pi^2}x \tag{30}$$

is a topic of current research, its optimum value is expected to satisfies the upper bound $R(x)=O(x^{1/4+\varepsilon})$ for any small number $\varepsilon>0$. Currently, $R(x)=O\left(x^{1/2}e^{-\sqrt{\log x}}\right)$ is the best unconditional remainder term.

Lemma 3.2. *Let $\mu(n)$ be the Mobius function. Then, for any sufficiently large number $x \geq 1$,*

$$\sum_{n \leq x} \mu^2(n) = \frac{6}{\pi^2} x + \Omega\left(x^{1/4}\right). \tag{31}$$

Proof. The generating series for squarefree integers is $\zeta(s)/\zeta(2s) = \sum_{n \geq 1} \mu^2(n) n^{-s}$ at $s = 2$. The Perron intergral yields

$$\sum_{n \leq x} \mu^2(n) = \frac{1}{i2\pi} \int_{c-\infty}^{c+\infty} \frac{\zeta(s)}{\zeta(s)} \frac{x^s}{s} ds = \frac{1}{\zeta(2)} x + \sum_{\zeta(\rho)=0} c_\rho x^{\rho/2}, \tag{32}$$

where $c \neq 0$ is a constant. The coefficients c_ρ are indexed by the zeros $\rho \in \mathbb{C}$ of the zeta function $\zeta(s)$. Since the zeta function has a zero $\rho_0 = 1/2 + i14.134725\ldots$, the claim follows. ■

Theorem 3.1. *Let $x \geq 1$ be a large number, let a and q be a pair of integers, $1 \leq a < q = O(\log^c x)$, with $c \geq 0$ constant, and let $\mu : \mathbb{Z} \longrightarrow \{-1, 0, 1\}$ be the Mobius function. Then,*

$$\sum_{\substack{n \leq x \\ n \equiv a \bmod q}} \mu(n)^2 = \frac{6}{\pi^2} \prod_{p \mid q} \left(1 - \frac{1}{p^2}\right)^{-1} \frac{x}{q} + O\left(\frac{x}{q} + q^{1/2+\varepsilon}\right), \tag{33}$$

where $\varepsilon > 0$ is an arbitrary small number.

Proof. Consult [25], [58], and the literature. ■

The range of moduli $q \leq x^{2/3}$ is discussed and improved to $q \leq x^{1-\varepsilon}$ in [41]. The q-dependence in the constant

$$\frac{1}{q} \sum_{\substack{n \geq 1 \\ \gcd(n,q)=1}} \frac{\mu(n)}{n^2} = \frac{1}{q} \prod_{p \nmid q} \left(1 - \frac{1}{p^2}\right) = \frac{6}{\pi^2} \frac{1}{q} \prod_{p \mid q} \left(1 - \frac{1}{p^2}\right)^{-1} \tag{34}$$

propagates the dependence in the asymptotic formula for consecutive s-power free integers. For example, the probability or density of two consecutive squarefree integers is not $\left(6/\pi^2\right)^2$, but a more complicated expression similar to (34). The equidistribution of s-power free integers in arithmetic progressions is affirmed by the result below. This also indicates a level of distribution of $2/3$ over any arithmetic progression $\{n = qm + a : m \geq 1\}$.

Theorem 3.2. *Let $x \geq 1$ be a large number, let a and q be a pair of integers, $1 \leq a < q = O(\log^c x)$, with $c \geq 0$ constant, and let $\mu : \mathbb{Z} \longrightarrow \{-1, 0, 1\}$ be the Mobius function. Then,*

$$\sum_{q \leq x^{2/3} \log^{-c-1} x} \max_{a \bmod q} \left| \sum_{\substack{n \leq x \\ n \equiv a \bmod q}} \mu(n)^2 - \frac{\varphi(q)}{d\varphi(q/d)} \prod_{p \nmid q} \left(1 - \frac{1}{p^2}\right) \frac{x}{q} \right| \ll \frac{x}{\log^c x}, \tag{35}$$

where $d = \gcd(a, q)$ and $c > 0$ is an arbitrary constant.

Proof. Consult [46] and the literature. ■

Lemma 3.3. *Let $x \geq 1$ be a large number, and let $\mu : \mathbb{Z} \longrightarrow \{-1, 0, 1\}$ be the Mobius function. If $q = O(\log^c x)$ with $c \leq 0$ constant, then,*

$$\sum_{\substack{n \leq x \\ \gcd(n,q)=1}} \mu^2(n) = \frac{6}{\pi^2} \prod_{p \nmid q} \left(1 + \frac{1}{p}\right)^{-1} x + O\left(x^{1/2}\right). \tag{36}$$

Proof. The proof is lengthier and more difficult than Lemma 3.1, see [14, Lemma 2]. ■

4 Correlation Functions For Squarefree Integers

A sequence of squarefree integers

$$n + a_0, \quad n + a_1, \quad n + a_2, \quad \ldots, \quad n + a_k, \tag{37}$$

imposes certain restriction on the $(k + 1)$-tuple $(a_0, a_1, \ldots, a_k)$. A stronger restriction is required for sequence of prime $(k + 1)$-tuples , see [2], and the literature for extensive details.

Definition 4.1. A k-tuple $(a_0, a_1, \ldots, a_k)$ is called *admissible* if the numbers $a_0, a_1, \ldots, a_k$ is not a complete residues system modulo p for any prime $p \leq k$.

Lemma 4.1. *Let $x \geq 1$ be a large number, and let $\mu : \mathbb{Z} \longrightarrow \{-1, 0, 1\}$ be the Mobius function. Then,*

$$\sum_{n \leq x} \mu(n)^2 \mu(n + 1)^2 = \prod_{p \geq 2} \left(1 - \frac{2}{p^2}\right) x + O\left(x^{2/3}\right). \tag{38}$$

Proof. The earliest proof seems to be that in [7], and [36]. Recent proofs appear in [35], and the literature. ∎

The constant coincides with the density of 2-consecutive squarefree integers. Its approximate numerical value is

$$\prod_{q \geq 2} \left(1 - \frac{2}{q^2}\right) = 0.3226990542425355761614 83\ldots, \tag{39}$$

where $q \geq 2$ ranges over the primes.

Lemma 4.2. *Let $x \geq 1$ be a large number, and let $\mu : \mathbb{Z} \longrightarrow \{-1, 0, 1\}$ be the Mobius function. Then,*

$$\sum_{n \leq x} \mu(n)^2 \mu(n + 1)^2 \mu(n + 2)^2 = \prod_{p \geq 2} \left(1 - \frac{3}{p^2}\right) x + O\left(x^{2/3}\right). \tag{40}$$

The earliest result in this direction appears to be

$$\sum_{n \leq x} \mu(n)^2 \mu(n + t)^2 = cx + O\left(x^{2/3}\right), \tag{41}$$

where $c > 0$ is the constant (29), is studied in [36]. Except for minor adjustments, the generalization to sequences of $(k + 1)$-tuples of squarefree integers has the same structure.

Theorem 4.1. *Let $a \geq 1$ and $s \geq 2$ be small integers. Let $x \geq 1$ be a large number, and let $\mu_s : \mathbb{Z} \longrightarrow \{-1, 0, 1\}$ be the s-power free characteristic function. Then,*

$$\sum_{n \leq x} \mu(n + a_0)^2 \mu(n + a_1)^2 \cdots \mu(n + a_k)^2 = \prod_{p \geq 2} \left(1 - \frac{\rho(s)}{p^2}\right) x + O\left(x^{2/3+\varepsilon}\right), \tag{42}$$

where $q \geq 1$ is a constant, and

$$\rho(s) = \#\{m \leq p^2 : qm + a_i \equiv 0 \bmod p^2 \text{ for } i = 0, 1, 2, ..., k\}, \tag{43}$$

and $\varepsilon > 0$ is an arbitrary small number depending on k and q.

Proof. Consult [36], [35, Theorem 1.2], [54], and the literature. ∎

The literature does not seem to offer any results for squarefree twin integers n and $n + a$, which are relatively prime to $q = q(a)$. A plausible result might have the form given below.

Conjecture 4.1. *Let $x \geq 1$ be a large number, and let $\mu : \mathbb{Z} \longrightarrow \{-1, 0, 1\}$ be the Mobius function. If $a \geq 1$ is a fixed integer, and $q = O(\log^c x)$ with $c \geq 0$ constant, then,*

$$\sum_{\substack{n \leq x \\ \gcd(n,q)=1 \\ \gcd(n+a,q)=1}} \mu(n)^2 \mu(n + a)^2 = c_2(q, a) \prod_{p \nmid q} \left(1 + \frac{1}{p}\right)^{-2} \prod_{p \geq 2} \left(1 - \frac{2}{p^2}\right) x + O\left(x^{1-\delta}\right), \tag{44}$$

where dependence correction factor $c_2(q, a) \geq 0$, and $\delta > 0$ is a small number.

The dependence correction factor $c_2(q,a) \geq 0$, and the parameter $q = q(a)$ depends on $a \geq 1$. For instance, for $a = 2b+1$ odd, the value $q = q(a)$ must be odd, and $c_2(q,a) > 0$, otherwise $c_2(q,a) = 0$ for even q.

5 Summatory Functions For s-Power Free Integers

The subset of k-power free integers is usually denoted by

$$\mathcal{Q}_s = \{n \in \mathbb{Z} : \mu_s(n) \neq 0\} \tag{45}$$

and the complementary subset of non s-free integers is denoted by

$$\overline{\mathcal{Q}_s} = \{n \in \mathbb{Z} : \mu_s(n) = 0\}. \tag{46}$$

The number s-power free integers have the following asymptotic.

Lemma 5.1. *Given an integer $s \geq 2$, let $\mu_s(n)$ be the sth-Mobius function. Then, for any sufficiently large number $x \geq 1$,*

$$\sum_{n \leq x} \mu_s(n) = \frac{1}{\zeta(s)} x + O\left(x^{1/s}\right). \tag{47}$$

Proof. The basic sth-Mobius function μ_s is explained in Definition 2.4. This result is attributed to Gegenbauer, 1885. Recent proofs are provided in [29] and the literature. ■

Lemma 5.2. *Given an integer $s \geq 2$, let $\mu_s(n)$ be the sth-Mobius function. Then, for any sufficiently large number $x \geq 1$,*

$$\sum_{n \leq x} \mu_s(n) = \frac{1}{\zeta(2s)} x + \Omega\left(x^{1/2s}\right). \tag{48}$$

Proof. Same as the proof of Lemma 3.2, mutatis mutandus. ■

Conjecture 5.1. *Given a pair of integers $s \geq 2$, and $q \geq 2$, let $\mu_s(n)$ be the sth-Mobius function. Then, for any sufficiently large number $x \geq 1$,*

$$\sum_{\substack{n \leq x \\ \gcd(n,q)=1}} \mu_s(n) = \frac{1}{\zeta(2s)} \prod_{p \nmid q} \left(1 + \frac{1}{p}\right)^{-1} x + O\left(x^{1/2s}\right). \tag{49}$$

6 Correlation Functions For s-Power Free Integers

Theorem 6.1. *Let $s \geq 2)$ be an integer. Let $x \geq 1$ be a large number, and let $\mu_s : \mathbb{Z} \longrightarrow \{-1,0,1\}$ be the characteristic function of s-power free integers. Then,*

$$\sum_{n \leq x} \mu_s(n)\mu_s(n+a) = \prod_{p \geq 2} \left(1 - \frac{\rho(p,a)}{p^s}\right) x + O\left(x^{\alpha(s)+\varepsilon}\right), \tag{50}$$

where

$$\rho(p) = \begin{cases} 2 & \text{if } p^s \nmid a, \\ 1 & \text{if } p^s \mid a, \end{cases} \tag{51}$$

and

$$\alpha(p,a) = \frac{14}{7s+8} \tag{52}$$

and $\varepsilon > 0$ is an arbitrary small number.

Proof. Different proofs are given in [47], [1, Theorem 1.2], which have slightly different remainder terms. ■

The main problems in this area are the determination of the best remainder terms for various summatory functions. For instance, the remainder term

$$R_s(x) = \sum_{n \le x} \mu_s(n) - \frac{1}{\zeta(2s)} x \tag{53}$$

in Theorem 6.1 is expected to satisfies the upper bound $R_s(x) = O(x^{1/2s+\varepsilon})$ for any small number $\varepsilon > 0$. A survey of the literature on s-power free integers and arithmetic functions is presented in [45]. Currently, $R_s(x) = O\left(x^{1/2s} e^{-\sqrt{\log x}}\right)$ is the best unconditional remainder term.

The literature does not seem to offer any results for s-power free twin integers n and $n + a$, with $a \ge 1$. A plausible result might have the form given below.

Conjecture 6.1. *Given a pair of integers $a \ge 1$ and $s \ge 2$. Let $x \ge 1$ be a large number, and let $\mu : \mathbb{Z} \longrightarrow \{-1, 0, 1\}$ be the Mobius function. If $a \ge 1$, and $q = O(\log^c x)$ with $c \ge 0$ constant, then,*

$$\sum_{\substack{n \le x \\ \gcd(n,q)=1 \\ \gcd(n+a,q)=1}} \mu_s(n)\mu_s(n+1) = c_s(q,a) \prod_{p \nmid q} \left(1 + \frac{1}{p}\right)^{-s} \prod_{p \ge 2} \left(1 - \frac{2}{p^s}\right) x + O\left(x^{1/2s-\delta}\right), \tag{54}$$

where $c_s(q, a) \ge 0$ is a constant, and $\delta > 0$ is a small number.

The constant $c_s(q, a) \ge 0$ and the parameter $q = q(a)$ depend on $a \ge 1$. For instance, for $a = 2b+1$ odd, the value $q = q(a)$ must be odd, and $c_s(q, a) > 0$, otherwise $c_s(q, a) = 0$ for even q.

7 Probabilities For Consecutive Squarefree Integers

The events of 2 consecutive squarefree integers X_0 and X_1 are dependent random variables. Similar, the events of 3 consecutive squarefree integers X_0, X_1, and X_2 are dependent random variables. The probability $P(\mu(X_0) = \pm 1, \mu(X_1) = \pm 1)$ for 2 consecutive squarefree integers is asymptotic to the constant attached to the main term in Lemma 4.1. Specifically,

$$\prod_{q \ge 2} \left(1 - \frac{2}{q^2}\right) = \left(\frac{6}{\pi^2}\right)^2 \prod_{q \ge 2} \left(1 + \frac{1}{q^2(q^2-2)}\right)^{-1} = 0.322699054242535576161483\ldots. \tag{55}$$

The reduction from independent events is measured by the dependence correction factor

$$c_2(2) = \prod_{q \ge 2} \left(1 + \frac{1}{q^2(q^2-2)}\right)^{-1} = 0.872985953449313618771745\ldots. \tag{56}$$

The probability $P(\mu(X_0) = \pm 1, \mu(X_1) = \pm 1, \mu(X_2) = \pm 1)$ for 3 consecutive squarefree integers is asymptotic to the constant attached to the main term in Lemma 4.2. Specifically,

$$\prod_{q \ge 2} \left(1 - \frac{3}{q^2}\right) = \left(\frac{6}{\pi^2}\right)^3 \prod_{q \ge 2} \left(1 + \frac{3q^2-1}{q^4(q^2-3)}\right)^{-1} = 0.125524878896821220184683\ldots. \tag{57}$$

The reduction from independent events is measured by the dependence correction factor

$$c_2(3) = \prod_{q \ge 2} \left(1 + \frac{3q^2-1}{q^4(q^2-3)}\right)^{-1} = 0.558526979127689105533330\ldots. \tag{58}$$

Accordingly, consecutive squarefree integers are highly correlated.

8 Primitive Roots Test

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

Definition 8.1. The order $\min\{k \in \mathbb{N} : u^k \equiv 1 \bmod p\}$ of an element $u \in \mathbb{F}_p$ is denoted by $\operatorname{ord}_p(u)$. An element is a *primitive root* if and only if $\operatorname{ord}_p(u) = p - 1$.

The Euler totient function counts the number of relatively prime integers $\varphi(n) = \#\{k \leq n : \gcd(k, n) = 1\}$.

Lemma 8.1. (Fermat-Euler) *If $a \in \mathbb{Z}$ is an integer such that $\gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \bmod n$.*

Lemma 8.2. (Primitive root test) *An integer $u \in \mathbb{Z}$ is a primitive root modulo an integer $n \in \mathbb{N}$ if and only if*

$$u^{\varphi(n)/p} - 1 \not\equiv 0 \mod n \tag{59}$$

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

The primitive root test is a special case of the Lucas primality test, introduced in [31, p. 302]. A more recent version appears in [9, Theorem 4.1.1], and similar sources.

Lemma 8.3. (Complexity of primitive root test) *Given a prime $p \geq 2$, and primes decomposition of the squarefree part $p_1 p_2 \cdots p_v \mid p-1$, a primitive root modulo p can be determined in deterministic polynomial time $O(\log^c p)$, some constant $c > 1$.*

Proof. The mechanics of the deterministic polynomial time algorithm are specified in [53, Chapter 11]. By [8, Theorem 1.2], the algorithm is repeated at most $O\left((\log p)^{1+\varepsilon}\right)$ times for each $u = O\left((\log p)^{1+\varepsilon}\right)$, with $\varepsilon > 0$. These prove the claim. ∎

9 Representations of the Characteristic Functions

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. Several of these representations are studied in this section.

9.1 Divisors Dependent Characteristic Function

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

Lemma 9.1. *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*

$$\Psi(u) = \frac{\varphi(p-1)}{p-1} \sum_{d \mid p-1} \frac{\mu(d)}{\varphi(d)} \sum_{\operatorname{ord}(\chi)=d} \chi(u) = \begin{cases} 1 & \text{if } \operatorname{ord}_p(u) = p-1, \\ 0 & \text{if } \operatorname{ord}_p(u) \neq p-1. \end{cases} \tag{60}$$

Proof. A full proof appears in [8, Lemma 3.1]. ∎

There are other proofs in the literature. Some details on this characteristic function are given in [16, p. 863], [33, p. 258], [38, p. 18]. The works in [12], and [59] attribute this formula to Vinogradov. But some authors make an earlier reference to Landau.

The characteristic function for multiple primitive roots is used in [11, p. 146] to study consecutive primitive roots. In [15] it is used to study the gap between primitive roots with respect to the Hamming metric. And in [59] 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 τ primitive and $a, b \in \mathbb{F}_p$ constants. In addition, the Artin primitive root conjecture for polynomials over finite fields was proved in [44] using this formula.

9.2 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 9.1. 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], [15] for typical applications and [37, 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 9.1, detects the order $\operatorname{ord}_p(u)$ 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 9.2, detects the order $\operatorname{ord}_p(u) \geq 1$ of the element $u \in \mathbb{F}_p$ by means of the solutions of the equation $\tau^n - u = 0$ in $\mathbb{F}_p$, where u, τ are constants, and $1 \leq n < p-1, \gcd(n, p-1) = 1$, is a variable.

Lemma 9.2. *Let $p \geq 2$ be a prime, and let τ 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 $\operatorname{ord}\psi = p$, then*

$$\Psi(u) = \sum_{\gcd(n,p-1)=1} \frac{1}{p} \sum_{0 \leq m \leq p-1} \psi\left((\tau^n - u)m\right) = \begin{cases} 1 & \text{if } \operatorname{ord}_p(u) = p-1, \\ 0 & \text{if } \operatorname{ord}_p(u) \neq p-1. \end{cases} \tag{61}$$

Proof. A full proof appears in [8, Lemma 3.2]. ■

9.3 Arbitrary Subset Characteristic Function

The previous construction easily generalize to arbitrary subset of the ring $\mathbb{Z}/p\mathbb{Z}$, and other rings.

Lemma 9.3. *Let $p \geq 2$ be a prime, and let $\mathcal{A} \subset \mathbb{Z}/p\mathbb{Z}$ be an arbitrary subset. Let $\psi \neq 1$ be a nonprincipal additive character of order $\operatorname{ord}\psi = p$. Then,*

$$\Psi_{\mathcal{A}}(u) = \sum_{x \in \mathcal{A}} \frac{1}{p} \sum_{0 \leq m \leq p-1} \psi\left((x - u)m\right) = \begin{cases} 1 & \text{if } u \in \mathcal{A}, \\ 0 & \text{if } u \notin \mathcal{A}. \end{cases} \tag{62}$$

Proof. Consider the equation

$$x - u = 0 \tag{63}$$

where u is fixed, and a variable $x \in \mathcal{A}$. Clearly, it has a solution if and only if the fixed element $u \in \mathcal{A}$. ■

10 Estimates Of Exponential Sums

This section provides simple estimates for the exponential sums of interest in this analysis. There are two objectives: To determine an upper bound, proved in Theorem 10.2, and to show that

$$\sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} = \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} + E(p), \tag{64}$$

where $E(p)$ is an error term, this is proved in Lemma 10.1.

10.1 Incomplete And Complete Exponential Sums

Theorem 10.1. ([51], [39]) *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 $x \leq p-1$,*

$$\sum_{n \leq x} e^{i2\pi b\tau^n/p} \ll p^{1/2} \log p. \tag{65}$$

Proof. A complete proof appears in [8, Theorem 5.1]. ■

This seems to be the best possible upper bound. A similar upper bound for composite moduli $p = m$ is also proved, [op. cit., equation (2.29)].

Theorem 10.2. *Let $p \geq 2$ be a large prime, and let τ be a primitive root modulo p. Then,*

$$\sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} \ll p^{1-\varepsilon} \tag{66}$$

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

Proof. A complete proof appears in [8, Theorem 5.2]. ■

The upper bound given in Theorem 10.2 seems to be optimum. A different proof, which has a weaker upper bound, appears in [19, Theorem 6], and related results are given in [4], [18], [21], and [22, Theorem 1].

10.2 Equivalent Exponential Sums

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

$$\{\tau^n : \gcd(n, p-1) = 1\} \quad \text{and} \quad \{b\tau^n : \gcd(n, p-1) = 1\} \subset \mathbb{F}_p \tag{67}$$

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

$$\sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} \quad \text{and} \quad \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p}, \tag{68}$$

have the same upper bound up to an error term. An asymptotic relation for the exponential sums (68) is provided in Lemma 10.1. This result expresses the first exponential sum in (68) as a sum of simpler exponential sum and an error term.

Lemma 10.1. *Let $p \geq 2$ be a large primes. If τ be a primitive root modulo p, then,*

$$\sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} = \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} + O(p^{1/2}\log^3 p), \tag{69}$$

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

Proof. A complete proof appears in [8, Lemma 5.1]. ■

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

$$\sum_{n\in\mathcal{A}} e^{i2\pi b\tau^n/p} = \sum_{n\in\mathcal{A}} e^{i2\pi\tau^n/p} + O(p^{1/2}\log^c p), \tag{70}$$

for some constant $c > 0$.

11 Asymptotic Formulas 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 $a, b > 0$. The symbol $f \ll g$ denote $f = O(g)$.

11.1 Main Term For $k+1$ Consecutive Primitive Roots

Lemma 11.1. *Let $p \geq 2$ be a large prime, let $k \ll \log p$, and let φ be the totient function. Then,*

$$\sum_{n\in\mathbb{F}_p} \prod_{0\leq i\leq k} \left(\frac{1}{p} \sum_{\gcd(n_i,p-1)=1} 1 \right) = \left(\frac{\varphi(p-1)}{p-1} \right)^{k+1} p + O\left(\log^2 p\right). \tag{71}$$

Proof. Each inner sum has the exact value $\varphi(p-1)/p$. Hence,

$$\begin{aligned} M(k,p) &= \sum_{n\in\mathbb{F}_p}\prod_{0\le i\le k}\left(\frac{1}{p}\sum_{\gcd(n_i,p-1)=1}1\right) \\ &= \left(\frac{\varphi(p-1)}{p}\right)^{k+1}\sum_{n\in\mathbb{F}_p}1 \qquad (72)\\ &= \left(\frac{\varphi(p-1)}{p}\right)^{k+1}p. \end{aligned}$$

Last, but not least use the readjustment

$$\frac{\varphi(p-1)}{p}=\frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \qquad (73)$$

to obtain the standard form of the main term. ■

11.2 Main Term For $k+1$ Consecutive Squarefree Primitive Roots

The list of numbers $a_0, a_1, \ldots, a_k$ forms an increasing sequence of distinct integers, an admissible $(k+1)$ tuple, see Definition 4.1.

Lemma 11.2. *Let $p\geq 2$ be a large prime, let $k\ll \log p$, and let φ be the totient function. Then,*

$$\sum_{n\in\mathbb{F}_p}\prod_{0\le i\le k}\left(\frac{1}{p}\sum_{\gcd(n_i,p-1)=1}\mu(n+a_i)^2\right)=\prod_{q\geq 2}\left(1-\frac{\rho(q)}{q^2}\right)\left(\frac{\varphi(p-1)}{p-1}\right)^{k+1}p+O\left(x^{2/3+\varepsilon}\right), \qquad (74)$$

where $\varepsilon>0$ is an arbitrarily small number.

Proof. Rearrange the finite sum and observe that each inner sum has the exact value $\varphi(p-1)/p = \sum_{\gcd(n,p-1)=1} 1$. Hence,

$$\begin{aligned} M(k,p) &= \sum_{n\in\mathbb{F}_p}\left(\frac{\mu(n+a_0)^2}{p}\sum_{\gcd(n_0,p-1)=1}1\cdots\frac{\mu(n+a_k)^2}{p}\sum_{\gcd(n_k,p-1)=1}1\right) \\ &= \left(\frac{\varphi(p-1)}{p}\right)^{k+1}\sum_{n\in\mathbb{F}_p}\mu(n+a_0)^2\cdots\mu(n+a_k)^2 \qquad (75)\\ &= \prod_{q\geq 2}\left(1-\frac{\omega(q)}{q^2}\right)\left(\frac{\varphi(p-1)}{p-1}\right)^{k+1}p+O\left(x^{2/3+\varepsilon}\right). \end{aligned}$$

The last line follows from Theorem 4.1 applied to the correlation function, and $\varepsilon>0$ is an arbitrarily small number. Now, use the readjustment

$$\frac{\varphi(p-1)}{p}=\frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \qquad (76)$$

to obtain the standard form of the main term. ■

11.3 Main Term For Squarefree Twin Primitive Roots

Lemma 11.3. *Let $p\geq 2$ be a large prime, let φ be the totient function, and let μ be the Mobius function. Then,*

$$\begin{aligned} &\sum_{n\in\mathbb{F}_p}\left(\frac{\mu^2(n)}{p}\sum_{\gcd(n_0,p-1)=1}1\right)\left(\frac{\mu^2(n+1)}{p}\sum_{\gcd(n_1,p-1)=1}1\right) \qquad (77)\\ &= \prod_{q\geq 2}\left(1-\frac{2}{q^2}\right)\left(\frac{\varphi(p-1)}{p-1}\right)^{2}p+O\left(p^{2/3}\right). \end{aligned}$$

Proof. Rearrange it and simplify it as

$$\begin{aligned} M_2(2,p) &= \sum_{n\in\mathbb{F}_p}\left(\frac{\mu^2(n)}{p}\sum_{\gcd(n_0,p-1)=1}1\right)\left(\frac{\mu^2(n+1)}{p}\sum_{\gcd(n_1,p-1)=1}1\right) \\ &= \left(\frac{\varphi(p-1)}{p}\right)^2\sum_{n\in\mathbb{F}_p}\mu^2(n)\mu^2(n+1) \qquad (78)\\ &= \left(\frac{\varphi(p-1)}{p}\right)^2\left(\prod_{q\geq 2}\left(1-\frac{2}{q^2}\right)p+O\left(p^{2/3}\right)\right) \end{aligned}$$

The last line follows from Lemma 4.1 or Theorem 4.1 applied to the correlation function. Lastly, use the readjustment

$$\frac{\varphi(p-1)}{p}=\frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \tag{79}$$

to obtain the standard form of the main term. ■

11.4 Main Term For Squarefree Triple Primitive Roots

Lemma 11.4. *Let $p\geq 2$ be a large prime, let φ be the totient function, and let μ be the Mobius function. Then, the number of three consecutive squarefree primitive root has the asymptotic formula*

$$\begin{aligned} &\sum_{n\in\mathbb{F}_p}\left(\frac{\mu^2(n)}{p}\sum_{\gcd(n_0,p-1)=1}1\right)\left(\frac{\mu^2(n+1)}{p}\sum_{\gcd(n_1,p-1)=1}1\right)\left(\frac{\mu^2(n+2)}{p}\sum_{\gcd(n_1,p-1)=1}1\right) \\ &= \prod_{q\geq 2}\left(1-\frac{3}{q^2}\right)\left(\frac{\varphi(p-1)}{p-1}\right)^3 p+O\left(p^{2/3}\right). \qquad (80) \end{aligned}$$

Proof. Rearrange it and simplify it as

$$\begin{aligned} M_2(3,p) &= \sum_{n\in\mathbb{F}_p}\left(\frac{\mu^2(n)}{p}\sum_{\gcd(n_0,p-1)=1}1\right)\left(\frac{\mu^2(n+1)}{p}\sum_{\gcd(n_1,p-1)=1}1\right) \\ &\quad\times\left(\frac{\mu^2(n+2)}{p}\sum_{\gcd(n_2,p-1)=1}1\right) \\ &= \left(\frac{\varphi(p-1)}{p}\right)^3\sum_{n\in\mathbb{F}_p}\mu^2(n)\mu^2(n+1)\mu^2(n+2) \qquad (81)\\ &= \left(\frac{\varphi(p-1)}{p}\right)^3\left(\prod_{q\geq 2}\left(1-\frac{3}{q^2}\right)p+O\left(p^{2/3}\right)\right) \end{aligned}$$

The last line follows from Lemma 4.2 or Theorem 4.1 applied to the correlation function. Lastly, use the readjustment

$$\frac{\varphi(p-1)}{p}=\frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \tag{82}$$

to obtain the standard form of the main term. ■

11.5 Main Term For s-Power Free Primitive Roots

Lemma 11.5. *Let $p\geq 2$ be a large prime, let $s\geq 2$ be an integer, and let μ_s be the characteristic function of s-power free integers. Then,*

$$\sum_{n\in\mathbb{F}_p}\frac{\mu_s(n)}{p}\sum_{\gcd(m,p-1)=1}1=\frac{1}{\zeta(s)}\frac{\varphi(p-1)}{p-1}p+O\left(p^{1/s}\right). \tag{83}$$

Proof. Simplify the double sum:

$$\frac{1}{p}\sum_{n\in\mathbb{F}_p}\mu_s(n)\sum_{\gcd(m,p-1)=1}1=\frac{\varphi(p-1)}{p}\sum_{n\in\mathbb{F}_p}\mu_s(n). \tag{84}$$

Replace the characteristic function for s-power free integers, see Lemma 2.2, and reverse the order of summation:

$$\begin{aligned}\frac{\varphi(p-1)}{p}\sum_{n\in\mathbb{F}_p}\mu_s(n) &= \frac{\varphi(p-1)}{p}\sum_{n\in\mathbb{F}_p}\sum_{d^s\mid n}\mu(d) \\ &= \frac{\varphi(p-1)}{p}\sum_{d\le p^{1/s}}\mu(d)\sum_{\substack{n\in\mathbb{F}_p\\ d^s\mid n}}1 \\ &= \frac{\varphi(p-1)}{p}\sum_{d\le p^{1/s}}\mu(d)\left(\frac{p}{d^s}+O(1)\right) \\ &= \frac{1}{\zeta(s)}\frac{\varphi(p-1)}{p}p+O\left(p^{1/s}\right),\end{aligned} \tag{85}$$

where $1/\zeta(s)=\sum_{n\ge1}\mu(n)n^{-s}$ is the inverse zeta function. Now, use the readjustment

$$\frac{\varphi(p-1)}{p}=\frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \tag{86}$$

to obtain the standard form of the main term. ■

11.6 Main Term For s-Power Free Twin Primitive Roots

Lemma 11.6. *Let $p\ge 2$ be a large prime, let $a_0\ne a_1$ and $s\ge 2$ be small integers. Let μ_s be the s-power free characteristic function. Then,*

$$\begin{aligned}&\sum_{n\in\mathbb{F}_p}\left(\frac{\mu_s(n+a_0)}{p}\sum_{\gcd(n_0,p-1)=1}1\right)\left(\frac{\mu_s(n+a_1)}{p}\sum_{\gcd(n_1,p-1)=1}1\right) \\ &=\prod_{q\ge2}\left(1-\frac{\rho(s)}{q^s}\right)\left(\frac{\varphi(p-1)}{p-1}\right)^2 p+O\left(p^{\alpha(s)+\varepsilon}\right),\end{aligned} \tag{87}$$

where $\rho(s)=1,2$, $\alpha(s)<1$ and $\varepsilon>0$ is an arbitrary small number.

Proof. Rearrange it and simplify it as

$$\begin{aligned}M_2(2,p) &= \sum_{n\in\mathbb{F}_p}\left(\frac{\mu_s(n)}{p}\sum_{\gcd(n_0,p-1)=1}1\right)\left(\frac{\mu_s(n+a)}{p}\sum_{\gcd(n_1,p-1)=1}1\right) \\ &= \left(\frac{\varphi(p-1)}{p}\right)^2\sum_{n\in\mathbb{F}_p}\mu_s(n)\mu_s(n+a) \\ &= \left(\frac{\varphi(p-1)}{p}\right)^2\left(\prod_{q\ge2}\left(1-\frac{\rho(s)}{q^s}\right)p+O\left(p^{\alpha(s)+\varepsilon}\right)\right)\end{aligned} \tag{88}$$

The last line follows from Theorem 6.1 applied to the correlation function. Lastly, use the readjustment

$$\frac{\varphi(p-1)}{p}=\frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \tag{89}$$

to obtain the standard form of the main term. ■

11.7 Main Term For Relatively Prime Primitive Roots

Lemma 11.7. *Let $p \geq 2$ be a large prime, and let $q \leq p-1$ be a fixed integer. Then,*

$$\frac{1}{p} \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1}} \sum_{\gcd(m,p-1)=1} 1 = \frac{\varphi(q)}{q} \frac{\varphi(p-1)}{p-1} p + O(\log^2 p). \tag{90}$$

Proof. Simplify the double sum:

$$\begin{aligned} M_r(p,q) &= \frac{1}{p} \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1}} \sum_{\gcd(m,p-1)=1} 1 \\ &= \frac{\varphi(p-1)}{p} \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1}} 1. \end{aligned} \tag{91}$$

Replace the characteristic function for relatively prime numbers, see Definition 2.5, and rearrange the order of summation:

$$\begin{aligned} \frac{\varphi(p-1)}{p} \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1}} 1 &= \frac{\varphi(p-1)}{p} \sum_{n \in \mathbb{F}_p} \sum_{\substack{d \mid n \\ d \mid q}} \mu(d) \\ &= \frac{\varphi(p-1)}{p} \sum_{d \mid q} \mu(d) \sum_{\substack{n \in \mathbb{F}_p \\ d \mid n}} 1 \\ &= p \frac{\varphi(p-1)}{p} \sum_{d \mid q} \frac{\mu(d)}{d} \\ &= \frac{\varphi(q)}{q} \frac{\varphi(p-1)}{p-1} p, \end{aligned} \tag{92}$$

where $\varphi(n)/n = \sum_{d \mid n} \mu(d)/d$, see Section 2. Lastly, use the readjustment

$$\frac{\varphi(p-1)}{p} = \frac{\varphi(p-1)}{p-1} \left(1 - \frac{1}{p}\right) \tag{93}$$

to obtain the standard form of the main term. ∎

11.8 Main Term For Relatively Prime Twin Primitive Roots

The identity $\varphi(n) = \sum_{\gcd(d,n)=1} 1$, and the estimate $\sum_{d \mid q} |\mu(d)| = O\left(q^{\delta}\right)$ for $\delta > 0$ is a small number, see Section 2, are used within the proofs.

Lemma 11.8. *If $p \geq 2$ is a large prime, let $a \geq 1$ and $q \leq p-1$ be a pair of fixed integers. Then,*

$$\frac{1}{p} \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1 \\ \gcd(n+a,q)=1}} \sum_{\gcd(m,p-1)=1} 1 = c_2(q,a) \left(\frac{\varphi(q)}{q}\right)^2 \frac{\varphi(p-1)}{p-1} p + O\left(p^{2\delta}\right), \tag{94}$$

where $c_2(q,a) \geq 0$ is a dependence correction factor, and $\delta > 0$ is a small number.

Proof. Simplify the double sum:

$$\frac{1}{p} \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1 \\ \gcd(n+a,q)=1}} \sum_{\gcd(m,p-1)=1} 1 = \frac{\varphi(p-1)}{p} \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1 \\ \gcd(n+a,q)=1}} 1. \tag{95}$$

Replace the characteristic function for relatively prime numbers, see Definition 2.5, and rearrange the order of summation:

$$\begin{aligned}
\frac{\varphi(p-1)}{p}\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1\\ \gcd(n+a,q)=1}} 1 &= \frac{\varphi(p-1)}{p}\sum_{n\in\mathbb{F}_p}\sum_{\substack{d\mid n\\ d\mid q}}\mu(d)\sum_{\substack{e\mid n+a\\ e\mid q}}\mu(e) \qquad (96)\\
&= \frac{\varphi(p-1)}{p}\sum_{d\mid q}\mu(d)\sum_{e\mid q}\mu(e)\sum_{\substack{n\in\mathbb{F}_p\\ d\mid n\\ e\mid n+1}} 1\\
&= \frac{\varphi(p-1)}{p}\sum_{d\mid q}\mu(d)\sum_{e\mid q}\mu(e)\left(c_2(q,a)\frac{p}{de}+O(1)\right),
\end{aligned}$$

where $c_2(q,a)\geq 0$ is a dependence correction factor. Continuing yield

$$\begin{aligned}
\frac{\varphi(p-1)}{p}\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1\\ \gcd(n+a,q)=1}} 1 &= c_2(q,a)p\frac{\varphi(p-1)}{p}\sum_{d\mid q}\frac{\mu(d)}{d}\sum_{e\mid q}\frac{\mu(e)}{e}+O\left(\sum_{d\mid q}|\mu(d)|\sum_{e\mid q}|\mu(e)|\right)\\
&= c_2(q,a)\left(\frac{\varphi(q)}{q}\right)^2\frac{\varphi(p-1)}{p}p+O\left(q^{2\delta}\right), \qquad (97)
\end{aligned}$$

where $\delta>0$ is a small number, and $\sum_{d\mid q}|\mu(d)|=O(q^{\delta})=O\left(p^{\delta}\right)$. Lastly, use the readjustment

$$\frac{\varphi(p-1)}{p}=\frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \qquad (98)$$

to obtain the standard form of the main term. ■

The above proof is a simplified version, it does not show the details of the dependence between the variables $d\mid$ and $e\mid q$ in the last line of (96). It simply includes a dependence correction constant $c_2(q)>0$.

11.9 Main Term For Squarefree And Relatively Prime Primitive Roots

Lemma 11.9. *Let $p\geq 2$ be a large prime, and let $q=O(\log p)$ be a fixed integer. Then,*

$$\frac{1}{p}\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1}}\sum_{\gcd(m,p-1)=1}\mu(n)^2=\frac{6}{\pi^2}\prod_{p\nmid q}\left(1+\frac{1}{p}\right)^{-1}\frac{\varphi(p-1)}{p-1}p+O\left(p^{1/2}\right) \qquad (99)$$

Proof. Simplify the double sum:

$$\begin{aligned}
M_r(p,q) &= \frac{1}{p}\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1}}\sum_{\gcd(m,p-1)=1}\mu(n)^2 \qquad (100)\\
&= \frac{\varphi(p-1)}{p}\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1}}\mu(n)^2.
\end{aligned}$$

Apply Lemma 3.3 to the inner sum:

$$\begin{aligned}
\frac{\varphi(p-1)}{p}\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1}}\mu(n)^2 &= \frac{\varphi(p-1)}{p}\left(\frac{6}{\pi^2}\prod_{p\nmid q}\left(1+\frac{1}{p}\right)^{-1}p+O\left(p^{1/2}\right)\right)\\
&= \frac{6}{\pi^2}\prod_{p\nmid q}\left(1+\frac{1}{p}\right)^{-1}\frac{\varphi(p-1)}{p}p+O\left(p^{1/2}\right).
\end{aligned}$$

Lastly, use the readjustment

$$\frac{\varphi(p-1)}{p}=\frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \tag{101}$$

to obtain the standard form of the main term. ■

11.10 Main Term For Squarefree And Relatively Prime Twin Primitive Roots

Lemma 11.10. *Assume conjecture 4.1. If $p\geq 2$ is a large prime, let $a\geq 1$ and $q\leq p-1$ be a pair of fixed integers. Then,*

$$\begin{aligned}&\frac{1}{p^2}\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1\\ \gcd(n+a,q)=1}}\ \sum_{\substack{\gcd(m_0,p-1)=1\\ \gcd(m_1,p-1)=1}}\mu(n)^2\mu(n+a)^2 \\ =\ & c_2(q,a)\prod_{r\mid q}\left(1-\frac{1}{r^s}\right)\prod_{p\geq 2}\left(1-\frac{2}{p^s}\right)\left(\frac{\varphi(p-1)}{p-1}\right)^2 p+O\left(p^{2\delta}\right),\end{aligned} \tag{102}$$

where $c_2(q,a)\geq 0$ is a dependence correction factor, and $\delta>0$ is a small number.

Proof. Simplify the double sum:

$$\frac{1}{p^2}\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1\\ \gcd(n+a,q)=1}}\ \sum_{\substack{\gcd(m_0,p-1)=1\\ \gcd(m_1,p-1)=1}}\mu(n)^2\mu(n+a)^2=\left(\frac{\varphi(p-1)}{p}\right)^2\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1\\ \gcd(n+a,q)=1}}\mu(n)^2\mu(n+a)^2. \tag{103}$$

Set $x=p$, and apply Conjecture 4.1 to the inner finite sum:

$$\begin{aligned}M_{sr}(2,p,q)\ &=\ \left(\frac{\varphi(p-1)}{p}\right)^2\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1\\ \gcd(n+a,q)=1}}\mu(n)^2\mu(n+a)^2 \\ &=\ \left(\frac{\varphi(p-1)}{p}\right)^2\left(c_2(q,a)\prod_{p\nmid q}\left(1+\frac{1}{p}\right)^{-2}\prod_{p\geq 2}\left(1-\frac{2}{p^2}\right)p+O\left(p^{1-\delta}\right)\right) \\ &=\ c_2(q,a)\prod_{p\nmid q}\left(1+\frac{1}{p}\right)^{-2}\prod_{p\geq 2}\left(1-\frac{2}{p^2}\right)\left(\frac{\varphi(p-1)}{p}\right)^2 p+O\left(p^{1-\delta}\right),\end{aligned} \tag{104}$$

where $c_2(q,a)\geq 0$ is a dependence correction factor, and $\delta>0$ is a small number. Lastly, use the readjustment

$$\frac{\varphi(p-1)}{p}=\frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \tag{105}$$

to obtain the standard form of the main term. ■

12 The Estimates For The Error Terms

The upper bounds for exponential sums over subsets of elements in finite fields $\mathbb{F}_p$ studied in Section 10 are used to estimate the error terms for the different configurations of consecutive primitive roots in Theorem 1.2 and the other results.

Lemma 12.1. *Let $p\geq 2$ be a large prime, and let τ be a primitive root mod p. If the element $u\neq 0,\pm1,v^2$ is not a primitive root, then,*

$$S(p,k)=\sum_{u\in\mathbb{F}_p}\left(\frac{1}{p}\sum_{\gcd(n,p-1)=1,\ 0<m\leq p-1}\ \sum e^{i2\pi((\tau^n-u)m)}\right)\ll p^{1-\varepsilon} \tag{106}$$

for all sufficiently large primes $p\geq 2$, and an arbitrarily small number $\varepsilon>0$.

Proof. By hypothesis $u \neq 0, \pm 1, v^2$ is not a primitive root. Thus, $S_1 \neq -\varphi(p-1)$. Rearrange the finite sum as

$$\begin{aligned} S_1 &= \sum_{u \in \mathbb{F}_p} \frac{1}{p} \sum_{\gcd(n,p-1)=1,} \sum_{0<m\leq p-1} e^{i2\pi((\tau^n-u)m)} \\ &= \frac{1}{p}\sum_{u \in \mathbb{F}_p} \left(\sum_{0<m\leq p-1,} e^{-i2\pi um/p} \right) \left(\sum_{\gcd(n,p-1)=1} e^{i2\pi m\tau^n/p} \right) \\ &= \frac{1}{p}\sum_{u \in \mathbb{F}_p} \left(\sum_{0<m\leq p-1,} e^{-i2\pi um/p} \right) \left(\sum_{\gcd(n,p-1)=1} e^{i2\pi \tau^n/p} + O(p^{1/2}\log^3 p) \right) \\ &= \frac{1}{p}\sum_{u \in \mathbb{F}_p} U_p \cdot V_p. \end{aligned} \tag{107}$$

The third line in equation (107) follows from Lemma 10.1. The first exponential sum U_p has the exact evaluation

$$|U_p| = \left| \sum_{0<m\leq p-1} e^{-i2\pi um/p} \right| = 1, \tag{108}$$

where $\sum_{0<m\leq p-1} e^{i2\pi um/p} = -1$ for any $u \in [1, p-1]$. The second exponential sum V_p has the upper bound

$$\begin{aligned} |V_p| &= \left| \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} + O\left(p^{1/2}\log^3 p\right) \right| \\ &\ll \left| \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} \right| + p^{1/2}\log^3 p \\ &\ll p^{1-\varepsilon}, \end{aligned} \tag{109}$$

where $\varepsilon < 1/2$ is an arbitrarily small number, see Theorem 10.2. Taking absolute value in (107), and replacing the estimates (108) and (109) return

$$\begin{aligned} |S_1| &\leq \frac{1}{p}\sum_{u \in \mathbb{F}_p} |U_p| \cdot |V_p| \\ &\ll \frac{1}{p}\sum_{u \in \mathbb{F}_p} (1) \cdot p^{1-\varepsilon} \\ &\ll \frac{1}{p^{\varepsilon}}\sum_{u \in \mathbb{F}_p} 1 \\ &\ll p^{1-\varepsilon}. \end{aligned} \tag{110}$$

■

No effort was made to optimize the error term in Lemma 12.1. However, it should be noted that the best possible is $p^{1/2+\varepsilon}$, see Theorem 10.2.

12.1 Error Term For $k+1$ Consecutive Primitive Roots

Lemma 12.2. *Let $p \geq 2$ be a large prime, let $k < \log p/\log\log\log p$ be an integer, and let τ be a primitive root mod p. If the element $n + a_i \neq 0, \pm 1, v^2$ is not a primitive root for $i = 0, 1, 2, ..., k$, then,*

$$E(k,p) = \sum_{n \in \mathbb{F}_p} \prod_{0\leq i\leq k} \left(\frac{1}{p} \sum_{\substack{\gcd(n_i,p-1)=1 \\ 0<m_i\leq p-1}} e^{i2\pi((\tau^{n_i}-n-a_i)m_i)} \right) \ll p^{1-\varepsilon} \tag{111}$$

for all sufficiently large primes $p \geq 2$, and an arbitrarily small number $\varepsilon > 0$.

Proof. By hypothesis $n + a_i \neq 0, \pm 1, v^2$ is not a primitive root for $i = 0, 1, 2, ..., k$. Thus, $E(k,p) \neq -(\varphi(p-1)/p)^{k+1}p$. Rewrite the multiple finite sum as a product $E(p,\tau) = S_1 \times S_2$. The first sum indexed by $m = m_0$ and $n = n_0$ has a nontrivial upper bound

$$|S_1| \ll p^{1-\varepsilon}, \tag{112}$$

see Lemma 12.1. The product of the remaining sums indexed by m_i and n_i, $i \in \{1, 2, \ldots k-1\}$ have the trivial upper bound

$$\begin{aligned} |S_2| &\leq \left| \frac{1}{p} \sum_{\substack{\gcd(n_1,p-1)=1 \\ 0<m_1\leq p-1}} e^{i2\pi((\tau^{n_1}-n-a_1)m_1)} \right| \cdots \left| \frac{1}{p} \sum_{\substack{\gcd(n_k,p-1)=1 \\ 0<m_k\leq p-1}} e^{i2\pi((\tau^{n_k}-n-a_k)m_k)} \right| \\ &\leq \frac{\varphi(p-1)}{p} \cdots \frac{\varphi(p-1)}{p} \\ &\leq \left(\frac{\varphi(p-1)}{p} \right)^k . \end{aligned} \tag{113}$$

Merging (112) and (113) returns

$$\begin{aligned} |E(p,\tau)| &\leq |S_1| \, |S_2| \\ &\leq \left(p^{1-\varepsilon}\right) \times \left(\frac{\varphi(p-1)}{p} \right)^k \\ &\leq p^{1-\varepsilon}. \end{aligned} \tag{114}$$

The last inequality uses $\varphi(p-1)/p \leq 1$. ■

12.2 Error Term For s-Power Free Primitive Roots

Lemma 12.3. *Let $p \geq 2$ be a large prime, let τ be a primitive root mod p, and let μ_s be the characteristic function of s-power free integers. If the element $n \neq 0, \pm 1, v^2$ is not a primitive root, then,*

$$E(s,p) = \sum_{n \in \mathbb{F}_p} \left(\frac{\mu_s(n)}{p} \sum_{\substack{\gcd(m,p-1)=1 \\ 1\leq a\leq p-1}} \psi\left((\tau^m - n)a\right) \right) \ll p^{1-\varepsilon} \tag{115}$$

for all sufficiently large primes $p \geq 2$, and an arbitrarily small number $\varepsilon > 0$.

Proof. Same as Lemma 12.1, mutatis mutandus. ■

12.3 Error Term For $k+1$ Consecutive Squarefree Primitive Roots

Lemma 12.4. *Let $p \geq 2$ be a large prime, let $0 \leq a_0, a_1, a_2, \ldots, a_k$ be an admissible $(k+1)$-tuple of integers, and let τ be a primitive root modulo p. If the element $n + a_i \neq 0, \pm 1, v^2$ is not a primitive root for $i = 0, 1, 2, ..., k$, then,*

$$E_s(k,p) = \sum_{n \in \mathbb{F}_p} \prod_{0\leq i\leq k} \left(\frac{\mu^2(n+a_i)}{p} \sum_{\substack{\gcd(n_i,p-1)=1 \\ 1\leq b_i\leq p-1}} \psi\left((\tau^{n_i} - n - a_i)b_i\right) \right) \ll p^{1-\varepsilon} \tag{116}$$

for all sufficiently large primes $p \geq 2$, and an arbitrarily small number $\varepsilon > 0$.

Proof. Same as Lemma 12.2, mutatis mutandus. ■

12.4 Error Term For Restricted $k+1$ Consecutive Primitive Roots

Lemma 12.5. *Let $p \geq 2$ be a large prime, let $0 \leq a_0, a_1, a_2, \ldots, a_k$ be an admissible $(k+1)$-tuple of integers, and let τ be a primitive root modulo p. If the element $n+a_i \neq 0, \pm 1, v^2$ is not a primitive root for $i = 0, 1, 2, ..., k$, and $f(n) \ll 1$ is a bounded arithmetic function, then,*

$$E_s(k,p) = \sum_{n \in \mathbb{F}_p} \prod_{0 \leq i \leq k} \left(\frac{f(n+a_i)}{p} \sum_{\substack{\gcd(n_i, p-1)=1 \\ 1 \leq b_i \leq p-1}} \psi\left((\tau^{n_i} - n - a_i) b_i \right) \right) \ll p^{1-\varepsilon} \tag{117}$$

for all sufficiently large primes $p \geq 2$, and an arbitrarily small number $\varepsilon > 0$.

Proof. Use the fact that $|f(n)| \ll 1$, and the same technique as Lemma 12.2, mutatis mutandus. ■

13 Some Collections Of Primes

Some information on the collections of primes of interest in the theory of consecutive and quasi consecutive primitive roots are recorded in this Section.

13.1 Average Primes

The subset of average random primes is taken to be

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, \cdots\}. \tag{118}$$

It consists of all the primes numbers. An average random prime $p \geq 2$ has the average totient $p-1 = \varphi(p)$, has the mean numbers of prime divisors,

$$\omega(p-1) \ll \log\log p, \tag{119}$$

and the average value

$$\frac{\varphi(p-1)}{p-1} = \prod_{q \mid p-1} \approx \frac{1}{\log\log\log p}, \tag{120}$$

where $r \leq q$ ranges over the primes. The theory of the set of primes is highly developed, and a topic of extensive research.

13.2 Primorial Primes

The subset of primorial primes

$$\mathcal{A} = \{p = 2 \cdot 3 \cdot 5 \cdot 7 \cdots q + 1 : \text{ prime } q \geq 2\} \tag{121}$$

is studied in [5], and listed in OEIS A014545. A primorial prime has highly composite totient $p-1 = \varphi(p)$, the maximal numbers of prime divisors

$$\omega(p-1) \ll \log p / \log\log p, \tag{122}$$

see Lemma 2.1, and the minimal value

$$\frac{\varphi(p-1)}{p-1} = \prod_{q \mid p-1} \left(1 - \frac{1}{q}\right) \approx \frac{1}{\log\log p}, \tag{123}$$

where $r \leq q$ ranges over the primes, see Theorem 2.2. The heuristic claims that there are infinitely many primorial primes. The theory of the subset of primes is at a rudimentary stage, and a topic of current research.

13.3 Coprimorial Primes

The subset of coprimorial primes is defined by

$$\mathcal{B} = \{p = 3 \cdot 5 \cdot 7 \cdots q + 2 : \text{ prime } q \geq 2\}. \tag{124}$$

The heuristic seems to show the existence of infinitely many coprimorial primes. The collection of these primes is not a topic of research in the literature. The totient $p - 1 = \varphi(p)$ of a coprimorial prime has very few prime divisors

$$\omega(p-1) \ll 1, \tag{125}$$

and nearly maximal value

$$\frac{\varphi(p-1)}{p-1} = \prod_{q \mid p-1} \left(1 - \frac{1}{q}\right) \approx 2. \tag{126}$$

The coprimorial primes have Germain primes type structure.

13.4 Germain Primes

The subset of Germain primes is defined by

$$\mathcal{S} = \{p = 2^a \cdot q + 1 : \text{ prime } q \geq 2 \text{ and } a \geq 1\}. \tag{127}$$

The heuristic claims that there are infinitely many Germain primes. The theory of the subset of Germain primes is not fully developed, but it is a topic of current research. The totient $p-1 = \varphi(p)$ of a Germain prime has two prime divisors

$$\omega(p-1) = 2, \tag{128}$$

and the nearly maximal value

$$\frac{\varphi(p-1)}{p-1} = \prod_{q \mid p-1} \left(1 - \frac{1}{q}\right) \approx 2, \tag{129}$$

where $r \leq q$ ranges over the primes.

13.5 Fermat Primes

The subset of Fermat primes is defined by

$$\mathcal{S} = \{p = 2^{2^n} + 1 : n \geq\}. \tag{130}$$

The heuristic claims that there are finitely many Fermat primes. The theory of this subset of primes is not fully developed, but it is a topic of current research. The totient $p - 1 = \varphi(p)$ of a Fermat prime has one prime divisor

$$\omega(p-1) = 1, \tag{131}$$

and the maximal value

$$\frac{\varphi(p-1)}{p-1} = \prod_{q \mid p-1} \left(1 - \frac{1}{q}\right) = 2. \tag{132}$$

where $r \leq q$ ranges over the primes.

14 Maximal Length Of Consecutive Primitive Roots

The number of prime divisors $\omega(n)$ of a random integer $n \in \mathbb{N}$ is a normal random variable with mean $\log \log n$, and standard error $\sqrt{\log \log n}$, see Theorem 2.1, and Lemma 2.1. Roughly, there are three major classes of totients $p-1 = \varphi(p)$ and the corresponding classes of the primes divisors counting function $\omega(p-1)$.

(1) The subset of primorial primes $p = 2{\cdot}3{\cdot}5{\cdot}7\cdots q{+}1$ have highly composite totients $p-1 = \varphi(p)$ and the maximal numbers of prime divisors, see Subsection 13.2.

(2) The average primes $p \geq 2$. The average totients $p-1 = \varphi(p)$ have the mean numbers of prime divisors, Subsection 13.1.

(3) The subset of Fermat primes, Germain primes, and coprimorial primes. The totient $p-1 = \varphi(p)$ of any of these primes has the minimal number of prime divisors. These primes are described in Section 13.

Lemma 14.1. *Let $p \geq 2$ be a large prime. Then, the maximal length $k \geq 1$ of a string of consecutive primitive roots is as follows.*

(i) $k \ll \log p/\log\log\log p$, *if* $\omega(p-1) \ll \log p/\log\log p$.

(ii) $k \ll \log p/\log\log\log\log p$, *if* $\omega(p-1) \ll \log\log p$.

(iii) $k \ll \log p$, *if* $\omega(p-1) \ll 1$.

Proof. The existence of an $(k+1)$-tuple implies that

$$p\left(\frac{\varphi(p-1)}{p-1}\right)^{k+1} \gg p^{1-\varepsilon} \tag{133}$$

is true, with $\varepsilon \in (0,1/2)$, see Theorem 1.1. Equivalently, this is

$$k \ll \frac{\varepsilon \log p}{\log\left(\frac{p-1}{\varphi(p-1)}\right)} \ll \frac{\varepsilon\log p}{\log\omega(p-1)}. \tag{134}$$

The three different cases are for

$$\frac{p-1}{\varphi(p-1)} \approx \log\log p, \qquad \frac{p-1}{\varphi(p-1)} \approx \log\log\log p, \qquad \text{and} \qquad \frac{p-1}{\varphi(p-1)} \approx 2 \tag{135}$$

respectively. ■

Definition 14.1. Given a prime $p \geq 2$, and k the longest run of consecutive primitive roots in the finite field $\mathbb{F}_p$, the *length merit ratio* is defined by $\hat{m} = k/\log p$.

The length merit ratio varies as $p \to \infty$, but it remains bounded by a constant $\hat{m} \ll 1$. The Fermat primes $p = 2^{2^n}+1$, $n \geq 0$, the Germain primes $p = 2^a q + 1$, $q \geq 2$ primes and $a \geq 1$, and some other collections, are expected to have the largest length merit ratio. Some numerical data for small primes are provided here. Observe that these small cases are subject to the Strong law of small numbers,[20].

Example 14.1. Extreme Case 1. Some statistic for the finite field $\mathbb{F}_p$ with $p = p = 2^4+1 = 17$.

Prime	$p = 17$
Parameters	$\omega(p-1) = 1$, $\varphi(p-1) = 8$
Primitive roots	$3, 5, 6, 7, 10, 11, 12, 14$
Length k	3
Merit factor	$k/\log p = 1.058869$

Similarly, the prime $p = 2^{16}+1$ has the parameters, $\omega(p-1) = 1$, $\varphi(p-1) = 2^{15}$, and $\log p = 11.09$. Thus, Lemma 14.1 predicts the existence of some 11-tuples or larger k-tuples of consecutive primitive roots in the set of primitive roots $\mathcal{R} = \{3, 5, 7, 11, 13, 15, \ldots.\}$.

Example 14.2. Extreme Case 3. Some statistic for the finite field $\mathbb{F}_p$ with $p = 2\cdot 3\cdot 5+1 = 31$.

Prime	$p = 31$
Parameters	$\omega(p-1) = 3$, $\varphi(p-1) = 8$
Primitive roots	$3, 11, 12, 13, 17, 21, 22, 24$
Length k	3
Merit factor	$k/\log p = 0.873620$

Table 1: Maximal k-Tuple of Primitive Roots Indexed By p.

p	k	$\hat{m}$	p	k	$\hat{m}$	p	k	$\hat{m}$
3	1	0.910239	29	2	0.593948	61	2	0.486514
5	2	1.242669	31	3	0.873620	67	3	0.713488
7	1	0.513898	37	4	1.107751	71	3	0.703782
11	3	1.251097	41	3	0.807847	73	3	0.699225
13	2	0.779742	43	3	0.797617	79	3	0.686585
17	3	1.058868	47	4	1.038921	83	7	1.584125
19	3	1.018869	53	5	1.259353	89	6	1.336708
23	3	0.956786	59	5	1.226230	97	5	1.092965

Table 2: Least Prime p and Maximal k-Tuple of Primitive Roots.

p	k	$\hat{m}$	p	k	$\hat{m}$
$3 = 2 \cdot 1 + 1$	1	0.910239226	$83 = 2^2 \cdot 41 + 1$	7	1.584125933
$5 = 2 \cdot 2 + 1$	2	1.242669869	$347 = 2 \cdot 173 + 1$	8	1.367679228
$11 = 2 \cdot 5 + 1$	3	1.251097174	$269 = 2^2 \cdot 67 + 1$	9	1.608662072
$37 = 2^2 \cdot 3^2 + 1$	4	1.107751574	$563 = 2 \cdot 281 + 1$	10	1.578960758
$53 = 2^2 \cdot 13 + 1$	5	1.259353244	$467 = 2 \cdot 233 + 1$	11	1.789686094
$89 = 2^3 \cdot 11 + 1$	6	1.336708859	$1187 = 2^2 \cdot 3^3 \cdot 11 + 1$	12	1.695110528

15 Consecutive Primitive Roots

Consecutive primitive roots is one of the simplest configuration of a subset of two or more primitive roots. A more general result was proved by Carlitz [6] using a counting technique based on Lemma 9.1. A new proof and counting technique
based on Lemma 9.2 is given here.

15.1 Strings Of $k+1$ Consecutive Primitive Roots

Let $a_0, a_1, a_2, \ldots, a_k$ be a fixed $(k+1)$-tuple of distinct integers. Let $p \geq 2$ be a large prime, and let $\tau \in \mathbb{F}_p$ be a primitive root. A string of $k+1$ consecutive primitive roots $n+a_0, n+a_1, n+a_2, \ldots, n+a_k$ exists if and only if the system of equations

$$\tau^{n_0} = n + a_0, \quad \tau^{n_1} = n + a_1, \quad \tau^{n_2} = n + a_2, \quad \ldots, \quad \tau^{n_k} = n + a_k, \tag{136}$$

has one or more solutions. A solution consists of a $(k+1)$-tuple $n_0, n_1, \ldots, n_k$ of integers such that $\gcd(n_i, p-1) = 1$ for $i = 0, 1, \ldots, k$, and some $n \in \mathbb{F}_p$. Let

$$N(k,p) = \#\left\{n \in \mathbb{F}_p : \operatorname{ord}_p(n + a_i) = p - 1\right\} \tag{137}$$

for $i = 0, 1, \ldots, k$, denotes the number of solutions.

Proof. (Theorem 1.1): The total number of solutions is written in terms of characteristic function for primitive roots, see Lemma 9.2, as

$$\begin{aligned} N(k,p) &= \sum_{n \in \mathbb{F}_p} \Psi(n+a_0)\,\Psi(n+a_1)\cdots\Psi(n+a_k) \qquad (138) \\ &= \sum_{n \in \mathbb{F}_p} \prod_{0 \leq i \leq k} \left(\frac{1}{p} \sum_{\substack{\gcd(n_i,p-1)=1 \\ 0 \leq u_i \leq p-1}} \psi\left((\tau^{n_i} - n - a_i)u_i)\right) \right) \\ &= M(k,p) + E(k,p). \end{aligned}$$

The main term is determined by the indices $u_0 = u_1 = \cdots = u_k = 0$, and has the form

$$M(k,p) = \sum_{n\in\mathbb{F}_p} \prod_{0\le i\le k} \left(\frac{1}{p} \sum_{\gcd(n_i,p-1)=1} 1 \right), \tag{139}$$

and the error term is determined by the indices $u_0 \ne 0, u_1 \ne 0, \ldots, u_k \ne 0$, and has the form

$$E(k,p) = \sum_{n\in\mathbb{F}_p} \prod_{0\le i\le k} \left(\frac{1}{p} \sum_{\substack{\gcd(n_i,p-1)=1 \\ 1\le u_i\le p-1}} \psi\left((\tau^{n_i} - n - a_i)u_i \right) \right). \tag{140}$$

Applying Lemma 11.1 to the main term and Lemma 12.2 to the error term, yield

$$\begin{aligned} N(k,p) &= M(k,p) + E(k,p) \qquad (141) \\ &= \left(\frac{\varphi(p-1)}{p-1} \right)^{k+1} p + O(\log^2 p) + O(p^{1-\varepsilon}) \\ &= \left(\frac{\varphi(p-1)}{p-1} \right)^{k+1} p + O(p^{1-\varepsilon}) \\ &> 0, \end{aligned}$$

for all sufficiently large primes $p \ge 2$, and an arbitrary small number $\varepsilon > 0$.

■

16 Probabilities Functions For Consecutive Primitive Roots

The forms of the main terms in Theorem 1.1 and Theorem 1.2 imply that a primitive root in a finite field $\mathbb{F}_p$ is a nearly independent random variable $X = X(p)$.

Definition 16.1. The probability of primitive roots in a finite field $\mathbb{F}_p$ is defined by

$$P\left(\operatorname{ord}_p(X) = p-1\right) = \frac{\varphi(p-1)}{p-1} + O\left(\frac{1}{p^{\varepsilon}}\right), \tag{142}$$

where $\varepsilon > 0$ is a small number.

The occurrence of each primitive root is approximately an independent variable X with probability $P(\operatorname{ord}_p X = p-1) = \varphi(p-1)/(p-1)$, as demonstrated in Definition 16.1. A random $(k+1)$-tuple of consecutive primitive roots is denoted by

$$Z_k = (X_0, X_1, \ldots, X_k), \tag{143}$$

where each primitive root X_i has order $\operatorname{ord}_p(X_i) = p-1$. The Fermat prime numbers $p = 2^{2^m} + 1$ and the Germain primes $p = 2^a q + 1$, where $a \ge 1$ and $q \ge 2$ is prime, have the simpler totients $p-1$, see Section 13, and descriptions of the probabilities functions of the $k+1$-tuples. The precise form for Germain primes is

$$P(Z_k) = \left(\frac{\varphi(p-1)}{p-1} \right)^{k+1} = \left(\frac{1}{2} - \frac{1}{2q} \right)^{k+1}, \tag{144}$$

Table 1 demonstrates this well, almost all the listed cases have Germain primes; the exception could be an instance of the Strong Law of Small Numbers. On the other extreme are the collections of highly composite totients $p-1$. The precise form for primorial primes $p = 2\cdot 3\cdot 5\cdots q + 1$, where $q \ge 3$ is prime, is

$$P(Z_k) = \left(\frac{\varphi(p-1)}{p-1} \right)^{k+1} = \prod_{r\le q} \left(1 - \frac{1}{q} \right)^{k+1}, \tag{145}$$

where $r \le q$ ranges over the primes. Some numerical data are displayed in Figure 1 and Figure 2.

Figure 1: Probability Function of Consecutive Primitive Roots, $p = 2^{16} + 1$

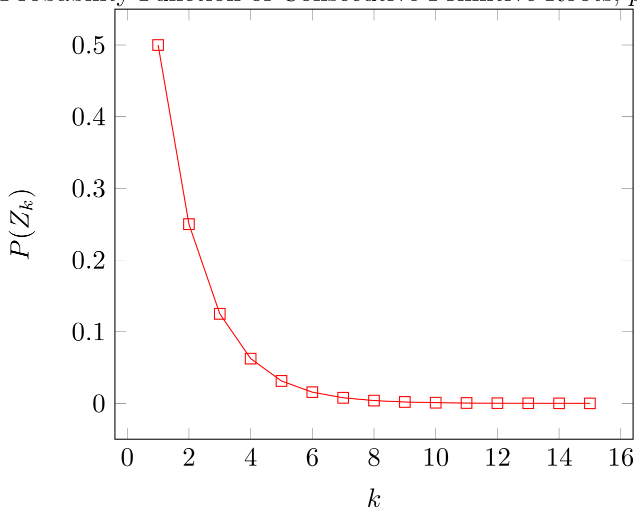
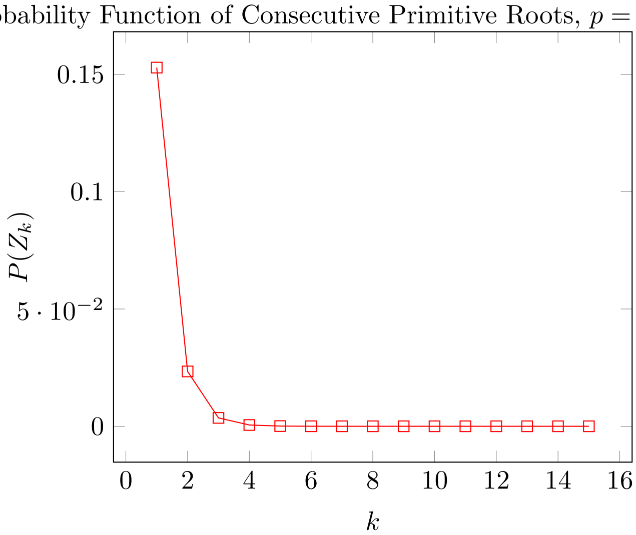


Figure 2: Probability Function of Consecutive Primitive Roots, $p = 2 \cdot 3 \cdots 31 + 1$



17 Consecutive Squarefree Primitive Roots

The result for the existence of multiple consecutive squarefree primitive roots seems to be new in the literature. The first cases for 2 consecutive squarefree primitive roots n and $n+1$, and 3 consecutive squarefree primitive roots n, $n+1$ and $n+2$ are feasible. But, the existence of 4 consecutive squarefree primitive roots n, $n+1$, $n+2$ and $n+3$ is infeasible. However, there are quasi consecutive squarefree primitive roots of length $k \ll \log p$ for a wide range of prime numbers. To describe these possibilities, let $(a_0, a_1, a_2, \ldots, a_k)$ be a fixed integers $(k+1)$-tuple of distinct integers. A string of $k+1$ quasi consecutive squarefree primitive roots $n+a_0, n+a_1, n+a_2, \ldots, n+a_k$ is a solution of the systems of equations:

1. $\tau^{n_0} = n + a_0, \quad \tau^{n_1} = n + a_1, \tau^{n_2} = n + a_2, \quad \ldots, \quad \tau^{n_k} = n + a_k,$
   the primitive root condition.
2. $\mu^2(n + a_0) = 1, \quad \mu^2(n + a_1) = 1, \quad \ldots, \quad \mu^2(n + a_k) = 1,$
   the squarefree condition.

A solution is a tuple $(n, n_0, n_1, \ldots, n_k) \in \mathbb{N}^{k+2}$, with $\gcd(n_i, p-1) = 1$, for $i = 0, 1, \ldots k$. Let

$$N_2(k,p) = \#\left\{n \in \mathbb{F}_p : \operatorname{ord}_p(n + a_i) = p-1, \mu^2(n + a_i) = 1\right\} \tag{146}$$

for $i = 0, 1, \ldots, k$, denotes the number of solutions.

17.1 Strings Of $k+1$ Consecutive Squarefree Primitive Roots

Proof. (Theorem 1.2): The total number of solutions is written in terms of characteristic function for primitive roots, see Lemma 9.2, and the characteristic function for squarefree integers, see Lemma 2.2, as

$$\begin{aligned} N_2(k,p) &= \sum_{n \in \mathbb{F}_p} \prod_{0 \le i \le k} \Psi\left(n + a_i\right) \mu^2(n + a_i) \qquad (147) \\ &= \sum_{n \in \mathbb{F}_p} \prod_{0 \le i \le k} \left(\frac{1}{p} \sum_{\substack{\gcd(n_i, p-1) = 1 \\ 0 \le u_i \le p-1}} \psi\left((\tau^{n_i} - n - a_i) u_i\right) \right) \\ &= M_2(k,p) + E_2(k,p). \end{aligned}$$

The main term is determined by the indices $u_0 = u_1 = \cdots = u_k = 0$, and has the form

$$M_2(k,p) = \sum_{n \in \mathbb{F}_p} \prod_{0 \le i \le k} \left(\frac{\mu^2(n + a_i)}{p} \sum_{\gcd(n_i, p-1) = 1} 1 \right), \tag{148}$$

and the error term is determined by the indices $u_0 \ne 0, u_1 \ne 0, \ldots, u_k \ne 0$, and has the form

$$E_2(k,p) = \sum_{n \in \mathbb{F}_p} \prod_{0 \le i \le k} \left(\frac{\mu^2(n + a_i)}{p} \sum_{\substack{\gcd(n_i, p-1) = 1 \\ 1 \le u_i \le p-1}} \psi\left((\tau^{n_i} - n - a_i) u_i\right) \right). \tag{149}$$

Applying Lemma 11.2 to the main term and Lemma 12.4 to the error term, yield

$$\begin{aligned} N_2(k,p) &= M_2(k,p) + E_2(k,p) \qquad (150) \\ &= \prod_{q \ge 2} \left(1 - \frac{\omega(q)}{q^2}\right) \left(\frac{\varphi(p-1)}{p-1}\right)^{k+1} p + O\left(p^{2/3}\right) + O(p^{1-\varepsilon}) \\ &= \prod_{q \ge 2} \left(1 - \frac{\omega(q)}{q^2}\right) \left(\frac{\varphi(p-1)}{p-1}\right)^{k+1} p + O(p^{1-\varepsilon}) \\ &> 0, \end{aligned}$$

for all sufficiently large primes $p \ge 2$, and an arbitrary small number $\varepsilon > 0$. ∎

17.2 Squarefree Primitive Roots

Let $p \geq 2$ be a large prime, and let $\tau \in \mathbb{F}_p$ be a primitive root. A squarefree primitive root $n \in \mathbb{F}_p$ exists if and only if the system of equations

$$\tau^m = n \quad \text{and} \quad \mu^2(n) = 1, \tag{151}$$

has one or more solutions $(m, n) \in \mathbb{N} \times \mathbb{N}$ such that $\gcd(m, p-1) = 1$, and $n \geq 2$. Let

$$N_2(p) = \#\left\{n \in \mathbb{F}_p : \operatorname{ord}_p(n) = p-1 \text{ and } \mu^2(n) = 1\right\} \tag{152}$$

denotes the number of solutions.

Theorem 17.1. *For any large prime $p \geq 2$, the finite field $\mathbb{F}_p$ contains squarefree primitive roots. Furthermore, the total number has the asymptotic formula*

$$N_2(p) = \prod_{q \geq 2}\left(1 - \frac{1}{q^2}\right)\left(\frac{\varphi(p-1)}{p}\right)p + O(p^{1-\varepsilon}), \tag{153}$$

where $\varepsilon > 0$ is an arbitrary small number.

Proof. The total number of solutions is written in terms of characteristic function for primitive roots, see Lemma 9.2, and the characteristic function for squarefree integers, see Lemma 2.2, as

$$\begin{aligned}
\sum_{n \in \mathbb{F}_p} \Psi(n)\, \mu^2(n) &= \sum_{n \in \mathbb{F}_p}\left(\frac{\mu^2(n)}{p} \sum_{\substack{\gcd(m,p-1)=1 \\ 0 \leq u \leq p-1}} \psi\left((\tau^m - n)u\right)\right) \\
&= M_2(p) + E_2(p).
\end{aligned} \tag{154}$$

The main term $M_2(p)$ is determined by the index $u = 0$, and the error term $E_2(p)$ is determined by the index $u \neq 0$. Applying Lemma 11.5 to the main term and Lemma 12.4 to the error term, yield

$$\begin{aligned}
N_2(p) &= M_2(p) + E_2(p) \\
&= \prod_{q \geq 2}\left(1 - \frac{1}{q^2}\right)\left(\frac{\varphi(p-1)}{p}\right)p + O\left(p^{1/2}\right) + O(p^{1-\varepsilon}) \\
&= \prod_{q \geq 2}\left(1 - \frac{1}{q^2}\right)\left(\frac{\varphi(p-1)}{p}\right)p + O(p^{1-\varepsilon}) \\
&> 0,
\end{aligned} \tag{155}$$

for all sufficently large primes $p \geq 2$, and an arbitrary small number $\varepsilon > 0$. ■

17.3 Squarefree Twin Primitive Roots

Let $p \geq 2$ be a large prime, and let $\tau \in \mathbb{F}_p$ be a primitive root. Each squarefree twin primitive roots $n + a_0$ and $n + a_1$ is a solution of the systems of equations

1. $\tau^{n_0} = n + a_0, \quad \tau^{n_1} = n + a_1,$ the primitive root condition.
2. $\mu^2(n + a_0) = 1, \quad \mu^2(n + a_1) = 1,$ the squarefree condition.

A solution is a triple $(n, n_0, n_1) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ such that $\gcd(n_i, p-1) = 1$ for $i = 0, 1$. Let

$$N_2(2, p) = \#\left\{n \in \mathbb{F}_p : \operatorname{ord}_p(n + a_i) = p-1, \text{ and } \mu^2(n + a_i) = 1\right\} \tag{156}$$

for $i = 0, 1$, denotes the number of solutions.

Theorem 17.2. *For any large prime $p \geq 2$, the finite field $\mathbb{F}_p$ contains 2 consecutive squarefree primitive roots. Furthermore, the number of pairs has the asymptotic formula*

$$N_2(2,p) = \prod_{q \geq 2} \left(1 - \frac{2}{q^2}\right) \left(\frac{\varphi(p-1)}{p-1}\right)^2 p + O(p^{1-\varepsilon}), \tag{157}$$

where $\varepsilon > 0$ is an arbitrary small number. The simplest case is for $a_0 = 0, a_1 = 1$.

Proof. The total number of solutions is written in terms of characteristic function for primitive roots, see Lemma 9.2, and the characteristic function for squarefree integers, see Lemma 2.2, as

$$\begin{aligned} \mathbb{N}_2(2,p) &= sum_{n \in \mathbb{F}_p} \Psi\left(n + a_0\right) \Psi\left(n + a_1\right) \mu^2(n + a_0) \mu^2(n + a_1) \qquad (158) \\ &= \sum_{n \in \mathbb{F}_p} \left(\frac{\mu^2(n + a_0)}{p} \sum_{\substack{\gcd(n_0, p-1) = 1 \\ 0 \leq u_0 \leq p-1}} \psi\left((\tau^{n_0} - n - a_0) u_0\right) \right) \\ &\quad \times \left(\frac{\mu^2(n + a_1)}{p} \sum_{\substack{\gcd(n_1, p-1) = 1 \\ 0 \leq u_1 \leq p-1}} \psi\left((\tau^{n_1} - n - a_1) u_1\right) \right) \\ &= M_2(2,p) + E_2(2,p). \end{aligned}$$

The main term $M_2(2,p)$ is determined by the indices $u_0 = u_1 = 0$, and the error term $E_2(2,p)$ is determined by the indices $u_0 \neq 0, u_1 \neq 0$. Applying Lemma 11.3 to the main term and Lemma 12.4 to the error term, yield

$$\begin{aligned} N_2(2,p) &= M_2(2,p) + E_2(2,p) \qquad (159) \\ &= \prod_{q \geq 2} \left(1 - \frac{2}{q^2}\right) \left(\frac{\varphi(p-1)}{p-1}\right)^2 p + O\left(p^{2/3}\right) + O(p^{1-\varepsilon}) \\ &= \prod_{q \geq 2} \left(1 - \frac{2}{q^2}\right) \left(\frac{\varphi(p-1)}{p-1}\right)^2 p + O(p^{1-\varepsilon}) \\ &> 0, \end{aligned}$$

for all sufficently large primes $p \geq 2$, and an arbitrary small number $\varepsilon > 0$. ■

17.4 Squarefree Triple Primitive Roots

Let $p \geq 2$ be a large prime, and let $\tau \in \mathbb{F}_p$ be a primitive root. Each squarefree triple primitive roots $n + a_0$, $n + a_1$, and $n + a_2$ is a solution of the systems of equations

1. $\tau^{n_0} = n + a_0, \quad \tau^{n_1} = n + a_1, \quad \tau^{n_2} = n + a_2,$ the primitive root condition.
2. $\mu^2(n + a_0) = 1, \quad \mu^2(n + a_1) = 1, \quad \mu^2(n + a_2) = 1,$ the squarefree condition.

A solution is a triple $(n, n_0, n_1, n_2) \in \mathbb{N}^4$ such that $\gcd(n_i, p-1) = 1$ for $i = 0, 1, 2$. Let

$$N_2(3,p) = \#\left\{n \in \mathbb{F}_p : \operatorname{ord}_p(n + a_i) = p - 1, \text{ and } \mu^2(n + a_i) = 1\right\} \tag{160}$$

for $i = 0, 1, 2$, denotes the number of solutions.

Theorem 17.3. *For any large prime $p \geq 2$, the finite field $\mathbb{F}_p$ contains 3 consecutive squarefree primitive roots. Furthermore, the number of pairs has the asymptotic formula*

$$N_2(3,p) = \prod_{q \geq 2} \left(1 - \frac{3}{q^2}\right) \left(\frac{\varphi(p-1)}{p-1}\right)^3 p + O(p^{1-\varepsilon}), \tag{161}$$

where $\varepsilon > 0$ is an arbitrary small number.

Proof. The simplest case is for $a_0 = 0, a_1 = 1, a_2 = 2$. The total number of solutions is written in terms of characteristic function for primitive roots, see Lemma 9.2, and the characteristic function for squarefree integers, see Lemma 2.2, as

$$\begin{aligned}
N_2(3,p) &= \sum_{n\in\mathbb{F}_p} \Psi(n)\,\Psi(n+1)\,\Psi(n+2)\,\mu^2(n)\mu^2(n+1)\mu^2(n+2) \qquad (162)\\
&= \sum_{n\in\mathbb{F}_p}\left(\frac{\mu^2(n)}{p}\sum_{\substack{\gcd(n_0,p-1)=1\\0\le u_0\le p-1}}\psi\left((\tau^{n_0}-n)u_0\right)\right)\\
&\quad\times\left(\frac{\mu^2(n+1)}{p}\sum_{\substack{\gcd(n_1,p-1)=1\\0\le u_1\le p-1}}\psi\left((\tau^{n_1}-n-1)u_1\right)\right)\\
&\quad\times\left(\frac{\mu^2(n+1)}{p}\sum_{\substack{\gcd(n_2,p-1)=1\\0\le u_2\le p-1}}\psi\left((\tau^{n_2}-n-2)u_2\right)\right)\\
&= M_2(3,p)+E_2(3,p). \qquad (163)
\end{aligned}$$

The main term $M_2(3,p)$ is determined by the indices $u_0 = u_1 = u_2 = 0$, and the error term $E_2(3,p)$ is determined by the indices $u_0 \neq 0, u_1 \neq 0, u_2 \neq 0$. Applying Lemma 11.4 to the main term and Lemma 12.4 to the error term, yield

$$\begin{aligned}
N_2(3,p) &= M_2(3,p)+E_2(3,p) \qquad (164)\\
&= \prod_{q\ge 2}\left(1-\frac{3}{q^2}\right)\left(\frac{\varphi(p-1)}{p-1}\right)^3 p + O\left(p^{2/3}\right) + O(p^{1-\varepsilon})\\
&= \prod_{q\ge 2}\left(1-\frac{3}{q^2}\right)\left(\frac{\varphi(p-1)}{p-1}\right)^3 p + O(p^{1-\varepsilon})\\
&> 0,
\end{aligned}$$

for all sufficiently large primes $p \geq 2$, and an arbitrary small number $\varepsilon > 0$. ■

18 Consecutive s-Power Free Primitive Roots

18.1 s-Power Free Primitive Roots

Let $p \geq 2$ be a large prime, and let $\tau \in \mathbb{F}_p$ be a primitive root. A s-power free primitive root $n \in \mathbb{F}_p$ exists if and only if the system of equations

$$\tau^m = n \quad \text{and} \quad \mu_s(n) = 1, \qquad (165)$$

has one or more solutions $(m,n) \in \mathbb{N}\times\mathbb{N}$ such that $\gcd(m,p-1) = 1$, and $n \geq 2$. Let

$$N_s(p) = \#\left\{n \in \mathbb{F}_p : \operatorname{ord}_p(n) = p-1, \mu_s(n) = \pm 1\right\}, \qquad (166)$$

see Lemma 2.2, denotes the number of solutions.

Theorem 18.1. *Let $s \geq 2$ be a fixed integer. For any large prime $p \geq 2$, the finite field $\mathbb{F}_p$ contains squarefree primitive roots. Furthermore, the total number has the asymptotic formula*

$$N_s(p) = \prod_{q\ge 2}\left(1-\frac{1}{q^s}\right)\left(\frac{\varphi(p-1)}{p-1}\right)p + O(p^{1-\varepsilon}), \qquad (167)$$

where $\varepsilon > 0$ is an arbitrary small number.

Proof. (Theorem 1.4): The total number of solutions is written in terms of characteristic function for primitive roots, see Lemma 9.2, and the characteristic function for s-power free integers, see Lemma 2.2, as

$$\begin{aligned}\sum_{n\in\mathbb{F}_p}\Psi(n)\,\mu_s(n) &= \sum_{n\in\mathbb{F}_p}\left(\frac{\mu_s(n)}{p}\sum_{\substack{\gcd(n,p-1)=1\\0\le u\le p-1}}\psi\left((\tau^n-n)u\right)\right)\\ &= M_s(p)+E_s(p).\end{aligned}\tag{168}$$

The main term $M_s(p)$ is determined by the indices $u=0$, and the error term $E_s(p)$ is determined by the indices $u\neq 0$. Applying Lemma 11.5 to the main term and Lemma 12.4 to the error term, yield

$$\begin{aligned}N_s(p) &= M_s(p)+E_s(p) \qquad (169)\\ &= \prod_{q\ge 2}\left(1-\frac{1}{q^s}\right)\left(\frac{\varphi(p-1)}{p-1}\right)p+O\left(p^{1/s}\right)+O(p^{1-\varepsilon})\\ &= \prod_{q\ge 2}\left(1-\frac{1}{q^s}\right)\left(\frac{\varphi(p-1)}{p-1}\right)p+O(p^{1-\varepsilon})\\ &> 0,\end{aligned}$$

for all sufficiently large primes $p\ge 2$, and an arbitrary small number $\varepsilon>0$. ■

18.2 s-Power Free Twin Primitive Roots

Given a triple of small integers $a_0\neq a_1$ and $s\ge 2$. Let $p\ge 2$ be a large prime, and let $\tau\in\mathbb{F}_p$ be a primitive root. Each string of 2 consecutive s-powerfree primitive roots $n+a_0$ and $n+a_1$ is a solution of the systems of equations:

1. $\tau^{n_0}=n+a_0,\quad \tau^{n_1}=n+a_1;$ the primitive root condition.
2. $\mu_s(n+a_0)=1,\quad \mu_s(n+a_1)=1;$ the s-power free condition.

A solution is a triple $(n,n_0,n_1)\in\mathbb{N}\times\mathbb{N}\times\mathbb{N}$, with $\gcd(n_i,p-1)=1$, for $i=0,1$. Let

$$N_s(2,p,a)=\#\left\{n\in\mathbb{F}_p:\operatorname{ord}_p(n+a_i)=p-1,\text{ and }\mu_s(n+a_i)=\pm 1\right\},\tag{170}$$

for $i=0,1$, denotes the number of solutions.

Proof. (Theorem 1.5): The total number of solutions is written in terms of characteristic function for primitive roots, see Lemma 9.2, and the characteristic function for squarefree integers, see Lemma 2.2, as

$$\begin{aligned}N_s(2,p) &= \sum_{n\in\mathbb{F}_p}\Psi(n+a_0)\,\Psi(n+a_1)\,\mu_s(n+a_0)\mu_s(n+a_1)\\ &= \sum_{n\in\mathbb{F}_p}\left(\frac{\mu_s(n+a_0)}{p}\sum_{\substack{\gcd(n_0,p-1)=1\\0\le u_0\le p-1}}\psi\left((\tau^{n_0}-n-a_0)u_0\right)\right)\\ &\quad\times\left(\frac{\mu_s(n+a)}{p}\sum_{\substack{\gcd(n_1,p-1)=1\\0\le u_1\le p-1}}\psi\left((\tau^{n_1}-n-a_1)u_1\right)\right)\\ &= M_s(2,p)+E_s(2,p).\end{aligned}\tag{171}$$

The main term $M_s(2,p)$ is determined by the indices $u_0 = u_1 = 0$, and the error term $E_s(2,p)$ is determined by the indices $u_0 \neq 0, u_1 \neq 0$. Applying Lemma 11.6 to the main term and Lemma 12.4 to the error term, yield

$$\begin{aligned} N_s(2,p) &= M_s(2,p) + E_s(2,p) \\ &= \prod_{q \geq 2} \left(1 - \frac{\rho(s)}{q^s}\right) \left(\frac{\varphi(p-1)}{p-1}\right)^2 p + O\left(p^{\alpha(s)-\varepsilon}\right) + O(p^{1-\varepsilon}) \\ &= \prod_{q \geq 2} \left(1 - \frac{\rho(s)}{q^s}\right) \left(\frac{\varphi(p-1)}{p-1}\right)^2 p + O(p^{1-\varepsilon}) \\ &> 0, \end{aligned} \tag{172}$$

where $\rho(s) = 1, 2$, and $\varepsilon > 0$ is an arbitrary small number, for all sufficiently large primes $p \geq 2$. ■

19 Relatively Prime Primitive Roots

The first proof based on Lemma 9.1 and restricted to $q = p - 1$ was given in [27]. A new proof based on Lemma 9.2, and for any $q \leq p - 1$, is given here. The second result for consecutive and relatively prime to $q \geq 2$ appears to be a new result in the literature.

19.1 Relatively Prime Primitive Roots

Proof. (Theorem 1.6) For a large prime $p \geq 2$, the total number of primitive roots relatively prime to a fixed integer q is precisely

$$N_r(p,q) = \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1}} \Psi(n). \tag{173}$$

In terms of characteristic function for primitive roots, see Lemma 9.2, this is written as

$$\begin{aligned} N_r(p,q) &= \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1}} \Psi(n) \\ &= \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1}} \left(\frac{1}{p} \sum_{\gcd(m,p-1)=1,} \sum_{0 \leq u \leq p-1} \psi\left((\tau^m - n)u\right) \right) \\ &= \frac{1}{p} \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1}} \sum_{\gcd(m,p-1)=1} 1 + \frac{1}{p} \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1}} \sum_{\gcd(m,p-1)=1,} \sum_{0 < u \leq p-1} \psi\left((\tau^m - n)u\right) \\ &= M_r(p,q) + E_r(p,q). \end{aligned} \tag{174}$$

The main term $M_r(p,q)$ is determined by a finite sum over the trivial additive character $\psi = 1$, and the error term $E_r(p,q)$ is determined by a finite sum over the nontrivial additive characters $\psi(t) = e^{i2\pi t/p} \neq 1$. Applying Lemma 11.7 to the main term and Lemma 12.1 to the error term, yield

$$\begin{aligned} N_r(p,q) &= M_r(p,q) + E_r(p,q) \\ &= \frac{\varphi(q)}{q} \frac{\varphi(p-1)}{p-1} p + O(\log^2 p) + O(p^{1-\varepsilon}) \\ &= \frac{\varphi(q)}{q} \frac{\varphi(p-1)}{p-1} p + O(p^{1-\varepsilon}) \\ &> 0, \end{aligned} \tag{175}$$

for all sufficiently large primes $p \geq 2$, and an arbitrary small number $\varepsilon > 0$. ■

19.2 Relatively Prime Twin Primitive Roots

The dependence correction factor $c_2(q,a) \geq 0$, and the parameter $q = q(a)$ depends on $a \geq 1$. For instance, for $a = 1$, the value $q = q(a)$ must be odd, and $c_2(q,a) > 0$, otherwise $c_2(q,a) = 0$ for even q. Basically, the vanishing and nonvanishing are described in these cases:

$$c_2(q,a) = \begin{cases} > 0 & \text{if } a = 2b+1, \text{ and } q = 2c+1, \text{ with } b \geq 0, c \geq 0, \\ = 0 & \text{if } a = 2b+1, \text{ and } q = 2c, \text{ with } b \geq 0, c \geq 1, \\ > 0 & \text{if } a = 2b, \text{ and } q \geq 1, \text{ with } b \geq 1. \end{cases} \tag{176}$$

To continue the analysis, assume that the parameters $a \geq 1$ and $q \geq 1$ are admissible, and $c_2(q,a) > 0$. Let $p \geq 2$ be a large prime, and let $\tau \in \mathbb{F}_p$ be a primitive root. Each pair of quasi consecutive primitive roots n, $n+a$ and relatively prime to $q = q(a) \geq 2$ is a solution of the systems of equations:

1. $\tau^{n_0} = n, \quad \tau^{n_1} = n + a;$ the primitive root condition.
2. $\gcd(n,q) = 1, \quad \gcd(n+a,q) = 1.$ the relatively prime condition.

A solution is a triple $(n, n_0, n_1) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$, with $\gcd(n_i, p-1) = 1$, for $i = 0, 1$. Let

$$N_r(2,p,q) = \# \{n \in \mathbb{F}_p : \operatorname{ord}_p(n) = \operatorname{ord}_p(n+a) = p-1, \gcd(n,q) = \gcd(n+1,q) = 1\} \tag{177}$$

denotes the number of solutions.

Proof. (Theorem 1.7): For a large prime $p \geq 2$, the total number of pairs of quasi consecutive primitive roots, both relatively prime to a fixed integer $q \geq 2$, is precisely

$$N_r(2,p,q) = \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1 \\ \gcd(n+a,q)=1}} \Psi(n)\Psi(n+a). \tag{178}$$

In terms of characteristic function for primitive roots, see Lemma 9.2, this is written as

$$\begin{aligned} N_r(2,p,q) &= \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1 \\ \gcd(n+a,q)=1}} \left(\frac{1}{p} \sum_{\substack{0 \leq u \leq p-1 \\ \gcd(c,p-1)=1}} \psi\left((\tau^c - n)u\right) \right) \left(\frac{1}{p} \sum_{\substack{0 \leq v \leq p-1 \\ \gcd(d,p-1)=1}} \psi\left((\tau^d - n - a)v\right) \right) \\ &= M_r(2,p,q) + E_r(2,p,q). \end{aligned} \tag{179}$$

The main term $M_r(2,p,q)$, which is determined by the indices $u = v = 0$, has the form

$$M_s(2,p,q) = \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1 \\ \gcd(n+a,q)=1}} \left(\frac{1}{p} \sum_{\substack{0 \leq u \leq p-1 \\ \gcd(c,p-1)=1}} 1 \right) \left(\frac{1}{p} \sum_{\substack{0 \leq v \leq p-1 \\ \gcd(d,p-1)=1}} 1 \right), \tag{180}$$

and the error term $E_r(2,p,q)$, which is determined by the indices $u \neq 0, v \neq 0$, has the form

$$E_r(2,p,q) = \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1 \\ \gcd(n+a,q)=1}} \left(\frac{1}{p} \sum_{\substack{1 \leq u \leq p-1 \\ \gcd(c,p-1)=1}} \psi\left((\tau^c - n)u\right) \right) \left(\frac{1}{p} \sum_{\substack{1 \leq v \leq p-1 \\ \gcd(d,p-1)=1}} \psi\left((\tau^d - n - a)v\right) \right). \tag{181}$$

Applying Lemma 11.8 to the main term and Lemma 12.2 to the error term, yield

$$\begin{aligned} N_r(2,p,q) &= M_r(2,p,q)+E_r(2,p,q) \qquad (182)\\ &= c_2(q,a)\left(\frac{\varphi(q)}{q}\right)^2\frac{\varphi(p-1)}{p-1}p+O(p^{\varepsilon})+O(p^{1-\varepsilon})\\ &= c_2(q,a)\left(\frac{\varphi(q)}{q}\right)^2\frac{\varphi(p-1)}{p-1}p+O(p^{1-\varepsilon})\\ &> 0, \end{aligned}$$

where $c_2(q,a)>0$ is a dependence correction factor with respect to an admissible pair $a,q\geq 1$, for all sufficiently large primes $p\geq 2$, and an arbitrary small number $\varepsilon>0$. ■

20 Squarefree And Relatively Prime Primitive Roots

The first result for squarefree and relatively prime primitive roots with respect to a fixed integer $q\leq p-1$ is given here. The second result for squarefree and relatively prime twin primitive roots n, $n+a$ with respect to a fixed integer $q\geq 2$, and conditional on Conjecture 4.1, is a new result in the literature.

20.1 Squarefree And Relatively Prime Primitive Roots

Theorem 20.1. *Let $p\geq 2$ be a large prime, and let $q=O(\log p)$ be an integer. Then, the finite field $\mathbb{F}_p$ contains squarefree primitive roots relatively prime to $q\geq 2$. Furthermore, the number of such elements has the asymptotic formula*

$$N_{sr}(p,q)=\frac{6}{\pi^2}\prod_{p\nmid q}\left(1+\frac{1}{p}\right)^{-1}\frac{\varphi(p-1)}{p-1}p+O(p^{1-\varepsilon}), \qquad (183)$$

where $\varepsilon>0$ is an arbitrary small number.

Proof. For a large prime $p\geq 2$, the total number of primitive roots relatively prime to a fixed integer $q<p$ is precisely

$$N_{sr}(p,q)=\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1}}\Psi(n)\mu(n)^2. \qquad (184)$$

In terms of characteristic function for primitive roots, see Lemma 9.2, this is written as

$$\begin{aligned} N_r(p,q) &= \sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1}}\Psi(n)\mu(n)^2 \qquad (185)\\ &= \sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1}}\left(\frac{\mu(n)^2}{p}\sum_{\gcd(m,p-1)=1,\,0\leq u\leq p-1}\sum\psi\left((\tau^m-n)u\right)\right)\\ &= \frac{1}{p}\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1}}\sum_{\gcd(m,p-1)=1}\mu(n)^2+\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1}}\frac{\mu(n)^2}{p}\sum_{\gcd(m,p-1)=1,\,0<u\leq p-1}\sum\psi\left((\tau^m-n)u\right)\\ &= M_{sr}(p,q)+E_{sr}(p,q). \end{aligned}$$

The main term $M_{sr}(p,q)$ is determined by a finite sum over the trivial additive character $\psi=1$, and the error term $E_{sr}(p,q)$ is determined by a finite sum over the nontrivial additive characters $\psi(t)=e^{i2\pi t/p}\neq 1$. Applying Lemma 11.9 to the main term and Lemma 12.3 or Lemma 12.5 to the error term, yield

$$\begin{aligned} N_{sr}(p,q) &= M_{sr}(p,q)+E_{sr}(p,q) \\ &= \frac{6}{\pi^2}\prod_{p\nmid q}\left(1+\frac{1}{p}\right)^{-1}\frac{\varphi(p-1)}{p-1}p+O(p^{1/2})+O(p^{1-\varepsilon}) \\ &= \frac{6}{\pi^2}\prod_{p\nmid q}\left(1+\frac{1}{p}\right)^{-1}\frac{\varphi(p-1)}{p-1}p+O(p^{1-\varepsilon}) \\ &> 0, \end{aligned} \tag{186}$$

for all sufficiently large primes $p \geq 2$, and an arbitrary small number $\varepsilon > 0$. ■

20.2 Squarefree And Relatively Prime Twin Primitive Roots

The dependence correction factor $c_2(q,a) \geq 0$, and the parameter $q = q(a)$ depends on $a \geq 1$. Basically, the vanishing and nonvanishing are described in these cases:

$$c_2(q,a) = \begin{cases} >0 & \text{if } a=2b+1, \text{ and } q=2c+1, \text{ with } b\geq 0, c\geq 0, \\ =0 & \text{if } a=2b+1, \text{ and } q=2c, \text{ with } b\geq 0, c\geq 1, \\ >0 & \text{if } a=2b, \text{ and } q\geq 1, \text{ with } b\geq 1. \end{cases} \tag{187}$$

To continue the analysis, assume that the parameters $a \geq 1$ and $q \geq 1$ are admissible, and $c_2(q,a) > 0$. Let $p \geq 2$ be a large prime, and let $\tau \in \mathbb{F}_p$ be a primitive root. Each pair of squarefree twin primitive roots n, $n+a$ and relatively prime to $q = q(a) \geq 2$ is a solution of the systems of equations:

1. $\tau^{n_0} = n, \quad \tau^{n_1} = n+a;$ — the primitive root condition.
2. $\mu(n)^2, \quad \mu(n+a)^2;$ — the squarefree condition.
3. $\gcd(n,q)=1, \quad \gcd(n+a,q)=1.$ — the relatively prime condition.

A solution is a triple $(n, n_0, n_1) \in \mathbb{N}\times\mathbb{N}\times\mathbb{N}$, with $\gcd(n_i, p-1) = 1$, for $i = 0, 1$. Let

$$N_{sr}(2,p,q) = \#\{n \in \mathbb{F}_p : \text{Conditions 1, 2, and 3 are satisfied.}\} \tag{188}$$

denotes the number of solutions.

Theorem 20.2. *Assume Conjecture* 4.1. *Let $p \geq 2$ be a large prime, let $a \geq 1$ and $q = O(\log p)$ be a pair of integers. Then, the finite field $\mathbb{F}_p$ contains a pair n and $n+a$ of squarefree primitive roots and relatively prime to $q \geq 2$. Furthermore, the number of such pairs has the asymptotic formula*

$$N_{sr}(2,p,q) = c_2(q,a)\prod_{p\nmid q}\left(1+\frac{1}{p}\right)^{-2}\prod_{p\geq 2}\left(1-\frac{2}{p^2}\right)\left(\frac{\varphi(p-1)}{p}\right)^2 p+O(p^{1-\varepsilon}), \tag{189}$$

where $c_2(q,a) > 0$ is a dependence correction factor, and $\varepsilon > 0$ is an arbitrary small number.

Proof. For a large prime $p \geq 2$, the total number of squarefree twin primitive roots, both relatively prime to a fixed integer $q \geq 2$, is precisely

$$N_{sr}(2,p,q) = \sum_{\substack{n\in\mathbb{F}_p \\ \gcd(n,q)=1 \\ \gcd(n+a,q)=1}} \Psi(n)\Psi(n+a)\mu(n)^2\mu(n+a)^2. \tag{190}$$

In terms of characteristic function for primitive roots, see Lemma 9.2, this is written as

$$\begin{aligned} N_{sr}(2,p,q) &= \sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1\\ \gcd(n+a,q)=1}} \left(\frac{\mu(n)^2}{p} \sum_{\substack{0\le u\le p-1\\ \gcd(c,p-1)=1}} \psi\left((\tau^c-n)u\right)\right) \\ &\quad \times \left(\frac{\mu(n+a)^2}{p} \sum_{\substack{0\le v\le p-1\\ \gcd(d,p-1)=1}} \psi\left((\tau^d-n-a)v\right)\right) \\ &= M_{sr}(2,p,q)+E_{sr}(2,p,q). \end{aligned} \tag{191}$$

The main term $M_{sr}(2,p,q)$ is determined by the indices $u=v=0$, and has the form

$$M_s(2,p,q) = \sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1\\ \gcd(n+a,q)=1}} \left(\frac{1}{p} \sum_{\substack{0\le u\le p-1\\ \gcd(c,p-1)=1}} \mu(n)^2\right)\left(\frac{1}{p} \sum_{\substack{0\le v\le p-1\\ \gcd(d,p-1)=1}} \mu(n+a)^2\right), \tag{192}$$

and the error term $E_{sr}(2,p,q)$ is determined by the indices $u\ne 0, v\ne 0$, and has the form as (191). Applying Lemma 11.10 to the main term and Lemma 12.5 to the error term, yield

$$\begin{aligned} N_{sr}(2,p,q) &= M_{sr}(2,p,q)+E_{sr}(2,p,q) \\ &= c_2(q,a)\prod_{p\nmid q}\left(1+\frac{1}{p}\right)^{-2}\prod_{p\ge 2}\left(1-\frac{2}{p^2}\right)\left(\frac{\varphi(p-1)}{p}\right)^2 p + O\left(p^{1-\delta}\right)+O(p^{1-\varepsilon}) \\ &= c_2(q,a)\prod_{p\nmid q}\left(1+\frac{1}{p}\right)^{-2}\prod_{p\ge 2}\left(1-\frac{2}{p^2}\right)\left(\frac{\varphi(p-1)}{p}\right)^2 p + O(p^{1-\varepsilon}) \\ &> 0, \end{aligned} \tag{193}$$

where $c_2(q,a)>0$ is an admissible dependence correction factor, for all sufficiently large primes $p\ge 2$, and an arbitrary small number $\varepsilon>0$. ■

21 Probabilities For Consecutive Squarefree Primitive Roots

The forms of the main terms in Theorem 1.3 and Theorem 1.4 imply that a squarefree primitive root in a finite field $\mathbb{F}_p$ is a nearly independent random variable $X=X(p)$.

Definition 21.1. The probability of squarefree primitive roots in a finite field $\mathbb{F}_p$ is defined by

$$P\left(\operatorname{ord}_p(X)=p-1 \text{ and } \mu(X)^2\ne 0\right) = \frac{\varphi(p-1)}{p-1}\prod_{q\ge 2}\left(1-\frac{1}{q^2}\right)+O\left(\frac{1}{p^{\varepsilon}}\right), \tag{194}$$

where $\varepsilon>0$ is a small number.

Some calculations described below demonstrates that two or more consecutive squarefree primitive roots are dependent random variables.

Lemma 21.1. *Let $p\ge 2$ be a large prime. Let X_i be a random squarefree primitive root. Then, a pair of random consecutive squarefree primitive roots X_0, X_1 in a finite field $\mathbb{F}_p$ is a dependent random variable. Specifically, the probability of a pair of random consecutive squarefree primitive roots is*

$$\begin{aligned} &P(\operatorname{ord}(X_0)=p-1, \operatorname{ord}(X_1)=p-1 \text{ and } \mu(X_0)=\pm 1, \mu(X_1)=\pm 1) \\ &= \left(\frac{\varphi(p-1)}{p-1}\right)^2\prod_{q\ge 2}\left(1-\frac{2}{q^2}\right)+O\left(\frac{1}{p^{\varepsilon}}\right), \end{aligned} \tag{195}$$

where $\varepsilon>0$ is a small number.

Proof. The density constant in the main term of Theorem 17.2 is the probability of having two consecutive squafree primitive roots. Next, use a series of steps to reduces to a simpler product:

$$\begin{aligned}\left(\frac{\varphi(p-1)}{p-1}\right)^2\prod_{q\geq 2}\left(1-\frac{2}{q^2}\right) &= \left(\frac{\varphi(p-1)}{p-1}\right)^2\prod_{q\geq 2}\left(1-\frac{1}{q^2}\right)^2\left(1+\frac{1}{q^2(q^2-2)}\right)^{-1}\\ &< \left(\frac{\varphi(p-1)}{p-1}\right)^2\prod_{q\geq 2}\left(1-\frac{1}{q^2}\right)^2. \end{aligned}\tag{196}$$

The last line is product of the individual probabilities, which implies that the two properties of the consecutive random integers X_0, X_1 are independent. The reduction from independent events is measured by the dependence correction factor

$$c_2(2)=\prod_{q\geq 2}\left(1+\frac{1}{q^2(q^2-2)}\right)^{-1}=0.8729859534493136187717451 1\ldots. \tag{197}$$

■

Lemma 21.2. *Let $p\geq 2$ be a large prime. Let X_i be a random squarefree primitive root. Then, a triple of random consecutive squarefree primitive roots X_0, X_1, X_2 in a finite field $\mathbb{F}_p$ is a dependent random variable. Specifically, the probability of a triple of random consecutive squarefree primitive roots is*

$$\begin{aligned}&P(\operatorname{ord}(X_0)=\operatorname{ord}(X_1)=\operatorname{ord}(X_2)=p-1 \text{ and } \mu(X_0)=\pm 1,\mu(X_1)=\pm 1,\mu(X_2)=\pm 1)\\ =&\left(\frac{\varphi(p-1)}{p-1}\right)^3\prod_{q\geq 2}\left(1-\frac{3}{q^2}\right)+O\left(\frac{1}{p^{\varepsilon}}\right),\end{aligned}\tag{198}$$

where $\varepsilon>0$ is a small number.

Proof. The density constant in the main term of Theorem 17.2 is the probability of having two consecutive squafree primitive roots. Next, use a series of steps to reduces to a simpler product:

$$\begin{aligned}\left(\frac{\varphi(p-1)}{p-1}\right)^3\prod_{q\geq 2}\left(1-\frac{3}{q^2}\right) &= \left(\frac{\varphi(p-1)}{p-1}\right)^3\prod_{q\geq 2}\left(1-\frac{1}{q^2}\right)^3\left(1+\frac{3q^2-1}{q^4(q^2-3)}\right)^{-1}\\ &< \left(\frac{\varphi(p-1)}{p-1}\right)^3\prod_{q\geq 2}\left(1-\frac{1}{q^2}\right)^3. \end{aligned}\tag{199}$$

The last line is product of the individual probabilities, which implies that the two properties of the consecutive random integers X_0, X_1, X_2 are independent. The reduction from independent events is measured by the dependence correction factor

$$c_2(3)=\prod_{q\geq 2}\left(1+\frac{3q^2-1}{q^4(q^2-3)}\right)^{-1}=0.5585269791276891055333 30\ldots. \tag{200}$$

■

The pattern of the probability function for consecutive squarefree primitive roots breaks down for 4 consecutive squarefree primitive roots since $\left(1-\frac{4}{q^2}\right)=0$ at $q=2$.

22 Problems

Several interesting problems of different level of complexities are presented in this section. The range of difficulty ranges from easy to very difficult.

22.1 Least Consecutive Primitive Roots In Finite Fields

Exercise 22.1. Let $p \geq 2$ be a large prime, and let $k = 2$. Determine an asymptotic formula for the least pair of consecutive primitive roots n and $n+1$ in the finite field $\mathbb{F}_p$. Is the magnitude $n = O(\log^c p)$, where $c > 0$ is a constant, correct?

Exercise 22.2. Let $p \geq 2$ be a large prime, and let $k = 2$. Determine an asymptotic formula for the least pair of consecutive squarefree primitive roots n and $n+1$ in the finite field $\mathbb{F}_p$. Is the magnitude $n = O(\log^c p)$, where $c > 0$ is a constant, correct?

Exercise 22.3. Let $p \geq 2$ be a large prime, and let $k = 3$. Determine an asymptotic formula for the least pair of consecutive primitive roots n, $n+1$, and $n+2$ in the finite field $\mathbb{F}_p$. Is the magnitude $n = O(\log^c p)$, where $c > 0$ is a constant, correct?

Exercise 22.4. Let $p \geq 2$ be a large prime, and let $k = 3$. Determine an asymptotic formula for the least pair of consecutive squarefree primitive roots n, $n+1$, and $n+2$ in the finite field $\mathbb{F}_p$. Is the magnitude $n = O(\log^c p)$, where $c > 0$ is a constant, correct?

Exercise 22.5. Show that there are infinitely many admissible 4-tuples (a_0, a_1, a_2, a_3), and each one generates infinitely many squarefree integers 4-tuples $(n+a_0, n+a_1, n+a_2, n+a_3)$ as $n \to \infty$. For example, $(n, n+1, n+3, n+5)$, with $n \geq 1$.

22.2 Simultaneous Primitive Root In Finite Fields

Exercise 22.6. Let $p \geq 2$ and $q \geq 2$ be large distinct primes. Develop an algorithm for computing a simultaneous primitive root $u \neq \pm 1, v^2$ modulo p and modulo q.

Exercise 22.7. Let $p \geq 2$, $q \geq 2$, and $r \geq 2$ be large distinct primes. Develop an algorithm for computing a simultaneous primitive root $u \neq \pm 1, v^2$ modulo p modulo q, and r.

22.3 Consecutive And Relatively Prime Primitive Roots

Exercise 22.8. Let $p \geq 2$ be a large prime, and let $q \geq 1$ be a fixed integer. Prove that there are infinitely many consecutive prime primitive roots and relatively prime to q. Determine an asymptotic formula for the number of $k \geq 3$ consecutive primitive roots n, $n+a$, and $n+b$ in the finite field $\mathbb{F}_p$ and relatively prime to q.

Exercise 22.9. Let $p \geq 2$ be a large prime, and let $q \geq 1$ be a fixed integer. Prove a result on the distribution of pairs of consecutive primitive roots relatively prime to q.

Exercise 22.10. Let $p \geq 2$ be a large prime, and let $B \geq 1$ be a fixed integer. Prove the existence of pairs of consecutive smooth primitive roots relative to B.

22.4 Summatory Functions And Primitive Roots

Exercise 22.11. Let $s \in \mathbb{Z}$ be a fixed integer, and let $p \geq 1$ be a prime. Evaluate the finite sum

$$\sum_{n<p} \Psi(n) n^s.$$

.

Exercise 22.12. Let $s \in \mathbb{Z}$ be a fixed integer, and let $p \geq 1$ be a prime. Evaluate the finite sum

$$\sum_{n<p} \Psi(n) n^s \mu(n).$$

.

22.5 Length Merit Factor

Exercise 22.13. Determine the an effective upper bound $C > 0$ for the length merit factor $m = k/\log p \leq C$ for all primes $p \geq 2$, see Definition 14.1.

Exercise 22.14. Compute a table of the length merit factor $m = k/\log p$ indexed by the primes $p \leq 1000$. .

Exercise 22.15. Compute a table of the length merit factor $m = k/\log p$ indexed by the length $k \leq 50$.

References

[1] Julia Brandes. *Twins of s-free numbers*. arXiv:1307.2066.

[2] William D. Banks, Tristan Freiberg, Caroline L. Turnage-Butterbaugh. *Consecutive primes in tuples,* arXiv:1311.7003.

[3] Berndt, Bruce C.; Evans, Ronald J.; Williams, Kenneth S. *Gauss and Jacobi sums.* Canadian Math. Soc. Series of Monographs. A Wiley-Interscience Publication. New York, 1998.

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

[5] Caldwell, Chris K.; Gallot, Yves. *On the primality of $n! \pm 1$ and $2 \times 3 \times 5 \times \cdots \times p \pm 1$*. Math. Comp. 71 (2002), no. 237, 441-448.

[6] Carlitz, L. *Sets of primitive roots.* Compositio Math. 13 (1956), 65-70.

[7] L. Carlitz. *On a problem in additive arithmetic*, Quart. J. Math., 3, (1932), 273-290.

[8] N. A. Carella. *Primitive Roots In Short Intervals*, arXiv:1806.01150.

[9] Crandall, Richard; Pomerance, Carl. *Prime numbers. A computational perspective*. Second edition. Springer, New York, 2005.

[10] Cohen, Stephen D. *Consecutive primitive roots in a finite field*. Proc. Amer. Math. Soc. 93 (1985), no. 2, 189-197.

[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] De Koninck, Jean-Marie; Luca, Florian. *Analytic number theory. Exploring the anatomy of integers*. Graduate Studies in Mathematics, 134. American Mathematical Society, Providence, RI, 2012.

[14] De Koninck, J. M.; Katai, I. *On the mean value of the index of composition of an integer*. Monatsh. Math. 145 (2005), no. 2, 131-144.

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

[16] Paul Erdos, 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] Guy, Richard K. *The Strong Law of Small Numbers.* American Mathematical Monthly. 95 (8): 697-712, 1988.

[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,* arXiv:math/0504026.

[23] Gun, S.; Luca, Florian; Rath, P.; Sahu, B.; Thangadurai, R. *Distribution of residues modulo p*. Acta Arith. 129 (2007), no. 4, 325-333.

[24] Hall, R. R. *Squarefree numbers on short intervals*. Mathematika 29 (1982), no. 1, 7-17.

[25] Hooley, C. *A note on square-free numbers in arithmetic progressions*, Bull. Lond. Math. Soc. 7 (1975), 133-138.

[26] Hall, R. R. *Squarefree numbers on short intervals*. Mathematika 29 (1982), no. 1, 7-17.

[27] Hausman, Miriam. *Primitive roots satisfying a co-prime condition*. Amer. Math. Monthly 83 (1976), no. 9, 720-723.

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

[29] Ivic, Aleksandar. *The Riemann zeta-function. Theory and applications*. Wiley, New York; Dover Publications, Inc., Mineola, NY, 2003.

[30] 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.

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

[32] Languasco, A.; Zaccagnini, A. *A note on Mertens' formula for arithmetic progressions.* J. Number Theory 127 (2007), no. 1, 37-46.

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

[34] Luca, Florian; Shparlinski, Igor E.; Thangadurai, R. *Quadratic non-residues versus primitive roots modulo p*. J. Ramanujan Math. Soc. 23 (2008), no. 1, 97-104.

[35] Ingela Mennema. *The distribution of consecutive square-free numbers*, Master Thesis, Leiden University, 2017.

[36] Mirsky, L. *Note on an asymptotic formula connected with r-free integers*. Quart. J. Math., Oxford Ser. 18, (1947). 178-182.

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

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

[39] 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.

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

[41] Ramon M. Nunes. *Square-free numbers in arithmetic progressions,* arXiv:1402.0684.

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

[43] Overholt, Marius. *A course in analytic number theory*. Graduate Studies in Mathematics, 160. American Mathematical Society, Providence, RI, 2014.

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

[45] Pappalardi, Francesco. *A survey on k-freeness*. Number theory, 71-88, Ramanujan Math. Soc. Lect. Notes Ser., 1, Ramanujan Math. Soc., Mysore, 2005.

[46] Orr, Richard C. *Remainder estimates for squarefree integers in arithmetic progression*. J. Number Theory 3 1971 474-497.

[47] T. Reuss. *Pairs of k-free Numbers, consecutive square-full Numbers*. arXiv:1212.3150.

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

[49] Rudnick, Zeev; Zaharescu, Alexandru. *The distribution of spacings between small powers of a primitive root*. Israel J. Math. 120 (2000), part A, 271-287.

[50] Szalay, Michael. *On the distribution of the primitive roots of a prime.* J. Number Theory 7 (1975), 184-188.

[51] 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.

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

[53] Shoup, Victor. *A computational introduction to number theory and algebra*. Cambridge University Press, Cambridge, 2005.

[54] Tsang, Kai Man. *The distribution of r-tuples of squarefree numbers*. Mathematika 32 (1985), no. 2, 265-275 (1986).

[55] Tanti, Jagmohan; Thangadurai, R. *Distribution of residues and primitive roots*. Proc. Indian Acad. Sci. Math. Sci. 123 (2013), no. 2, 203-211.

[56] Vegh, Emanuel. *Pairs of consecutive primitive roots modulo a prime*. Proc. Amer. Math. Soc. 19 (1968), 1169-1170.

[57] Vegh, Emanuel. *Primitive roots modulo a prime as consecutive terms of an arithmetic progression.* J. Reine Angew. Math. 235 (1969), 185-188.

[58] R. Warlimont. *Squarefree numbers in arithmetic progressions*, J. London Math. Soc. (2)22(1980), 21-24.

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

ConsecutivePrimitiveRoots-10-0-19-47.tex.