2021

Topics In Analytic Number Theory And Consecutive Primitive Roots

Nelson Carella
CUNY Bronx Community College

Topics In Analytic Number Theory And Consecutive Primitive Roots

N. A. Carella

Contents

Chapter 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

$$n + a_0, \quad n + a_1, \quad n + a_2, \quad \ldots, \quad n + a_k, \tag{1.1}$$

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

$$\sum_{n \in \mathbb{F}_p} \Psi(n+a_0)\,\Psi(n+a_1)\cdots\Psi(n+a_k)\,f(n+a_0)\,f(n+a_1)\cdots f(n+a_k), \tag{1.2}$$

and

$$\sum_{n \in \mathcal{A}} \Psi(n+a_0)\,\Psi(n+a_1)\cdots\Psi(n+a_k)\,f(n+a_0)\,f(n+a_1)\cdots f(n+a_k), \tag{1.3}$$

respectively, where $\Psi : \mathbb{N} \longrightarrow \{0,1\}$ is the characteristic function of primitive roots modulo p, see Section 13, 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 seems to be that in [12] 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 12.2. Later, a qualitative result for the existence of some consecutive primitive roots was proved in [115]. A quantitative and weaker result for two consecutive primitive roots is proved in [107], the same result, but emphasizing the numerical aspects, is also

proved in [19]. More recently, some partial result but no proof for k-consecutive primitive roots appears in [114].

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*

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

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

The complete proof for this case is given in Section 17.1.

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*

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

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 16.1. 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 18.1. A result for two consecutive squarefree primitive roots n and $n+1$ in a finite field $\mathbb{F}_p$ is given in Theorem 18.2 and a result for three consecutive squarefree primitive roots n, $n+1$ and $n+2$ is given in Theorem 18.3. The next case for four squarefree primitive roots n, $n+1$, $n+2$ and $n+3$ is not feasible, see (3.1). 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*

$$n + a_0, \quad n + a_1, \quad n + a_2, \quad \ldots, \quad n + a_k.$$

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

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

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

The complete proof for this case is given in Section 17.3.

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*

$$N_s(p) = \frac{1}{\zeta(s)} \frac{\varphi(p-1)}{p-1} p + O(p^{1-\varepsilon}), \tag{1.4}$$

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*

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

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

The complete proofs for these cases are given in Section 19.1.

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 [60] using the divisors dependent characteristic function in Lemma 12.2. A generalized version for $q \leq p-1$, using the divisors free characteristic function in Lemma 12.3, 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*

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

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*

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

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 20.1 and Section 20.2 respectively.

Chapter 2

The Prime Divisors Counting Functions

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

2.1 Prime Divisors Counting Function

The symbols $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ and $\mathbb{P} = \{2, 3, 5, \ldots\}$ denote the sets of natural numbers, the set of integers, and the set of prime numbers respectively. 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

$$\omega(n) = \sum_{p|n} 1.$$

Definition 2.2. The prime power divisors counting function $\Omega : \mathbb{N} \longrightarrow \mathbb{N}$ is defined by

$$\Omega(n) = \sum_{p^v|n} 1.$$

The former is not sensitive to the multiplicity of each prime $p \mid n$, but the latter does count the multiplicity of each prime $p \mid n$.

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

Both of these results are standard results in analytic number theory, see [87, Theorem 2.6].

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

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

$$\text{(ii)} \quad \sum_{\substack{n \le x \\ n \equiv a \bmod q}} \left(\omega(n) - \varphi(q)^{-1} \log\log x\right)^2 \le \frac{C(a,q)}{\varphi(q)} x \log\log x,$$

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

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

$$\begin{aligned} \sum_{\substack{n \le x \\ n \equiv a \bmod q}} \omega(n) &= \sum_{\substack{p \le x \\ p \equiv a \bmod q}} \sum_{k \le x/p} 1 \\ &= x \sum_{\substack{p \le x \\ p \equiv a \bmod q}} \frac{1}{p} - \sum_{\substack{p \le x \\ p \equiv a \bmod q}} \left\{\frac{x}{p}\right\}. \end{aligned} \tag{2.1}$$

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

$$\sum_{\substack{n \le x \\ n \equiv a \bmod q}} \omega(n) = x\left(\frac{1}{\varphi(q)} \log\log x + \beta(a,q) + O\left(\frac{1}{\log x}\right)\right) + O\left(\frac{x}{\varphi(q)\log x}\right), \tag{2.2}$$

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

Observe that there are a few versions of Mertens theorem in arithmetic progression, see [25, Theorem 15.4], [74], et alii. The basic case $q = 1$ of Theorem 2.1 is proved in [25, Theorem 7.2], [91, Proposition 2.6], et cetera.

The number of prime divisors $\omega(n)$ of a random integer $n \in \mathbb{N}$ is a normal random variable with mean $\varphi(q)^{-1} \log\log x$, and standard error $\sqrt{\varphi(q)^{-1} \log\log x}$, as verified in Theorem 2.1. The more general concept of the Erdos-Kac theorem provides finer details on the distribution of the random variable $\omega(n) \in \mathbb{N}$.

Theorem 2.2. [30] *If $x \ge 1$ is a large number, and $a \le q = o(\log x)$ be a pair of integers. Then,*

$$D(b,c) = \lim_{x \to \infty} \frac{1}{x} \left\{ n \le x : b \le \frac{w(n) - \varphi(q)^{-1} \log\log x}{\sqrt{\varphi(q)^{-1} \log\log x}} \le c \right\} = \frac{1}{2\pi} \int_b^c e^{-z^2/2} dz,$$

for any pair of distinct real numbers $b \le c$.

The original version was for the set of all natural numbers, for instance $q = 1$. But, it seamlessly extends to many subsets of integers of interest in number theory. The most obvious being the subset of integers in arithmetic progressions $\mathcal{A}(a, q) = \{n \in \mathbb{N} : n \equiv a \bmod q\}$ for a pair of integers $a < q$.

Chapter 3

Mobius Function

3.1 Mobius Function

Some information on the prime divisors counting functions studied in Chapter 2 are used in this Chapter to define and state the properties of other arithmetic functions dependent on the prime decomposition of the integers.

Definition 3.1. The Mobius function $\mu : \mathbb{N} \longrightarrow \{-1, 0, 1\}$ is defined by

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

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

$$\mu(n), \quad \mu(n+4), \quad \cdots, \quad \mu(n+4m) \tag{3.1}$$

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

Definition 3.2. For $n \geq 1$, the quasiMobius function $\mu_* : \mathbb{N} \longrightarrow \{-1, 1\}$ is defined, in terms of the prime divisors counting function, by

$$\mu_*(n) = (-1)^{\omega(n)}.$$

Definition 3.3. For $n \geq 1$, the Louiville function $\lambda : \mathbb{N} \longrightarrow \{-1, 1\}$ is defined, in terms of the prime divisors counting function, by

$$\lambda(n) = (-1)^{\Omega(n)}.$$

The quasiMobius function and the Mobius function fail to be multiplicative, but the the Louiville function is completely multiplicative.

The quasiMobius function and the Mobius function coincide on the subset of square-free integers. From this observation arises a fundamental identity.

Lemma 3.1. *For any integer $n \geq 1$, the Mobius function has the expansions*

$$\mu(n) = (-1)^{\omega(n)}\mu^2(n) \qquad \text{and} \qquad \mu(n) = (-1)^{\Omega(n)}\mu^2(n). \tag{3.2}$$

Lemma 3.2. *For any integer $n \geq 1$, the Liouville function has the expansion*

$$\lambda(n) = \sum_{d^2|n} \mu(n/d^2). \tag{3.3}$$

Proof. Observe that $\lambda(n)$ is a completely multiplicative function, so it is sufficient to verify the claim for prime powers $p^v, v \geq 1$, refer to [1, p. 50], and [97, p. 471], for similar information. ■

Lemma 3.3. *For any integer $n \geq 1$, the characteristic function for squarefree integers has the expansion*

$$\mu(n)^2 = \sum_{d^2|n} \mu(d) = \begin{cases} 1 & n = p_1 p_2 \cdots p_v, \\ 0 & n \neq p_1 p_2 \cdots p_v, \end{cases} \tag{3.4}$$

where the $p_i \geq 2$ are primes.

Definition 3.4. 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 3.5. The characteristic function for s-power free integers is defined by

$$\mu_s(n) = \begin{cases} 1 & \text{if } p^s \nmid n \text{ for any prime } p \mid n, \\ 0 & \text{if } p^s \mid n \text{ for any prime } p \mid n. \end{cases} \tag{3.5}$$

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

Lemma 3.4. *For any integer $n \geq 1$, the characteristic function for squarefree integers has the expansion*

$$\mu(n)^2 = \sum_{d^2|n} \mu(d). \tag{3.6}$$

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

$$\mu_s(n) = \sum_{d^s|n} \mu(d). \tag{3.7}$$

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 [13] and [79].

Definition 3.6. 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

$$\sum_{\substack{d|a \\ d|q}} \mu(d) = \begin{cases} 1 & \text{if and only if } \gcd(a, q) = 1, \\ 0 & \text{if and only if } \gcd(a, q) \neq 1. \end{cases} \tag{3.8}$$

This indicator function is widely used to remove the relatively prime dependence in many applications.

Lemma 3.5. *Let $n \geq 1$ be an integer, and let $\delta > 0$ be a small real number. Then,*

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

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

(iii) $\displaystyle\sum_{d|q} |\mu(d)| = O\left(q^{\delta}\right).$

Lemma 3.6. Mobius inversion formula *Let $f, g : \mathbb{N} \longrightarrow \mathbb{N}$ be arithmetic functions, and $n \geq 1$ an integer. Then*

(i) $f(n) = \displaystyle\sum_{d|n} g(d) \qquad \text{and} \qquad g(n) = \sum_{d|n} \mu(d) f(n/d)$
is an additive inverse pair.

(ii) $f(n) = \displaystyle\prod_{d|n} g(d) \qquad \text{and} \qquad g(n) = \prod_{d|n} f(n/d)^{\mu(d)}$
is a multiplicative inverse pair.

3.2 Summatory Mobius Function Over Over The Integers

The observed signs changes of the semimultiplicative function $\mu : \mathbb{N} \longrightarrow \{-1, 0, 1\}$ are sufficiently random. This phenomenon is known as the *Mobius randomness principle*, [62, p. 338].

Theorem 3.1. *Let $x \geq 1$ be a large number, and let $1 \leq a < q$ be a pair of relatively prime integers such that $q \leq (\log x)^c$, where $c \geq 0$ is a constant. Then*

$$\sum_{\substack{n \leq x \\ n \equiv a \bmod q}} \mu(n) = O\left(xe^{-d\sqrt{\log x}}\right),$$

where $d > 0$ is an absolute constant.

Lemma 3.7. *Let $x \geq 1$ be a large number, and let $q \ll (\log x)^b$, with $b \geq 0$ constant. Then,*

$$\sum_{\substack{n \leq x \\ \gcd(q,n)=1}} \mu(n) = O\left(xe^{-c\sqrt{\log x}}\right), \tag{3.9}$$

where $c > 0$ is an absolute constant.

Proof. Use the indicator function, Lemma 3.5, to remove the relatively prime dependence.

$$\begin{aligned} \sum_{\substack{n\leq x\\ \gcd(q,n)=1}} \mu(n) &= \sum_{n\leq x} \mu(n) \sum_{\substack{d|n\\ d|q}} \mu(d) \\ &= \sum_{d|q} \mu(d) \sum_{\substack{n\leq x\\ d|n}} \mu(d). \end{aligned} \tag{3.10}$$

Taking absolute value, and apply Theorem 3.1 to the inner sum, return

$$\begin{aligned} \left| \sum_{\substack{n\leq x\\ \gcd(q,n)=1}} \mu(n) \right| &\leq \sum_{d|q} |\mu(d)| \left| \sum_{\substack{n\leq x\\ d|n}} \mu(n) \right| \\ &= O\left(x \sum_{d|q} \frac{e^{-c\sqrt{\log x/d}}}{d} \right) \\ &= O\left(x \sum_{d\leq x} \frac{e^{-c\sqrt{\log x/d}}}{d} \right) \\ &= O\left(x e^{-c_0\sqrt{\log x}} \right), \end{aligned} \tag{3.11}$$

where $c_0 > 0$ is an absolute constant. ■

3.3 Summatory Mobius Function Over The Shifted Primes

As the Mertens sum $M(x) = \sum_{n\leq x} \mu(n)$, the simplest summatory function over the shifted primes is a closely related open problem.

Conjecture 3.1. *If $a \neq 0$ is a fixed integer, then*

$$\sum_{p\leq x} \mu(p-a) = o\left(\pi(x)\right). \tag{3.12}$$

The case $a = 0$ reduces to $\sum_{p\leq x} \mu(p-a) = -\pi(x)$. A proof on average was recently proposed in [69]. Unlike the linear summatory function in (3.12), the nonlinear summatory function for squarefree shifted primes has an easy solution.

Lemma 3.8. *If $x \geq 1$ is a large number, and a is a fixed integer, then*

$$\sum_{p\leq x} \mu^2(p-a) = a_1 \operatorname{li}(x) + O\left(x e^{-c\sqrt{\log x}} \right), \tag{3.13}$$

where a_1 is a constant, and $c > 0$ is an absolute constant.

Proof. Use Lemma 3.4 to rewrite it as

$$\begin{aligned}\sum_{p\le x}\mu^2(p-a) &= \sum_{p\le x}\mu(n)\sum_{d^2|p-a}\mu(d) \\ &= \sum_{d\le x^{1/2}}\mu(d)\sum_{\substack{p\le x\\ p\equiv a \bmod d^2}} 1.\end{aligned} \tag{3.14}$$

Set $x_0 = O(\log^b x)$. Now, partition the outer sum and apply the Siegel-Walfizs theorem for primes in arithmetic progressions.

$$\begin{aligned}\sum_{d\le x^{1/2}}\mu(d)\sum_{\substack{p\le x\\ p\equiv a \bmod d^2}} 1 &= \sum_{d\le x_0}\mu(d)\sum_{\substack{p\le x\\ p\equiv a \bmod d^2}} 1 + \sum_{x_0<d\le x^{1/2}}\mu(d)\sum_{\substack{p\le x\\ p\equiv a \bmod d^2}} 1 \\ &= \sum_{d\le x_0}\mu(d)\left(\frac{\mathrm{li}(x)}{\varphi(d^2)} + O\left(xe^{-c\sqrt{\log x/d}}\right)\right) \\ &\qquad + \sum_{x_0<d\le x^{1/2}}\sum_{\substack{p\le x\\ p\equiv a \bmod d^2}} 1 \\ &= a_1\,\mathrm{li}(x) + O\left(xe^{-c_0\sqrt{\log x}}\right),\end{aligned} \tag{3.15}$$

where

$$a_1 = \sum_{n\ge 1}\frac{\mu(n)}{\varphi(n^2)} > 0, \tag{3.16}$$

and $c > 0$ is an absolute constant. ■

The nonlinear correlation of Mobius functions over the integers

$$\sum_{n\le x}\mu^2(n)\mu^2(n-a) = \begin{cases}\zeta(2)^{-1}x(1+o(1)) & \text{if } a=0,\\ c_1x(1+o(1)) & \text{if } a\neq 0,\end{cases} \tag{3.17}$$

where $c_1 > 0$ is a constant, and the nonlinear correlation of Mobius functions over the shifted primes

$$\sum_{p\le x}\mu^2(p)\mu^2(p-a) = \begin{cases}\pi(x) & \text{if } a=0,\\ a_1\,\mathrm{li}(x)(1+o(1)) & \text{if } a\neq 0,\end{cases} \tag{3.18}$$

are completely solved. While, the linear correlation function over the integers

$$\sum_{n\le x}\mu(n)\mu(n-a) = o\,(x) \tag{3.19}$$

and the linear correlation function over the primes

$$\sum_{p\le x}\mu(p)\mu(p-a) = o\,(x) \tag{3.20}$$

for $a \neq 0$ are topics of current research.

3.4 Problems

3.4.1 Explicit Formulas

Exercise 3.1. Let $\mu(n) = -1, 0, 1$ be the Mobious function, and let $x \geq 1$ be a large number. Show that

$$\sum_{\substack{n \leq x \\ \gcd(q,n)=1}} \mu(n) = \frac{1}{i2\pi} \int_{c-i\infty}^{c+i\infty} \prod_{p|q} \left(1 - \frac{1}{p^s}\right)^{-1} \frac{1}{\zeta(s)} \frac{x^x}{s} ds$$

where $q \geq 1$ is an integer, $c > 1$ is real, and $\Re e(s) > 1$.

3.4.2 Open Problems

Exercise 3.2. Let $\mu(n) = -1, 0, 1$ be the Mobious function, and let $x \geq 1$ be a large number. Prove or disprove the following. If $a \neq$ is a fixed integer, then

$$\sum_{p \leq x} \mu(p - a) = o\left(\pi(x)\right).$$

Exercise 3.3. Let $\mu(n) = -1, 0, 1$ be the Mobious function, and let $x \geq 1$ be a large number. Prove or disprove the following. If $a \neq$ is a fixed integer, then

$$\sum_{n \leq x} \mu(n)\mu(n - a) = o\left(x\right).$$

Exercise 3.4. Let $\mu(n) = -1, 0, 1$ be the Mobious function, and let $x \geq 1$ be a large number. Use Lemma 3.1 to show that

$$\sum_{n \leq x} \mu(n)\mu(n - a) = \sum_{n \leq x} \lambda(n(n - a))\mu^2(n)\mu^2(n - a).$$

More precisely,

$$\sum_{n \leq x} \mu(n)\mu(n - a) = \sum_{n \leq x} \lambda(n)\lambda(n - a)\mu^2(n(n - a))$$

for all integers $a \in \mathbb{Z}$.

Chapter 4

Totients Functions

Various average orders of the Euler totient functions are required in the analysis of the primitive root, and elliptic groups of points of elliptic curves. Some of the essential analytic methods are introduced here.

4.1 Definitions Of Main Totients Functions

Let $p_1, p_2, p_3, \ldots, p_k$ be the sequence of primes in increasing order, and let $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ be an arbitrary integer. The Euler totient function counts the number of relatively prime integers $\varphi(n) = \#\{k : \gcd(k, n) = 1\}$.

Definition 4.1. The Euler totient function over the finite ring $\mathbb{Z}/n\mathbb{Z}$ is defined by $\varphi(n) = n \prod_{p|n} (1 - 1/p)$.

The Carmichael function is a more general version of the Euler totient function over the integers.

Definition 4.2. The Carmichael totient function over the finite ring $\mathbb{Z}/n\mathbb{Z}$ is defined by

$$\lambda(n) = \begin{cases} \varphi(2^e), & n = 2^e, e = 0, 1, \text{ or } 2, \\ \varphi(2^e)/2, & n = 2^e, e \geq 3, \\ \varphi(p^e), & n = p^e \text{ or }, 2p^e \text{ and } e \geq 1, \end{cases} \tag{4.1}$$

where $p \geq 3$ is prime, and

$$\lambda(n) = \operatorname{lcm}\left(\lambda(p_1^{e_1})\lambda(p_2^{e_2}), \ldots, \lambda(p_t^{e_t})\right). \tag{4.2}$$

The two functions coincide, that is, $\varphi(n) = \lambda(n)$ if $n = 2, 4, p^m, \text{ or } 2p^m, m \geq 1$. And $\varphi\left(2^m\right) = 2\lambda\left(2^m\right)$. In a few other cases, there are some simple relationships between $\varphi(n)$ and $\lambda(n)$. The Carmichael totient function has a more complex structure than the Euler totient function, however, many inherited properties such as

(1) $\lambda(n) \mid \varphi(n)$,

(2) $\varphi(n) = \xi(n)\lambda(n)$,

can be used to derive information about the Carmichael totient function.

4.2 Basic Properties

For each $n \in \mathbb{N}$, this counting function is compactly expressed by the additive to multiplicative identity

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d} = n \prod_{p|n} \left(1 - \frac{1}{p}\right). \tag{4.3}$$

Some of the multiplicative properties of the totient function are recorded in this section.

Lemma 4.1. *Given a pair of integers $m, n \in \mathbb{N}$, the totient function satisfies the followings relations.*

(i) $\varphi(mn) = \varphi(m)\varphi(n)$, *if* $\gcd(m, n) = 1$.

(ii) $\varphi(mn) = \dfrac{d}{\varphi(d)}\varphi(m)\varphi(n)$, *where* $\gcd(m, n) = d$.

(iii) $\varphi(m)\varphi(n) = \displaystyle\sum_{d|\gcd(m,n)} \varphi(mn/d)\mu(d)$, *for any* $m, n \geq 1$.

(iv) $\varphi(m) \mid \varphi(n)$, *if* $m \mid n$.

(v) $\varphi(n) \equiv 0 \bmod 2$, *if* $n \geq 3$.

Lemma 4.2. *There totient function and its inverse have the following representations.*

$$\varphi(n) = \sum_{1 \leq m \leq n,} \sum_{\substack{d|m \\ d|n}} \mu(d) \qquad \text{and} \qquad \frac{1}{\varphi(n)} = \frac{1}{n} \sum_{d|n} \frac{\mu(d)^2}{\varphi(d)}.$$

Proof. Employ the characteristic function of relatively prime integers

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \gcd(d, n) = 1, \\ 0 & \gcd(d, n) \neq 1, \end{cases} \tag{4.4}$$

to derive these identities. ■

4.3 Sums Of Euler Function Over The Integers

Several standard results on the average orders of some combinations of totient functions are provided here.

Theorem 4.1. *Let $\varphi(n)$ be the totient function, and let $\delta(n)$ be the delta function. Then, for all $x \geq 16$, and a constant c_1, the followings hold.*

(i) $\displaystyle\sum_{n \leq x} \varphi(n) = \frac{3}{\pi^2} x^2 + O(x)$, *unconditionally.*

(ii) $\displaystyle\sum_{n\le x}\varphi(n)=\frac{3}{\pi^2}x^2+c_1x+\Omega_{\pm}\left(x^{1/2}\log^2 x\right)$, *unconditionally oscillations.*

(iii) $\displaystyle\sum_{n\le x}\varphi(n)=\frac{3}{\pi^2}x^2+\frac{\delta(x)}{2}\varphi(x)+O(x^{1/2}\log^2 x)$, *conditional on RH.*

Proof. The complete proof appears in [14, Theorem 1.2]. ■

The standard proof, probably due to Dirichlet, see [87, p. 36], [112, p. 46], and other authors, gives $\sum_{n\le x}=3\pi^{-2}x^2+O(x\log x)$.

Theorem 4.2. *Let $\varphi(n)$ be the totient function, and let $x\ge 16$. Then, then the followings hold.*

(i) $\displaystyle\sum_{n\le x}\frac{\varphi(n)}{n}=\frac{6}{\pi^2}x+O(1)$, *unconditionally.*

(ii) $\displaystyle\sum_{n\le x}\frac{\varphi(n)}{n}=\frac{6}{\pi^2}x+\Omega_{\pm}\left(x^{-1/2}\right)$, *unconditional oscillations.*

(iii) $\displaystyle\sum_{n\le x}\frac{\varphi(n)}{n}=\frac{6}{\pi^2}x+O\left(\frac{\log^2 x}{x^{1/2}}\right)$, *conditional on RH.*

Proof. (i) Let $\{z\}=z-[z]$ be the fractional part function. Rewriting and expanding the formula yield

$$\begin{aligned}\sum_{n\le x}\frac{\varphi(n)}{n} &= \sum_{n\le x,}\sum_{d|n}\frac{\mu(d)}{d} \\ &= \sum_{d\le x}\frac{\mu(d)}{d}\sum_{\substack{m\le x/d\\ d|n}}1 \\ &= \sum_{d\le x}\frac{\mu(d)}{d}\left(\frac{x}{d}-\{x/d\}\right) \\ &= x\sum_{d\le x}\frac{\mu(d)}{d^2}-\sum_{d\le x}\frac{\mu(d)}{d}\{x/d\}.\end{aligned} \tag{4.5}$$

Using the fractional Mobius function $W(x)=\sum_{n\le x}\mu(n)/n=-1+O(xe^{-\sqrt{\log x}})$, the last finite sum has the asymptotic order

$$\sum_{n\le x}\frac{\mu(n)}{n}\left\{\frac{x}{n}\right\}=\int_1^x\left\{\frac{x}{t}\right\}dW(t)=O\left(e^{-\sqrt{\log x}}\right). \tag{4.6}$$

Hence,

$$\begin{aligned}x\sum_{d\le x}\frac{\mu(d)}{d^2}-\sum_{d\le x}\frac{\mu(d)}{d}\{x/d\} &= x\left(\frac{1}{\zeta(2)}+O\left(\frac{1}{x}\right)\right)+O\left(e^{-\sqrt{\log x}}\right) \\ &= \frac{6}{\pi^2}x+O(1).\end{aligned}$$

(ii) Use $V(x)=\sum_{n\le x}\mu(n)/n=\Omega_{\pm}\left(x^{-1/2}\right)$, and partial summation. ■

4.4 Sums Of Euler Totient Functions Over The Squarefree Integers

Theorem 4.3. *For all $x \geq 1$ be a large number, and let $\mu(n)$ be the Mobius function. Then, the average order of the normalized squarefree totient function over the integers has the followings asymptotic formulas.*

(i) $$\sum_{n\leq x}\frac{\varphi(n)}{n}\mu^2(n) = \frac{6}{\pi^2}x\prod_{p\geq 2}\left(1-\frac{1}{p(p+1)}\right)+O\left(xe^{-c_0\sqrt{\log x}}\right),$$
where $c_0 > 0$ is an absolute constant, unconditionally.

(ii) $$\sum_{n\leq x}\frac{\varphi(n)}{n}\mu^2(n) = \frac{6}{\pi^2}x\prod_{p\geq 2}\left(1-\frac{1}{p(p+1)}\right)+O\left(x^{1/2}\log x\right),$$
conditional on RH.

Proof. (i) Letting $f(n) = \varphi(n)/n$. The finite sum

$$\sum_{p\leq x} f(p) = \sum_{p\leq x}\left(1-\frac{1}{p}\right) = \frac{x}{\log x}+O\left(\frac{x}{\log^2 x}\right), \tag{4.7}$$

implies the density $\tau = 1$. Applying the Wirsing type formula in Lemma 9.10, returns

$$\begin{aligned}\sum_{n\leq x}\frac{\varphi(n)}{n}\mu^2(n) &= \left(e^{-\gamma}+o(1)\right)\frac{x}{\log x}\prod_{p\leq x}\left(1+\frac{p-1}{p^2}\right) \\ &= \left(e^{-\gamma}+o(1)\right)\frac{x}{\log x}\prod_{p\leq x}\left(1+\frac{1}{p}\right)\prod_{p\leq x}\left(1-\frac{1}{p(p+1)}\right).\end{aligned} \tag{4.8}$$

Applying Lemma 9.9 to the first product in (4.8), and completing the second product, see Exercise 9.5, return

$$\begin{aligned}S(x) &= \sum_{n\leq x}\frac{\varphi(n)}{n}\mu^2(n) \\ &= \left(e^{-\gamma}+o(1)\right)\frac{x}{\log x}\left(\frac{6e^{\gamma}}{\pi^2}\log x+O\left(e^{-c_0\sqrt{\log x}}\right)\right)\prod_{p\leq x}\left(1-\frac{1}{p(p+1)}\right) \\ &= \left(\frac{6}{\pi^2}x+O\left(xe^{-c_0\sqrt{\log x}}\right)\right)\left(\prod_{p\geq 2}\left(1-\frac{1}{p(p+1)}\right)+O\left(\frac{1}{x\log x}\right)\right) \\ &= \frac{6}{\pi^2}x\prod_{p\geq 2}\left(1-\frac{1}{p(p+1)}\right)+O\left(xe^{-c_0\sqrt{\log x}}\right),\end{aligned} \tag{4.9}$$

where $c_0 > 0$ is an absolute constant. ■

4.5 Sums Of Carmichael Functions Over The Squarefree Integers

Theorem 4.4. *For all $x \geq 1$ be a large number, and let $\mu(n)$ be the Mobius function. Then, the average order of the normalized squarefree Carmichael function over the integers has the followings asymptotic formulas.*

(i) $$\sum_{n \leq x} \frac{\lambda(n)}{n} \mu^2(n) = \frac{6}{\pi^2} x \prod_{p \geq 2} \left(1 + \frac{1}{p(p+1)}\right) + O\left(xe^{-c_0\sqrt{\log x}}\right),$$
where $c_0 > 0$ is an absolute constant, unconditionally.

(ii) $$\sum_{n \leq x} \frac{\lambda(n)}{n} \mu^2(n) = \frac{6}{\pi^2} x \prod_{p \geq 2} \left(1 + \frac{1}{p(p+1)}\right) + O\left(x^{1/2} \log x\right),$$
conditional on RH.

Proof. After making thwe necessary changes, the proofs are similar to those of Theorem 4.3.

■

4.6 Sums Of Carmichael Function Over The Integers

Theorem 4.5. ([32, Theorem 3]) *For all $x \geq 16$, then the followings hold.*

(i) *The average order has the asymptotic formula*

$$\frac{1}{x} \sum_{n \leq x} \lambda(n) = \frac{x}{\log x} e^{\frac{B \log\log x}{\log\log\log x}(1+o(1))},$$

where the constants are $\gamma = 0.5772\ldots$ and

$$B = e^{-\gamma} \prod_{p \geq 2} \left(1 - \frac{1}{(p-1)^2(p+1)}\right) = 0.34537\ldots.$$

(ii) *The normalized function has the asymptotic formula*

$$\sum_{n \leq x} \frac{\lambda(n)}{n} = \frac{x}{\log x} e^{\frac{B \log\log x}{\log\log\log x}(1+o(1))}.$$

Proof. (ii) Set $U(x) = \sum_{n \leq x} \lambda(n)$. Summation by part yields

$$\begin{aligned} \sum_{n \leq x} \frac{\lambda(n)}{n} &= \int_1^x \frac{1}{t} dU(t) \\ &= \frac{U(x)}{x} - \frac{U(1)}{1} + \int_1^x \frac{U(t)}{t^2} dt. \end{aligned} \tag{4.10}$$

Invoke case (i) to complete the claim. ■

Lemma 4.3. *Let $x \geq 16$, and $\lambda(n)$ be the Carmichael totient function. Then*

$$\sum_{n \leq x} \frac{\varphi(\lambda(n))}{\lambda(n)} \geq k_1 \frac{x}{\log\log x}(1 + o(1)),$$

where $k_1 > 0$ is a constant.

Proof. Begin with the expression

$$\begin{aligned} \frac{\varphi(\lambda(n))}{\lambda(n)} &= \prod_{p|\lambda(n)} \left(1 - \frac{1}{p}\right) \\ &\geq \frac{1}{e^{\gamma}} \frac{1}{\log\log \lambda(n)} \left(1 + O\left(\frac{1}{\log\log \lambda(n)}\right)\right) \end{aligned} \tag{4.11}$$

holds for all integers $n \geq 1$, with equality on a subset of integers of zero density. In light of the lower bound and upper bound

$$\frac{n}{(\log n)^{a \log\log\log n}} \leq \lambda(n) \leq \frac{n}{(\log n)^{b \log\log\log n}} \tag{4.12}$$

for some constants $a > 0$ and $b > 0$ and large $n \geq 1$, see [32, Theorem 1], proceed to determine a lower bound for the sum:

$$\begin{aligned} \sum_{n \leq x} \frac{\varphi(\lambda(n))}{\lambda(n)} &\geq k_1 \int_2^x \frac{1}{\log\log t} dt \\ &= k_1 \frac{x}{\log\log x} + k_2 \int_2^x \frac{1}{t(\log t)(\log\log t)^2} dt, \end{aligned} \tag{4.13}$$

where $k_1 > 0$ and k_2 are constants. This is sufficient to complete the claim. ■

More advanced techniques for the composition of arithmetic functions are studied in [81], [6], et cetera.

The ratio $\varphi(\varphi(n))/\varphi(n) = \varphi(\lambda(n))/\lambda(n)$ for all integers $n \geq 1$. But, the composition only satisfy $\varphi(\varphi(n)) \geq \varphi(\lambda(n))$, and agrees on a subset of integers of zero density.

Lemma 4.4. ([84, Theorem 2]) *Let $x \geq 1$ be a large number. Then*

$$\#\{n : \varphi(\varphi(n)) \geq \varphi(\lambda(n))\} \ll \frac{x}{(\log\log x)^c}$$

for any constant $c > 0$.

4.7 Sums Of Totients Functions Over The Primes

The ratio $\varphi(p-1)/(p-1)$ for all primes $p \geq 2$ has an established literature. But, the ratio $\lambda(p-1)/(p-1)$ does not has any meaningful literature, its average order is estimated here in Lemma 4.8, and a more precise version is stated in the exercises.

Lemma 4.5. ([106, Lemma 1]) *Let $x \geq 1$ be a large number, and let $\varphi(n)$ be the Euler totient function. Then*

$$\sum_{p \leq x} \frac{\varphi(p-1)}{p-1} = a_0 \operatorname{li}(x) + O\left(\frac{x}{\log^B x}\right),$$

where the constant

$$a_0 = \prod_{p \geq 2} \left(1 - \frac{1}{p(p-1)}\right) = .37399581\ldots, \tag{4.14}$$

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

More general versions of Lemma 4.5 are proved in [118], and [54].

Lemma 4.6. ([118, Lemma 4.4]) *Let $x \geq 1$ be a large number, and let $\varphi(n)$ be the Euler totient function, and let $k \geq 1$ be an integer. Then*

$$\sum_{p \leq x} \left(\frac{\varphi(p-1)}{p-1}\right)^k = a_k \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right),$$

where the constant

$$a_k = \prod_{p \geq 2} \left(1 - \frac{p^k - (p-1)^k}{p^k(p-1)}\right). \tag{4.15}$$

Lemma 4.7. *Let $x \geq 1$ be a large number, and let $\varphi(n)$ be the Euler totient function, and let $k \geq 1$ be an integer. Then, the first moment has the asymptotic*

$$\sum_{p \leq x} \left(\frac{\varphi(p-1)}{p-1}\right)^k p = a_k \frac{x^2}{2\log x} + O\left(\frac{x^2}{\log^2 x}\right).$$

Proof. Let $W(t) = \sum_{p \leq x} \left(\varphi(p-1)/(p-1)\right)^k$. By partial summation

$$\begin{aligned} \sum_{p \leq x} \left(\frac{\varphi(p-1)}{p-1}\right)^k p &= \int_2^x t dW(t) \qquad (4.16) \\ &= a_k \frac{x^2}{\log x} + O\left(\frac{x^2}{\log^2 x}\right) - \int_2^x W(t)dt \\ &= a_k \frac{x^2}{2\log x} + O\left(\frac{x^2}{\log^2 x}\right). \end{aligned}$$

■

4.8 Sums Of Carmichael Functions Over The Primes

Lemma 4.8. *Let $x \geq 1$ be a large number, and let $\lambda(n)$ be the Carmichael totient function. Then*

$$\sum_{p \leq x} \frac{\lambda(p-1)}{p-1} \gg \frac{x}{(\log x)(\log\log x)}.$$

Proof. Begin with the expression

$$\begin{aligned} \frac{\lambda(p-1))}{p-1} &= \prod_{q|\lambda(p-1)} \left(1-\frac{1}{q}\right) \\ &\gg \frac{1}{\log \lambda(p-1)} \end{aligned} \tag{4.17}$$

holds for all integers $p-1 \geq 1$, with equality on a subset of integers of zero density. In light of the lower bound and upper bound

$$\frac{n}{(\log n)^{a \log\log\log n}} \leq \lambda(n) \leq \frac{n}{(\log n)^{b \log\log\log n}} \tag{4.18}$$

for some constants $a > 0$ and $b > 0$ and large $n \geq 1$, see [32, Theorem 1], proceed to determine a lower bound for the sum:

$$\begin{aligned} \sum_{p \leq x} \frac{\lambda(p-1)}{p-1} &\gg k_1 \int_2^x \frac{1}{\log\log t} d\pi(t) \\ &\gg \frac{x}{(\log x)(\log\log x)}. \end{aligned} \tag{4.19}$$

Confer the exercises for similar information. ■

4.9 Extreme Values Of The Totient Function

Some estimates for the extreme values of the Euler totient function are stated in this subsection. Currently the best unconditional upper bound of this arithmetical function is

$$\frac{n}{\varphi(n)} < e^{\gamma} \log\log n + \frac{5}{2\log\log n} \tag{4.20}$$

for any integer $n \in \mathbb{N}$ with one exception for $n = 2 \cdot 3 \cdots 23$, see [103]. 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 4.9. *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

$$\begin{aligned} \varphi(n) &= n \prod_{p|n} \left(1-\frac{1}{p}\right) \\ &\leq n\left(1-\frac{1}{\log n}\right) \\ &= n + O\left(\frac{1}{\log n}\right). \end{aligned} \tag{4.21}$$

In the other direction, there is the lower bound

$$\begin{aligned}\varphi(n) &= n\prod_{p|n}\left(1-\frac{1}{p}\right) \\ &\geq n\prod_{\log n<p\leq 2\log n}\left(1-\frac{1}{p}\right) \\ &= n+O\left(\frac{n}{\log\log n}\right).\end{aligned} \tag{4.22}$$

Both relations (4.21) and (4.22) confirm the claim. (ii) The prime divisors of $n+1$ are $q=2$ and some prime $q>\log n$, so the claim follows from

$$\varphi(n+1)=(n+1)\prod_{p|(n+1)}\left(1-\frac{1}{p}\right)\leq\frac{n}{2}\left(1-\frac{1}{\log n}\right)=\frac{n}{2}+O\left(\frac{n}{\log n}\right). \tag{4.23}$$

■

Theorem 4.6. *Let $p\geq 2$ be a large prime. Then, the followings extreme values hold.*

(i) $\dfrac{\varphi(n)}{n}\leq 1-\dfrac{1}{n}$, *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 4.9, and this accounts for the wide range and large gaps in the sequence of totient gaps

$$\varphi(2)-\varphi(1),\ \ \varphi(3)-\varphi(2),\ \ \varphi(4)-\varphi(3),\ \ \ldots,\ \ \varphi(n+1)-\varphi(n),\ \ \ldots. \tag{4.24}$$

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 $\varphi(2\cdot 3\cdot 5+1)-\varphi(2\cdot 3\cdot 5+2)=14$.

4.10 Average Lower And Upper Bounds

The totient function has the explicit lower bound

$$\frac{\varphi(n)}{n}>\frac{1}{e^{\gamma}\log\log n+5/(2\log\log n)} \tag{4.25}$$

for any integer $n\geq 1$, see [103, Theorem 7]. The subset of integers that satisfy the extreme values of this inequality is a very thin subset of integers. In contrast, almost every integers has a large lower and upper bounds. The lower and upper bounds for almost every integer are significantly smaller by an iterated factor of log as demonstrated below.

Theorem 4.7. *For almost all integers $n \geq 1$, the ratio $n/\varphi(n)$ has the followings bounds.*

(i) $\log\log\log n \ll \dfrac{n}{\varphi(n)}$.

(ii) $\dfrac{n}{\varphi(n)} \ll \log\log\log n$.

Proof. (ii) By the Erdos-Kac theorem, (confer [30], [61, Theorem 431], [49], et cetera), almost every integer $n \geq 1$ has $\omega(n) \ll \log\log n$ prime divisors. In addition, the interval $[1, (\log\log n)^2]$ contains $\pi((\log\log n)^2) \gg \log\log n$ primes. Thus,

$$\begin{aligned} \frac{n}{\varphi(n)} &= \prod_{p|n}\left(1-\frac{1}{p}\right)^{-1} \\ &\ll \prod_{p\ll(\log\log n)^2}\left(1-\frac{1}{p}\right)^{-1} \\ &\ll \log\log\log n. \end{aligned} \tag{4.26}$$

The reverse inequality is similar. ■

Theorem 4.8. *Let $x \geq 1$ be a large number. Then, there are constants $c_0 > 0$ and $c_1 > 0$ for which the Euler totient function has the followings bounds.*

(i) $\dfrac{\varphi(n)}{n} \geq \dfrac{c_0}{\log\log\log n}$ *for almost all large integers $n \geq 1$.*

(ii) $\dfrac{\varphi(n)}{n} \leq \dfrac{c_1}{\log\log\log n}$ *for almost all large integers $n \geq 1$.*

The proof of this theorem uses the same technique as Theorem 4.7.

4.11 Power Sums of Relatively Prime Integers

Lemma 4.10. *For a complex number $s \in \mathbb{C}$, there is a generalized Mobius inversion pair*

$$n^s = \sum_{d|n}\varphi_s(d) \qquad \text{and} \qquad \varphi_s(n) = n^s\sum_{d|n}\frac{\mu(d)}{d^s}.$$

The case $s = 1$ is well known. This identity has a nice connection to powers sums of relatively prime integers, some details appear in [97, p. 438].

Lemma 4.11. *Let $s \geq 0$ be an integer, and let $\operatorname{rad}(n) = \prod_{p|n} p$ be the radical of $n \geq 1$. Then,*

(i) $\displaystyle\sum_{\substack{k\leq n\\ \gcd(k,n)=1}} 1 = \varphi(n)$,

where $\operatorname{rad}(n) = \prod_{p|n} p$ is the radical, number of relatively prime numbers.

(ii) $$\sum_{\substack{k\le n\\ \gcd(k,n)=1}} k = \frac{\varphi(n)n}{2},$$
sum of relatively prime numbers.

(iii) $$\sum_{\substack{k\le n\\ \gcd(k,n)=1}} k^2 = \frac{\varphi(n)}{6}\left(2n^2+\mu(\mathrm{rad}(n))\,\mathrm{rad}(n)\right),$$
sum of square of relatively prime numbers.

(iv) $$\sum_{\substack{k\le n\\ \gcd(k,n)=1}} k^s = \frac{\varphi(n)n^s}{s+1}+O\left(\frac{n^s}{s}\right),$$
sum of s-power of relatively prime numbers.

Proof. (ii) For $s=1$, using the the relatively prime characteristic function, and reversing the order of summation yield

$$\sum_{\substack{1\le k<n\\ \gcd(k,n)=1}} k = \sum_{1\le k\le n} k\sum_{\substack{d|k\\ d|n}}\mu(d) = \sum_{d|n}\mu(d)d\sum_{1\le k\le n/d} k. \tag{4.27}$$

Substitute the power sum $\sum_{k\le z} k = z(z+1)/2$ to obtain

$$\begin{aligned}\sum_{d|n}\mu(d)d\sum_{1\le k\le n/d} k &= \frac{1}{2}\sum_{d|n}\mu(d)d\left(\left(\frac{n}{d}\right)^2+\left(\frac{n}{d}\right)\right)\\ &= \frac{n}{2}\sum_{d|n}\mu(d)\frac{n}{d}+\frac{n}{2}\sum_{d|n}\mu(d)\\ &= \frac{n}{2}\varphi(n)\end{aligned} \tag{4.28}$$

for $n\ge 2$. (iv) As before, for $s\ge 2$, this is

$$\sum_{\substack{1\le k<n\\ \gcd(k,n)=1}} k^s = \sum_{1\le k\le n} k^s\sum_{\substack{d|k\\ d|n}}\mu(d) = \sum_{d|n}\mu(d)d\sum_{1\le k\le n/d} k^s. \tag{4.29}$$

Substitute the power sum $\sum_{k\le z} k^s = z^{s+1}/(s+1)+O(z^s)$ to obtain

$$\begin{aligned}\sum_{d|n}\mu(d)d\sum_{1\le k\le n/d} k^s &= \frac{1}{s+1}\sum_{d|n}\mu(d)d\left(\left(\frac{n}{d}\right)^{s+1}+\left(\frac{n}{d}\right)^s\right)\\ &= \frac{n^{s+1}}{s+1}\varphi_s(n)+O\left(\frac{n^s}{s}\right),\end{aligned} \tag{4.30}$$

where $\varphi_s(n)=n^s\sum_{d|n}\mu(d)d^s$ is the generalized totient function. ■

4.12 Results For The Ratio $n/\varphi(n)$

This section continues with the analysis of the error term of the average order for the reciprocal $1/\varphi(n)$ of the Euler totient function $\varphi(n)$. It proves that the best error term is the same as that determined by Landau over a century ago, in [68, p. 184]. The simpler analysis for the ratio $n/\varphi(n)$ is considered first.

Theorem 4.9. *Let $x \geq 1$ be a large number. Then, the average order of the ratio $n/\varphi(n)$ has the asymptotic formula*

$$\sum_{n\leq x} \frac{n}{\varphi(n)} = a_0 x + O(\log x),$$

where $a_0 = \zeta(2)\zeta(3)/\zeta(6)$ is a constant.

Proof. The result is derived using the identity $\sum_{d|n} \mu^2(d)/\varphi(d)$. Substituting this formula, and reversing the order of summation yield

$$\begin{aligned}
\sum_{n\leq x} \frac{n}{\varphi(n)} &= \sum_{n\leq x} \sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} \\
&= \sum_{d\leq x} \frac{\mu^2(d)}{\varphi(d)} \sum_{n\leq x,\, d\,|\, n} 1 \\
&= \sum_{d\leq x} \frac{\mu^2(d)}{\varphi(d)} \left(\frac{x}{d} - \left\{\frac{x}{d}\right\}\right) \\
&= x \sum_{d\leq x} \frac{\mu^2(d)}{d\varphi(d)} - \sum_{d\leq x} \frac{\mu^2(d)}{\varphi(d)} \left\{\frac{x}{d}\right\}.
\end{aligned} \tag{4.31}$$

The first finite sum

$$\begin{aligned}
x \sum_{n\leq x} \frac{\mu^2(n)}{n\varphi(n)} &= x \left(\sum_{n\geq 1} \frac{\mu^2(n)}{n\varphi(n)} - \sum_{n>x} \frac{\mu^2(n)}{n\varphi(n)} \right) \\
&= a_0 x + O\left(\log\log x\right),
\end{aligned} \tag{4.32}$$

see Exercise 4.10. The constant $a_0 > 0$ has an expression in terms of zeta functions as

$$\sum_{n\geq 1} \frac{\mu^2(n)}{n\varphi(n)} = \prod_{p\geq 2} \left(1 + \frac{1}{p(p-1)}\right) = \frac{\zeta(2)\zeta(3)}{\zeta(6)}. \tag{4.33}$$

The second finite sum

$$\sum_{n\leq x} \frac{\mu^2(n)}{\varphi(n)} \left\{\frac{x}{n}\right\} \gg \log x \tag{4.34}$$

is alway positive and exhibits no cancellations. ■

The form of the error term in (4.34) concretely proves that it cannot be improved.

Theorem 4.10. *Let $x \geq 1$ be a large number. Then, the average order of the ratio $1/\varphi(n)$ is as follows.*

$$\sum_{n \leq x} \frac{1}{\varphi(n)} = c_0 + c_1 \log x + O\left(\frac{\log x}{x}\right),$$

where c_0 and c_1 are constants.

Proof. The result is derived Theorem 4.9 by partial summation. More precisely, let $R(t) = \sum_{n \leq x} n/\varphi(n) = a_0 x + O(\log x)$. Then

$$\begin{aligned}
\sum_{n \leq x} \frac{1}{\varphi(n)} &= \sum_{n \leq x} \frac{1}{n} \frac{n}{\varphi(n)} \\
&= \int_1^x \frac{1}{t} dR(t) \qquad (4.35) \\
&= \frac{R(t)}{t}\Bigg|_1^x + \int_1^x \frac{R(t)}{t^2} dt, \\
&= \frac{a_0 x + O(\log x)}{x} + a_1 + \int_1^x \frac{a_0 t + O(\log t)}{t^2} dt, \\
&= c_0 + c_1 \log x + O\left(\frac{\log x}{x}\right),
\end{aligned}$$

where $a_0 > 0, a_1 = -R(1), c_0$, and $c_1 = a_0$ are constants. ■

The work in [109] is devoted to improving the error term from $O((\log x)/x)$ to $O((\log x)^{2/3}/x)$. This analysis was based on the estimate

$$\sum_{n \leq x} \frac{\{x/n\} - 1/2}{n} = O\left((\log x)^{2/3}\right). \qquad (4.36)$$

However, by Theorem 4.10, confer (4.34), the error term in (4.35) satisfies $\gg (\log x)/x$.

4.13 Sums Of Euler Functions Over Integers In Arithmetic Progressions

The results for the Euler function over arithmetic progressions are significantly more involved.

Theorem 4.11. ([95, p. 191]) *Let $x \geq 1$ be a large number, let $1 \leq a \leq q$ be integers, and let $\varphi(n)$ be the Euler totient function. Then*

$$\sum_{\substack{n \leq x \\ n \equiv a \bmod q}} \varphi(n) = \frac{3}{\pi^2} \frac{1}{q} \prod_{p \mid q} \left(1 - \frac{1}{p^2}\right)^{-1} \prod_{p \mid \gcd(a,q)} \left(1 - \frac{1}{p}\right) x^2 + O(x \log x).$$

Lemma 4.12. *Let $x \geq 1$ be a large number, let $1 \leq a \leq q$ be integers, and let $\varphi(n)$ be the Euler totient function. Then*

$$\sum_{\substack{n \leq x \\ n \equiv a \bmod q}} \frac{\varphi(n)}{n} = \frac{6}{\pi^2}\frac{1}{q}\prod_{p|q}\left(1-\frac{1}{p^2}\right)^{-1}\prod_{p|\gcd(a,q)}\left(1-\frac{1}{p}\right)x + O(\log x).$$

Proof. This follows form Theorem 4.11 by partial summation. ■

The expression $\log_k x$ denote the k-iteration of the logarithm, and the expression

$$a = \prod_{\log_2 x < r \leq 2\log_2 x} r \tag{4.37}$$

is the product of all the consecutive primes r within the stated range.

Lemma 4.13. *Let $x \geq 1$ be a large number, and let $a = \prod_{\log_2 x < r \leq 2\log_2 x} r$ and $q = \prod_{r \leq 2\log_2 x} r$. Then,*

$$\sum_{\substack{n \leq x \\ n \equiv a \bmod q}} \frac{\varphi(n)}{n} = C(q,a)x + O(\log x).$$

as $x \to \infty$, where $C(q,a) > 0$ is a constant depending on a,and q.

Proof. This the same as Lemma 4.12. Accordingly, it is sufficient to calculate the constant. Toward this end, observe that

$$\begin{aligned} C(q,a) &= \frac{6}{\pi^2}\frac{1}{q}\prod_{p|q}\left(1-\frac{1}{p^2}\right)^{-1}\prod_{p|\gcd(a,q)}\left(1-\frac{1}{p}\right) \\ &= \frac{6}{\pi^2}\frac{1}{q}\prod_{p \leq \log\log x}\left(1-\frac{1}{p^2}\right)^{-1}\prod_{\log\log x < p \leq 2\log\log x}\left(1+\frac{1}{p}\right). \end{aligned} \tag{4.38}$$

Here, $\gcd(a,q) = \prod_{\log\log x < p \leq 2\log\log x} r$, and

$$\prod_{p|\gcd(a,q)}\left(1-\frac{1}{p}\right) = \prod_{\log\log x < p \leq 2\log\log x}\left(1-\frac{1}{p}\right), \tag{4.39}$$

which cancels the corresponding upper parts of the first product. The remaining tail product

$$\prod_{\lg\log x < p \leq 2\log\log x}\left(1+\frac{1}{p}\right)^{-1} = c_0 + O\left(\frac{1}{\log\log x}\right), \tag{4.40}$$

where $c_0 > 0$ is a constant, which is a routine application of Mertens theorem. Therefore,

$$\begin{aligned} C(q,a) &= \frac{6}{\pi^2}\frac{1}{q}\prod_{p \leq \log\log x}\left(1-\frac{1}{p^2}\right)^{-1}\prod_{\log\log x < p \leq 2\log\log x}\left(1+\frac{1}{p}\right) \\ &= \frac{6}{\pi^2}\left(\frac{\pi^2}{6} + O\left(\frac{1}{\log\log x}\right)\right)\left(c_0 + O\left(\frac{1}{\log\log x}\right)\right) \\ &= c_0 + O\left(\frac{1}{\log\log x}\right). \end{aligned} \tag{4.41}$$

This conpletes the proof. ■

4.14 Sums Of Euler Functions Over Primes In Arithmetic Progressions

A finite sum over the shifted primes is computed in the next result.

Lemma 4.14. *Let $x \geq 1$ be a real number, and let $1 \leq a < q$, $\gcd(a,q) = 1$ be integers with $q = O(\log^C x)$. Then*

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

where $c_q > 0$, and $B > C > 0$ are constants depending on $q > 1$.

Proof. Use idenity $\varphi(n)/n = \sum_{d|n} \mu(d)/d$ to rewrite the summatory function as

$$\begin{aligned} \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \frac{\varphi(p-1)}{p-1} &= \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} \sum_{d \,|\, p-1} \frac{\mu(d)}{d} \\ &= \sum_{d \leq x} \frac{\mu(d)}{d} \sum_{\substack{p \leq x \\ p \equiv a \bmod q \\ p \equiv 1 \bmod d}} 1. \end{aligned} \tag{4.42}$$

The prime number theorem on arithmetic progression leads to

$$\begin{aligned} \sum_{d \leq x} \frac{\mu(d)}{d} \sum_{\substack{p \leq x \\ p \equiv a \bmod q \\ p \equiv 1 \bmod d}} 1 &= \sum_{d \leq x} \frac{\mu(d)}{d} \cdot \pi(x/dq, dq, b) \\ &= \sum_{d \leq x} \frac{\mu(d)}{d} \left(\frac{1}{\varphi(dq)} \frac{x}{\log x} + O\left(\frac{x}{\log^B x}\right)\right) \\ &= \frac{x}{\log x} \sum_{d \leq x} \frac{\mu(d)}{d\varphi(dq)} + O\left(\frac{x}{\log^B x} \sum_{d \leq x} \frac{1}{d}\right), \end{aligned} \tag{4.43}$$

where $b \equiv 1 \bmod d$, and $b \equiv a \bmod q$ is a residue class modulo dq. Choose a constant $B > 2$, and use the identity

$$\frac{\varphi(dq)}{dq} = \frac{\varphi(d)}{d} \frac{\varphi(q)}{q} \prod_{r \,|\, \gcd(d,q)} \left(1 - \frac{1}{r}\right)^{-1}, \tag{4.44}$$

where $r \geq 2$ is prime, to rewrite it as

$$\begin{aligned} & \frac{x}{\log x} \sum_{d \leq x} \frac{\mu(d)}{d\varphi(dq)} + O\left(\frac{x}{\log^B x} \sum_{d \leq x} \frac{1}{d}\right) \\ = & \frac{1}{\varphi(q)} \frac{x}{\log x} \sum_{d \leq x} \frac{\mu(d)}{d\varphi(d)} \prod_{r \mid \gcd(d,q)} \left(1 - \frac{1}{r}\right) + O\left(\frac{x}{\log^{B-1} x}\right). \\ = & \frac{c_q}{\varphi(q)} \frac{x}{\log x} + O\left(\frac{x}{\log^{B-1} x}\right). \end{aligned} \tag{4.45}$$

The constant $c_q > 0$ is specified by the finite sum, which has a product expansion as

$$\sum_{d \leq x} \frac{\mu(d)}{d\varphi(d)} \prod_{r \mid \gcd(d,q)} \left(1 - \frac{1}{r}\right) = \prod_{p \geq 2} \left(1 - \frac{1}{p(p-1)} \prod_{p \mid q} \left(1 - \frac{1}{p}\right)\right) + O\left(\frac{1}{x}\right). \tag{4.46}$$

■

4.15 Sums Of Totients Functions Over Subsets Of Integers

The asymptotic formulas for the normalized summatory totient function $\varphi(n)/n$ and $\varphi(n)$ over the subset of integers $\mathcal{A} = \{n \geq 1 : \gcd(\varphi(n), q) = 1\}$ are computed here. These results are based on the counting function $A(x) = \{n \leq x : n \in \mathcal{A}\}$.

Theorem 4.12. ([77, Theorem 2]) *For a prime power $q \geq 2$, and a large number $x \geq 1$, the counting function $A(x)$ has the asymptotic foirmula*

$$\sum_{\substack{n \leq x \\ \gcd(\varphi(n),q)=1}} 1 = c_q \frac{x}{(\log x)^{1/(q-1)}} \left(1 + O_q\left(\frac{\log\log x}{\log x}\right)\right),$$

where $c_q > 0$ is a constant.

Theorem 4.13. *For large number $x \geq 1$, the average order for the normalized Euler totient function $\varphi(n)/n$ over the subset $\mathcal{A}$ has the asymptotic formula*

$$\sum_{\substack{n \leq x \\ \gcd(\varphi(n),q)=1}} \frac{\varphi(n)}{n} = \frac{6c_q}{\pi^2} \frac{x}{(\log x)^{1/(q-1)}} \left(1 + O_q\left(\frac{\log\log x}{\log x}\right)\right),$$

where $c_q > 0$ is a constant.

Proof. Let $\mathcal{A} = \{n \geq 1 : \gcd(\varphi(n), q) = 1\}$ and let $A(x) = \{n \leq x : n \in \mathcal{A}\}$ be the corresponding the counting function. Using the standard indentity $\varphi(n) =$

$n\sum_{d|n}\mu(n)/d$ the average order is expressed as

$$\begin{aligned}\sum_{\substack{n\le x\\ \gcd(\varphi(n),q)=1}}\frac{\varphi(n)}{n} &= \sum_{\substack{n\le x\\ \gcd(\varphi(n),q)=1}}\sum_{d|n}\frac{\mu(n)}{d}\\ &= \sum_{d\le x}\frac{\mu(n)}{d}\sum_{\substack{n\le x\\ \gcd(\varphi(n),q)=1\\ d|n}}1\\ &= \sum_{d\le x}\frac{\mu(n)}{d}\sum_{\substack{n\le x/d\\ \gcd(\varphi(n),q)=1}}1,\end{aligned}\tag{4.47}$$

where $\mu(n)\in\{-1,0,1\}$ is the Mobius function. Applying Theorem 4.12 leads to

$$\begin{aligned}\sum_{\substack{n\le x\\ \gcd(\varphi(n),q)=1}}\frac{\varphi(n)}{n} &= \sum_{d\le x}\frac{\mu(d)}{d}\left(c_q\frac{x/d}{(\log x/d)^{1/(q-1)}}\left(1+O_q\left(\frac{\log\log x/d}{\log x/d}\right)\right)\right)\\ &= c_q\frac{x}{(\log x)^{1/(q-1)}}\left(1+O_q\left(\frac{\log\log x}{\log x}\right)\right)\sum_{d\le x}\frac{\mu(d)}{d^2},\end{aligned}\tag{4.48}$$

where the implied constant absorbs a negligible dependence on d. Now, use Lemma **??** to approximate the finite sum as

$$\sum_{n\le x}\frac{\mu(n)}{n^2}=\frac{6}{\pi^2}+O\left(\frac{1}{x\log^2 x}\right)\tag{4.49}$$

and to complete the proof. ■

Theorem 4.14. *For large number $x\ge 1$, the average order of the Euler totient function $\varphi(n)$ over the subset $\mathcal{A}=\{n\ge 1:\gcd(\varphi(n),q)=1\}$ has the asymptotic formula*

$$\sum_{\substack{n\le x\\ \gcd(\varphi(n),q)=1}}\varphi(n)=\frac{3c_q}{\pi^2}\frac{x^2}{(\log x)^{1/(q-1)}}\left(1+O_q\left(\frac{\log\log x}{\log x}\right)\right),$$

where $c_q>0$ is a constant.

Proof. By Theorem 4.13, the appropiate measure is $W(x)=\sum_{n\le x,\gcd(\varphi(n),q)=1}\varphi(n)/n$,

and summation by part yields

$$\begin{aligned}
\sum_{\substack{n\le x\\ \gcd(\varphi(n),q)=1}} \varphi(n) &= \sum_{\substack{n\le x\\ \gcd(\varphi(n),q)=1}} n\cdot\frac{\varphi(n)}{n} \qquad (4.50)\\
&= \int_1^x t\, dW(t)\\
&= xW(x)+O(1)-\int_1^x W(t)dt\\
&= x\left(\frac{6c_q}{\pi^2}\frac{x}{(\log x)^{1/(q-1)}}\left(1+O_q\left(\frac{\log\log x}{\log x}\right)\right)\right)-\int_1^x W(t)dt\\
&= \frac{3c_q}{\pi^2}\frac{x}{(\log x)^{1/(q-1)}}\left(1+O_q\left(\frac{\log\log x}{\log x}\right)\right).
\end{aligned}$$

■

4.16 Problems

4.16.1 Estimates For Series And Finite Sums

Exercise 4.1. Show that there is a pair of constants $a, b > 0$ such that

$$a \log x \leq \sum_{n \leq x} \frac{\mu^2(n)}{\varphi(n)} \left\{ \frac{x}{n} \right\} \leq b \log x.$$

Exercise 4.2. Prove the estimate

$$\sum_{n>x} \frac{\mu^2(n)}{n\varphi(n)} = O\left(\frac{\log\log x}{x} \right).$$

Exercise 4.3. Estimate the finite sum, show that there is a pair of constants $a, b > 0$ such that

$$a \log x \leq \sum_{n \leq x} \frac{1}{n} \left\{ \frac{x}{\gamma(n)} \right\} \leq b \log x.$$

Exercise 4.4. Let $\gamma(n) = \prod_{p|n} p$ be the kernel of $n \geq 1$. Find a second method, refer to (**??**) for more details, to evaluate the series

$$\sum_{n \geq 1} \frac{1}{n\gamma(n)} = \frac{\zeta(2)\zeta(3)}{\zeta(6)}.$$

4.16.2 Extreme Values

Exercise 4.5. Let $x \geq 1$ be a large number, and let $n = 1 + \prod_{p \leq \log x} p$. Show that the lower bound

$$\varphi(n) \geq n - \frac{c_1 n}{\log\log n},$$

and

$$\varphi(n+1) \geq n/2 - \frac{c_2 n}{\log\log n},$$

with $c_1, c_2 > 0$ constants, hold.

Exercise 4.6. Find an upper bound of the form $c_0 + o(\log x)$, with $c_0 \neq 0$ constant, for the finite sum

$$\sum_{d \leq x} \frac{\mu(d)}{d} \left\{ \frac{x}{d} \right\} = O(1),$$

see Theorem 4.1.

4.16.3 Identities And Inverse Pairs

Exercise 4.7. Use the multiplicative properties of these arithmetic functions $\mu(n)$ and $\varphi(n)$ to convert the identity into a product and to show that

$$\frac{n}{\varphi(n)} = \sum_{d|n} \frac{\mu^2(n)}{\varphi(n)}.$$

Exercise 4.8. Let $p^k \,||\, n$ denote the maximal prime power divisor of n, (p-adic valuation $v_p(n) = k$). Prove the phi-sigma identity

$$\frac{\varphi(n)\sigma(n)}{n^2} = \prod_{p^\alpha || n} \left(1 - \frac{1}{p^{\alpha+1}}\right).$$

Exercise 4.9. Let $p^k \,||\, n$ denote the maximal prime power divisor of n, and let $s \in \mathbb{C}$ be a complex number. Prove a general version of the phi-sigma identity

$$\frac{\varphi_s(n)\sigma_s(n)}{n^2} = \prod_{p^\alpha || n} \left(1 - \frac{1}{p^{(\alpha+1)s}}\right).$$

Exercise 4.10. Prove the identity

$$\frac{n}{\varphi(n)} = \prod_{p|n} \left(1 - \frac{1}{p}\right)^{-1}.$$

Exercise 4.11. Prove the inverse Mobius functions pair

$$\sum_{d|n} \varphi(d) = n \quad \Longleftrightarrow \quad \varphi(n) = \sum_{d|n} \frac{\mu(d)}{d}.$$

Exercise 4.12. Let $\omega(n) = \#\{p \mid n : p \text{ prime divisor }\}$, and let $d(n) = \#\{d \mid n : d \text{ integer divisor}\}$. Prove the number of divisor identity

$$d(n) = \sum_{d^2|n} 2^{\omega(n/d^2)}.$$

4.16.4 Estimates For Finite Sums Over Primes

Exercise 4.13. Prove that the average order of the Euler totient function over the shifted primes satisfies

$$\sum_{p \le x} \frac{\varphi(p-a)}{p-a} = a_1 \operatorname{li}(x) + o\left(\operatorname{li}(x)\right),$$

$\operatorname{li}(x)$ is the logarithm function, and $a_1 = a_1(a) > 0$ is a constant depending on $a \ge 1$.

Exercise 4.14. Let $x \ge 1$ be a large number, and let $k \ge 1$ be an integer. Determine the optimal error term for

$$R_k(x) = \sum_{p \le x} \left(\frac{\varphi(p-1)}{p-1}\right)^k - a_k \frac{x}{\log x},$$

$a_k > 0$ is a constant, see Lemma 4.6 for more details.

Exercise 4.15. Prove that the average order of the Carmichael totient function over the shifted primes satisfies

$$\sum_{p\leq x}\frac{\lambda(p-a)}{p-a}=b_1\frac{\mathrm{li}(x)}{\log\log x}+o\left(\frac{\mathrm{li}(x)}{\log\log x}\right).$$

where $b_1=b_1(a)>0$ is a constant depending on $a\geq 1$, see [32, Theorem 1], and the more recent literature for impectus.

Exercise 4.16. Let $x\geq 1$ be a large number, and let $k\geq 1$ be an integer. Prove that the average order of the more general Carmichael totient function over the shifted primes satisfies

$$\sum_{p\leq x}\left(\frac{\lambda(p-a)}{p-a}\right)^k=b_k\frac{\mathrm{li}(x)}{\log\log x}+o\left(\frac{\mathrm{li}(x)}{\log\log x}\right).$$

where $b_k=b_k(a,k)>0$ is a constant depending on $a\geq 1$, and $k\geq 1$.

4.16.5 Totients Functions Relations

Exercise 4.17. Estimate the normal order of the totient ratio $\xi(n)=\varphi(n)/\lambda(n)$: For any number $\varepsilon>0$, there exists a function $f(n)$ such that

$$f(n)-\varepsilon\leq\xi(n)\leq f(n)+\varepsilon.$$

Exercise 4.18. Estimate the average order of the totient ratio $\xi(n)=\varphi(n)/\lambda(n)$ over the integers and over the shifted primes:

$$\sum_{n\leq x}\xi(n)=\sum_{n\leq x}\frac{\varphi(n)}{\lambda(n)}\qquad\text{and}\qquad\sum_{p\leq x}\xi(p-1)=\sum_{p\leq x}\frac{\varphi(p-1)}{\lambda(p-1)}.$$

Exercise 4.19. Estimate the average order of the inverse totient function over the integers and over the shifted primes:

$$\sum_{n\leq x}\frac{1}{\varphi(n)}\qquad\text{and}\qquad\sum_{p\leq x}\frac{1}{\varphi(p-1)}.$$

Exercise 4.20. Estimate the average order of the inverse lambda function over the integers and over the shifted primes:

$$\sum_{n\leq x}\frac{1}{\lambda(n)}\qquad\text{and}\qquad\sum_{p\leq x}\frac{1}{\lambda(p-1)}.$$

4.16.6 Open Problems

Exercise 4.21. (Carmichael problem) Define the value set (inverse image) of the totient function by

$$\varphi^{-1}(n)=\{m\geq 1:\varphi(n)=m\}=V_n.$$

Prove that $\#V_n>1$ for all integers $n\geq 1$.

Exercise 4.22. Let $1 \leq a < q$ be a pair of relatively prime integers. Estimate the summatory Carmichael function

$$\sum_{\substack{n \leq x \\ n \equiv a \bmod q}} \lambda(n).$$

Exercise 4.23. Let $a \neq 0$ be a fixed integer. Estimate the Carmichael correlation function

$$\sum_{n \leq x} \lambda(n)\lambda(n+a).$$

Exercise 4.24. (Lehmer conjecture) Let $n \geq 1$ be an integer, and let φ be the totient function. Prove that $\varphi(n) \mid n-1$ if and only if n is prime.

Chapter 5

Generating Series Of Totients Functions

5.1 Generating Series For $\varphi(n)^k$

The generating series for a score of Euler totient function related arithmetic functions are computed in this section.

Lemma 5.1. *For a complex number $s \in \mathbb{C}$, the generating series for the Euler totient function $\varphi(n)^k$, with $k \geq 1$, has the followings representations.*

$$\text{(i)} \quad \sum_{n\geq 1} \frac{\varphi(n)^k}{n^s} = \zeta(s) \prod_{p\geq 2} \left(1 - \frac{1}{p^s} + \frac{(1-1/p)^k(p^s-1)}{p^s(p^{s-k}-1)}\right).$$

$$\text{(ii)} \quad \sum_{n\geq 1} \frac{\varphi(n)^k}{n^s} = \frac{1}{\zeta(s)} \prod_{p\geq 2} \left(1 + \frac{1}{p^s-1} + \frac{(1-1/p)^k p^s}{(p^s-1)(p^{s-k}-1)}\right).$$

The first representation is absolutely convergent for $\mathcal{R}e(s) > k+1$. It has simple pole at $s = 0$, $s = 1$, and $s = k+1$. But, the simple poles at the the zeros $\rho = \beta + it$ of the zeta function are not visible. While, the second is absolutely convergent for $\mathcal{R}e(s) > k+1$, and has simple poles at $s = 0$, $s = 1$, and $s = k+1$. In addition, the simple poles at the the zeros $\rho = \beta + it$ of the zeta function are visible.

Proof. Begin with the value $\varphi(p^v) = p^v(1-1/p)$ at the prime $p^v \geq 2$, with $v \geq 1$.

The first representation has product expansion

$$\begin{aligned}\sum_{n\geq 1}\frac{(\varphi(n)/n)^k}{n^{s-k}} &= \prod_{p\geq 2}\left(1+\frac{(1-1/p)^k}{p^{s-k}}+\frac{(1-1/p)^k}{p^{2(s-k)}}+\frac{(1-1/p)^k}{p^{3(s-k)}}+\cdots\right)\\ &= \prod_{p\geq 2}\left(1+\frac{(1-1/p)^k}{p^{s-k}-1}\right)\\ &= \zeta(s)\prod_{p\geq 2}\left(1-\frac{1}{p^s}\right)\prod_{p\geq 2}\left(1+\frac{(1-1/p)^k}{p^{s-k}-1}\right)\\ &= \zeta(s)\prod_{p\geq 2}\left(1-\frac{1}{p^s}+\frac{(1-1/p)^k(p^s-1)}{p^s(p^{s-k}-1)}\right). \qquad (5.1)\end{aligned}$$

The third line uses the geometric series to simplify the infinite sum, the fourth line introduces a zeta term, and the two products are merged into one product on the last line. For the second representation uses the inverse zeta in the fourth line.

The first generating series is absolutely convergent for $\mathcal{R}e(s) > k+1$. There are simple poles at $s=0$, $s=1$, and $s=2$. But, the simple poles at the the zeros $\rho=\beta+it$ of the zeta function are not visible. While, the second representation has simple poles at $s=0$, $s=1$, and $s=2$. In addition, the simple poles at the zeros $\rho=\beta+it$ of the zeta function are visible. ■

The case $k=1$ reduces to

$$\sum_{n\geq 1}\frac{\varphi(n)}{n^s}=\zeta(s)\prod_{p\geq 2}\left(1-\frac{1}{p^s}+\frac{(1-1/p)(p^s-1)}{p^s(p^{s-1}-1)}\right). \qquad (5.2)$$

It is absolutely convergent for $\mathcal{R}e(s)>2$. It has simple poles at $s=1$, and $s=2$. But, the simple poles at the zeros $\rho=\beta+it$ of the zeta function, but not visible.

In this case, there is another simple derivation due to the identity $\sum_{d|n}\varphi(d)=n$. It reduces to

$$g(s)=\sum_{n\geq 1}\frac{\varphi(n)}{n^s}=\frac{\zeta(s-1)}{\zeta(s)}, \qquad (5.3)$$

where $s\in\mathbb{C}$, see Exercise 6.3. It visibly shows that it has simple pole at $s=2$, and the zeros $\rho=\beta+it$ of the zeta function. It should have a pole at $s=1$ to match the representation in (5.2), but it is not easy to verify.

5.2 The Generating Series For $\varphi(n)/n$

The generating series for the ratio $\varphi(n)/n$ is slightly simpler than for $\varphi(n)$, this is given below.

Lemma 5.2. *For a complex number $s\in\mathbb{C}$, the generating series for the ratio $(\varphi(n)/n)^k$, with $k\geq 1$, has the followings representations.*

(i) $$\sum_{n\geq 1}\frac{(\varphi(n)/n)^k}{n^s}=\zeta(s)\prod_{p\geq 2}\left(1-\frac{1}{p^s}+\frac{(1-1/p)^k}{p^s}\right).$$

(ii) $$\sum_{n\geq 1}\frac{(\varphi(n)/n)^k}{n^s}=\frac{1}{\zeta(s)}\prod_{p\geq 2}\left(1+\frac{1}{p^s-1}+\frac{(1-1/p)^k p^s}{(p^s-1)^2}\right).$$

Proof. Observe that $\varphi(p^v)/p^v=1-1/p$ at the prime power $p^v\geq 2$, with $v\geq 1$. Thus, the first representation has the product expansion

$$\begin{aligned}\sum_{n\geq 1}\frac{(\varphi(n)/n)^k}{n^s} &= \prod_{p\geq 2}\left(1+\frac{(1-1/p)^k}{p^s}+\frac{(1-1/p)^k}{p^{2s}}+\frac{(1-1/p)^k}{p^{3s}}+\cdots\right)\\ &= \prod_{p\geq 2}\left(1+\frac{(1-1/p)^k}{p^s-1}\right)\\ &= \zeta(s)\prod_{p\geq 2}\left(1-\frac{1}{p^s}\right)\prod_{p\geq 2}\left(1+\frac{(1-1/p)^k}{p^s-1}\right)\\ &= \zeta(s)\prod_{p\geq 2}\left(1-\frac{1}{p^s}+\frac{(1-1/p)^k}{p^s}\right). \qquad (5.4)\end{aligned}$$

The third line uses the geometric series to simplify the infinite sum, the fourth line introduces a zeta term, and the two products are merged into one product on the last line. For the second representation uses the inverse zeta in the fourth line.

The first representation is absolutely convergent for $\mathcal{R}e(s)>k+1$. It has simple poles at $s=0$ and $s=1$. But, the simple poles at the zeros $\rho=\beta+it$ of the zeta function are not visible. While the second representation is absolutely convergent for $\mathcal{R}e(s)>k+1$. It has simple poles at $s=0$ and $s=1$. In addition, the simple poles at the zeros $\rho=\beta+it$ of the zeta function are visible. ■

The case $k=1$ reduces to

$$g(s)=\sum_{n\geq 1}\frac{\varphi(n)/n}{n^s}=\zeta(s)\prod_{p\geq 2}\left(1-\frac{1}{p^s}+\frac{p-1}{p^{s+1}}\right), \qquad (5.5)$$

where $s\in\mathbb{C}$. The simple poles at $s=0$ and $s=1$ occur on the product and the zeta function respectively.

5.3 The Generating Function For $n/\varphi(n)$

The generating series for the ratio $n/\varphi(n)$ has various representations. Two of these will be derived here. These are useful for verifying different properties of the series and the summatory function $\sum_{n\leq x}(n/\varphi(n))^k$.

Lemma 5.3. *For a complex number $s\in\mathbb{C}$, the generating series for the ratio $(n/\varphi(n))^k$, with $k\geq 1$, has the followings representations.*

(i) $$\sum_{n\geq 1}\frac{(n/\varphi(n))^k}{n^s}=\zeta(s)\prod_{p\geq 2}\left(1-\frac{1}{p^s}+\frac{(1-1/p)^{-k}}{p^s}\right).$$

(ii) $$\sum_{n\geq 1}\frac{(n/\varphi(n))^k}{n^s}=\frac{1}{\zeta(s)}\prod_{p\geq 2}\left(1+\frac{1}{p^s-1}+\frac{(1-1/p)^{-k}p^s}{(p^s-1)^2}\right).$$

Proof. Begin with the value $p^v/\varphi(p^v)=(1-1/p)^{-1}$ at the prime power $p^v\geq 2$, with $v\geq 1$. The product representation has the expansion

$$\begin{aligned}\sum_{n\geq 1}\frac{(n/\varphi(n))^k}{n^s} &= \prod_{p\geq 2}\left(1+\frac{(1-1/p)^{-k}}{p^s}+\frac{(1-1/p)^{-k}}{p^{2s}}+\frac{(1-1/p)^{-k}}{p^{3s}}+\cdots\right)\\ &= \prod_{p\geq 2}\left(1+\frac{(1-1/p)^{-k}}{p^s-1}\right)\\ &= \zeta(s)\prod_{p\geq 2}\left(1-\frac{1}{p^s}\right)\prod_{p\geq 2}\left(1+\frac{(1-1/p)^{-k}}{p^s-1}\right)\\ &= \zeta(s)\prod_{p\geq 2}\left(1+\frac{1}{p^s-1}+\frac{(1-1/p)^{-k}}{p^s}\right). \qquad (5.6)\end{aligned}$$

The third line uses the geometric series to simplify the infinite sum, the fourth line introduces a zeta term, and the two products are merged into one product on the last line. For the second representation uses the inverse zeta in the fourth line.

The first representation is absolutely convergent for $\mathcal{R}e(s)>1$. It has simple poles at $s=0$ and $s=1$. But, the simple poles at the zeros $\rho=\beta+it$ of the zeta function are not visible. While the second representation is absolutely convergent for $\mathcal{R}e(s)>1$. It has simple poles at $s=0$ and $s=1$. In addition, the simple poles at the zeros $\rho=\beta+it$ of the zeta function are visible. ■

The case $k=1$ is simpler and reduces to

$$g(s)=\sum_{n\geq 1}\frac{n/\varphi(n)}{n^s}=\zeta(s)\prod_{p\geq 2}\left(1+\frac{1}{p^s(p-1)}\right), \qquad (5.7)$$

where $s\in\mathbb{C}$. The product shows a simple poles at $s=0$ and $s=1$. But, the simple poles at the zeros $\rho=\beta+it$ of the zeta function are not visible. The analysis for $k=2$ appears in [25, p. 338]. In particular,

$$g(s)=\sum_{n\geq 1}\frac{(n/\varphi(n))^2}{n^s}=\zeta(s)\prod_{p\geq 2}\left(1+\frac{p-2}{p^{s+2}}\right). \qquad (5.8)$$

5.4 Problems

Exercise 5.1. Show that for $k \geq 1$, the series can be approximated by

$$g(s) = \sum_{n\geq 1} \frac{(\sigma(n)/n)^k}{n^s} = \zeta(s) \prod_{p\geq 2} \left(1 + \frac{k}{p^{s+1}} + \frac{k-1}{p^{2s+1}} + O\left(\frac{1}{p^{2s+1}}\right)\right),$$

where $s \in \mathbb{C}$. Verify that it has simple poles at $s = 0$ and $s = 1$, these occur on the product and the zeta function respectively.

Exercise 5.2. Show that for $k = 2$, the residue of the complex function $g(s)/\zeta(s)$ at $s = 1$ is given by the product evaluated at $s = 1$. More precisely, taking the limit as $s \to 1$, this is

$$\frac{1}{\zeta(1)} \sum_{n\geq 1} \frac{(\sigma(n)/n)^2}{n} = \prod_{p\geq 2} \left(1 + \frac{2}{p^2} + \frac{1}{p^3} + \sum_{n\geq 2} \frac{\left(\sum_{0\leq m\leq m} p^{-m}\right)^2 - \left(\sum_{0\leq m<m} p^{-m}\right)^2}{p^n}\right),$$

see [25, p. 338] for other related details.

Exercise 5.3. Show that the generating series for the Euler totient function $\varphi(n)^k$, with $k \geq 1$, is

$$\sum_{n\geq 1} \frac{\varphi(n)^k}{n^s} = \prod_{p\geq 2} \left(1 + \sum_{m\geq 1} \frac{\sum_{d|p^m} \varphi(d)^k}{p^{ms}}\right),$$

where $s \in \mathbb{C}$ is a complex number, is absolutely convergent for $\mathcal{R}e(s) > k+1$. HinT: Take the Dirichlet convolution of the two series

$$\begin{aligned} \sum_{n\geq 1} \frac{1}{n^s} \sum_{n\geq 1} \frac{\varphi(n)^k}{n^s} &= \sum_{n\geq 1} \frac{\sum_{d|n} \varphi(d)^k}{n^s} \\ &= \prod_{p\geq 2} \left(1 + \sum_{m\geq 1} \frac{\sum_{d|p^m} \varphi(d)^k}{p^{ms}}\right). \end{aligned}$$

Chapter 6

Explicit Formulas Method

The generating series method is a powerful technique for estimating or computing the asymptotic formulas for the average orders of arithmetic functions.

The generating series for the ratio $(n/\varphi(n))^k$ has negligible dependence on the zeros of the zeta function. Accordingly, the corresponding summatory function for this ratio has small error terms of polynomial magnitude as a function of x, not exponentially large.

In contrast, the generating series for the inverse ratio $(n/\varphi(n))^k$ is dependent of the zeros of the zeta function. Accordingly, the corresponding summatory function has large error terms of exponential magnitudes as functions of x, not polynomially large.

6.1 The Ratio $\varphi(n)/n$

The explicit formula for the ratio $\varphi(n)/n$ has representation as a meromorphic function

$$\begin{aligned} f(z) &= \int_{\mathcal{C}} \frac{\zeta(s-1)}{\zeta(s)} e^{sz} ds \qquad (6.1) \\ &= \lim_{T_n \to \infty} \sum_{0 < \Im m(\rho) < T_n} \frac{1}{(k-1)!} \frac{d^{(k-1}}{ds^{(k-1}} (s-\rho) \frac{\zeta(s-1)}{\zeta'(s)} e^{sz} \Bigg|_{s=\rho}, \end{aligned}$$

where $\mathcal{C}$ is a curve on the complex plane, $T_n \to \infty$ is a sequence of numbers, $k = k_\rho \geq 1$ is the multiplicity of the zero ρ, and $z \in \mathbb{C}$, with $\Re e(z) > 0$, is a complex number, confer [100]. The expression collapses to

$$f(z) = \int_{\mathcal{C}} \frac{\zeta(s-1)}{\zeta(s)} e^{sz} ds = \lim_{T_n \to \infty} \sum_{0 < \Im m(\rho) < T_n} \frac{\zeta(s-1)}{\zeta'(s)} e^{sz} \qquad (6.2)$$

whenever the zeros are simple.

Theorem 6.1. *Let $x \geq 1$ be a large number. Then, the average order of the ratio $(\varphi(n)/n)^k$, with $k \geq 1$, is*

$$\sum_{n\leq x}\left(\frac{\varphi(n)}{n}\right)^k = x\prod_{p\geq 2}\left(1+\frac{p^k-(p-1)^k}{p(p-1)^k}\right)+a_k+O(\log x),$$

where a_k is a constant.

Proof. The result is derived using the generating series and the Perron formula. Let $g(s)=\zeta(s)\prod_{p\geq 2}\left(1+\frac{p^k-(p-1)^k}{p^s(p-1)^k}\right)$. Since the product has a pole at $s=0$, it can be expressed in the form

$$g(s)=\zeta(s)\prod_{p\geq 2}\left(1+\frac{p^k-(p-1)^k}{p^s(p-1)^k}\right)=\zeta(s)\frac{f(s)}{s}, \tag{6.3}$$

where $f(s)$ is a holomorphic function for any complex number $s\in\mathbb{C}$. Hence, the function

$$g(s)\frac{x^s}{s}=\zeta(s)f(s)\frac{x^s}{s^2} \tag{6.4}$$

has a simple pole at $s=1$ and a double pole at $s=0$. Therefore, the Perron formula yields

$$\begin{aligned}\sum_{n\leq x}\left(\frac{n}{\varphi(n)}\right)^k &= \frac{1}{i2\pi}\int_{c-i}^{c+i} f(s)\frac{x^s}{s}ds &(6.5)\\ &= x\prod_{p\geq 2}\left(1+\frac{p^k-(p-1)^k}{p(p-1)^k}\right)+c_1+O(\log x), &(6.6)\end{aligned}$$

with c_1 constant.

■

The analysis for $k=2$ appears in [25, p. 337], and the constant

$$d_1=\prod_{p\geq 2}\left(1-\frac{2}{p^2}+\frac{1}{p^3}\right). \tag{6.7}$$

6.2 Explicit Formula For The Ratio $n/\varphi(n)$

Theorem 6.2. *Let $x\geq 1$ be a large number. Then, the explicit formula for the ratio $n/\varphi(n)$ is*

$$\sum_{n\leq x}\frac{n}{\varphi(n)}=a_0+a_1x+\sum_{\zeta(\rho)=0}\frac{x^\rho}{\rho}-\sum_{n\geq 1}\frac{x^{-2n}}{2n},$$

where $a_0, a_1=\zeta(2)\zeta(3)\zeta(6)$ are constants.

Proof. The result is derived using the generating series and the Perron formula. The generating series $g(s) = \zeta(s)\prod_{p\geq 2}\left(1+\frac{1}{p^s(p-1)}\right)$ has a simple pole at $s=0$, and at $s=1$. Hence, the function

$$f(s) = g(s)\frac{x^s}{s} = \frac{\zeta(s)x^s}{s}\prod_{p\geq 2}\left(1+\frac{1}{p^s(p-1)}\right) \tag{6.8}$$

has a double pole at $s=0$, and simple pole at $s=1$. The nontrivial zeros $\rho=\beta+it$, and the trivial zeros $\rho=-2n$ of the zeta function contributes to the error term. Therefore, the Perron formula yields

$$\begin{aligned}\sum_{n\leq x}\frac{n}{\varphi(n)} &= \frac{1}{i2\pi}\int_{c-i\infty}^{c+i\infty} g(s)\frac{x^s}{s}ds \\ &= a_0 + a_1 x + \sum_{\rho}\frac{x^\rho}{\rho} + \sum_{n\geq 1}\frac{x^{-2n}}{-2n},\end{aligned} \tag{6.9}$$

where $a_0, a_1 \in \mathbb{C}$ are constants. ■

6.3 Average Orders

An application the explicit formula in Theorem 6.2 is considered here.

Lemma 6.1. *Let $x\geq 1$ be a large number, and let $\varepsilon>0$ be a small number. Then, the average orders of the ratio $n/\varphi(n)$ are the followings.*

(i) $\displaystyle\sum_{n\leq x}\frac{n}{\varphi(n)} = a_0 + a_1 x + O\left(xe^{-c\sqrt{\log x}}\right)$, *unconditionally.*

(ii) $\displaystyle\sum_{n\leq x}\frac{n}{\varphi(n)} = a_0 + a_1 x + O\left(x^{1/2+\varepsilon}\right)$, *conditional on RH.*

where $c>0$ is an absolute constant, and $a_0, a_1 \in \mathbb{C}$ are constants.

Proof. To prove the first statement, assume the zerofree region $\{\Re e(s) > 1 - O(1/\log x)\}$ of the zeta function $\zeta(s)$. The contribution from the nontrivial zeros of the zeta function is

$$\sum_{\zeta(\rho)=0}\frac{x^\rho}{\rho} = O\left(xe^{-c\sqrt{\log x}}\right). \tag{6.10}$$

The right side is derived from a standard zerofree region near the line $\Re e(s)=1$ of the zeta function. Moreover, the contribution from the trivial zeros is

$$\sum_{n\geq 1}\frac{x^{-2n}}{-2n} = -\log\left(1-\frac{1}{x^2}\right) = O(\log x). \tag{6.11}$$

The combined estimate proves the claim. For the second statement use the zerofree region $\{\Re e(s) > 1/2\}$. ■

Theorem 6.3. *Let $x \geq 1$ be a large number. Then, the average order of the ratio $1/\varphi(n)$ is as follows.*

(i) $\displaystyle\sum_{n\leq x} \frac{1}{\varphi(n)} = c_0 + c_1 \log x + O\left((\log x)e^{-c\sqrt{\log x}}\right)$, *unconditionally.*

(ii) $\displaystyle\sum_{n\leq x} \frac{1}{\varphi(n)} = c_0 + c_1 x + O\left(x^{-1/2+\varepsilon}\right)$, *conditional on RH.*

where c_0 and c_1 are constants, and $c > 0$ is an absolute constant.

Proof. The result is derived by partial summation. More precisely, let $R(t) = \sum_{n\leq x} n/\varphi(n)$. Then

$$\begin{aligned}
\sum_{n\leq x} \frac{1}{\varphi(n)} &= \sum_{n\leq x} \frac{1}{n}\frac{n}{\varphi(n)} \\
&= \int_1^x \frac{1}{t} dR(t) \qquad (6.12)\\
&= \frac{R(t)}{t}\Bigg|_1^x + \int_1^x \frac{R(t)}{t^2} dt, \\
&= \frac{a_0 + a_1 x + O\left(xe^{-c\sqrt{\log x}}\right)}{x} - R(1) + \int_1^x \frac{a_0 + a_1 t + O\left(te^{-c\sqrt{\log t}}\right)}{t^2} dt, \\
&= c_0 + c_1 \log x + O\left((\log x)e^{-c\sqrt{\log x}}\right),
\end{aligned}$$

where c_0 and c_1 are constants, and $c > 0$ is an absolute constant. ■

Theorem 6.4. *Let $x \geq 1$ be a large number. Then, the average order of the ratio $(n/\varphi(n))^k$, with $k \geq 1$, is*

$$\sum_{n\leq x} \left(\frac{n}{\varphi(n)}\right)^k = x \prod_{p\geq 2} \left(1 + \frac{p^k - (p-1)^k}{p(p-1)^k}\right) + c_k + O(\log x),$$

where c_k is a constant.

Proof. The result is derived using the generating series and the Perron formula. Let $g(s) = \zeta(s) \prod_{p\geq 2} \left(1 + \frac{p^k-(p-1)^k}{p^s(p-1)^k}\right)$. Since the product has a pole at $s = 0$, it can be expressed in the form

$$g(s) = \zeta(s) \prod_{p\geq 2} \left(1 + \frac{p^k - (p-1)^k}{p^s(p-1)^k}\right) = \zeta(s)\frac{f(s)}{s}, \qquad (6.13)$$

where $f(s)$ is a holomorphic function for any complex number $s \in \mathbb{C}$plane. Hence, the function

$$g(s)\frac{x^s}{s} = \zeta(s)f(s)\frac{x^s}{s^2} \qquad (6.14)$$

has a simple pole at $s = 1$ and a double pole at $s = 0$. Therefore, the Perron formula yields

$$\sum_{n \le x} \left(\frac{n}{\varphi(n)} \right)^k = \frac{1}{i2\pi} \int_{c-i\infty}^{c+i\infty} \zeta(s) f(s) \frac{x^s}{s^2} ds \tag{6.15}$$

$$= x \prod_{p \ge 2} \left(1 + \frac{p^k - (p-1)^k}{p(p-1)^k} \right) + c_k + O(\log x), \tag{6.16}$$

with c_k constant.

■

6.4 Problems

Exercise 6.1. Show that for $k \geq 1$, the series can be approximated by

$$g(s) = \sum_{n\geq 1} \frac{(\sigma(n)/n)^k}{n^s} = \zeta(s) \prod_{p\geq 2} \left(1 + \frac{k}{p^{s+1}} + \frac{k-1}{p^{2s+1}} + O\left(\frac{1}{p^{2s+1}}\right)\right),$$

where $s \in \mathbb{C}$. Verify that it has simple poles at $s = 0$ and $s = 1$, these occur on the product and the zeta function respectively.

Exercise 6.2. Show that for $k = 2$, the residue of the complex function $g(s)/\zeta(s)$ at $s = 1$ is given by the product evaluated at $s = 1$. More precisely, taking the limit as $s \to 1$, this is

$$\frac{1}{\zeta(1)} \sum_{n\geq 1} \frac{(\sigma(n)/n)^2}{n} = \prod_{p\geq 2} \left(1 + \frac{2}{p^2} + \frac{1}{p^3} + \sum_{n\geq 2} \frac{\left(\sum_{0\leq m\leq m} p^{-m}\right)^2 - \left(\sum_{0\leq m<m} p^{-m}\right)^2}{p^n}\right),$$

see [25, p. 338] for other related details.

Exercise 6.3. Show that the generating series for the Euler totient function $\varphi(n)^k$, with $k \geq 1$, is

$$\sum_{n\geq 1} \frac{\varphi(n)^k}{n^s} = \prod_{p\geq 2} \left(1 + \sum_{m\geq 1} \frac{\sum_{d|p^m} \varphi(d)^k}{p^{ms}}\right),$$

where $s \in \mathbb{C}$ is a complex number, is absolutely convergent for $\mathcal{R}e(s) > k+1$. Hint: Take the Dirichlet convolution of the two series

$$\begin{aligned} \sum_{n\geq 1} \frac{1}{n^s} \sum_{n\geq 1} \frac{\varphi(n)^k}{n^s} &= \sum_{n\geq 1} \frac{\sum_{d|n} \varphi(d)^k}{n^s} \\ &= \prod_{p\geq 2} \left(1 + \sum_{m\geq 1} \frac{\sum_{d|p^m} \varphi(d)^k}{p^{ms}}\right). \end{aligned}$$

Chapter 7

Sets Of s-Powerfree Integers

7.1 Summatory Functions For Squarefree Integers

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

$$\mathcal{Q}_2 = \{n \in \mathbb{Z} : \mu^2(n) \neq 0\} \tag{7.1}$$

and the complementary subset of non squarefree integers is denoted by

$$\overline{\mathcal{Q}_2} = \{n \in \mathbb{Z} : \mu^2(n) = 0\}. \tag{7.2}$$

The number of squarefree integers have the following asymptotic formulas.

Lemma 7.1. *Let $\mu : \mathbb{Z} \longrightarrow \{-1, 0, 1\}$ be the Mobius function. Then, for any sufficiently large number $x \geq 1$,*

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

Proof. Use Lemma 3.4 or confer to the literature. ■

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

$$\frac{6}{\pi^2} = \prod_{q \geq 2} \left(1 - \frac{1}{q^2}\right) = 0.60798829516462761713575 4\ldots, \tag{7.3}$$

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

$$R(x) = \sum_{n \leq x} \mu^2(n) - \frac{6}{\pi^2} x \tag{7.4}$$

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

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

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

$$\sum_{n \leq x} \mu^2(n) = \frac{1}{i2\pi} \int_{c-\infty}^{c+\infty} \frac{\zeta(s)}{\zeta(s)} \frac{x^s}{s} ds = \frac{1}{\zeta(2)} x + \sum_{\zeta(\rho)=0} c_\rho x^{\rho/2}, \tag{7.5}$$

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 7.1. *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,*

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

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

Proof. Consult [56], [120], and the literature. ■

The range of moduli $q \leq x^{2/3}$ is discussed and improved to $q \leq x^{1-\varepsilon}$ in [88]. The q-dependence in the constant

$$\frac{1}{q} \sum_{\substack{n \geq 1 \\ \gcd(n,q)=1}} \frac{\mu(n)}{n^2} = \frac{1}{q} \prod_{p \nmid q} \left(1 - \frac{1}{p^2}\right) = \frac{6}{\pi^2} \frac{1}{q} \prod_{p \mid q} \left(1 - \frac{1}{p^2}\right)^{-1} \tag{7.6}$$

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 $(6/\pi^2)^2$, but a more complicated expression similar to (7.6). 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 7.2. *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,*

$$\sum_{q \leq x^{2/3} \log^{-c-1} x} \max_{a \bmod q} \left| \sum_{\substack{n \leq x \\ n \equiv a \bmod q}} \mu(n)^2 - \frac{\varphi(q)}{d\varphi(q/d)} \prod_{p \nmid q} \left(1 - \frac{1}{p^2}\right) \frac{x}{q} \right| \ll \frac{x}{\log^c x}, \tag{7.7}$$

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

Proof. Consult [90] and the literature. ■

Lemma 7.3. *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,*

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

Proof. The proof is lengthier and more difficult than Lemma 7.1, see [26, Lemma 2]. ■

7.2 Correlation Functions For Squarefree Integers

A sequence of squarefree integers

$$n + a_0, \quad n + a_1, \quad n + a_2, \quad \ldots, \quad n + a_k, \tag{7.8}$$

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 [7], and the literature for extensive details.

Definition 7.1. 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 7.4. *Let $x \geq 1$ be a large number, and let $\mu : \mathbb{Z} \longrightarrow \{-1, 0, 1\}$ be the Mobius function. Then,*

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

Proof. The earliest proof seems to be that in [13], and [79]. Recent proofs appear in [78], and the literature. ■

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

$$\prod_{q \geq 2} \left(1 - \frac{2}{q^2}\right) = 0.32269905424253557616148 3\ldots, \tag{7.9}$$

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

Lemma 7.5. *Let $x \geq 1$ be a large number, and let $\mu : \mathbb{Z} \longrightarrow \{-1, 0, 1\}$ be the Mobius function. Then,*

$$\sum_{n \leq x} \mu(n)^2 \mu(n+1)^2 \mu(n+2)^2 = \prod_{p \geq 2} \left(1 - \frac{3}{p^2}\right) x + O\left(x^{2/3}\right). \tag{7.10}$$

The earliest result in this direction appears to be

$$\sum_{n\leq x}\mu(n)^2\mu(n+t)^2 = cx + O\left(x^{2/3}\right), \tag{7.11}$$

where $c > 0$ is the constant (7.3), is studied in [79]. Except for minor adjustments, the generalization to sequences of $(k+1)$-tuples of squarefree integers has the same structure.

Theorem 7.3. *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,*

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

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

$$\rho(s) = \#\{m \leq p^2 : qm + a_i \equiv 0 \bmod p^2 \text{ for } i = 0, 1, 2, ..., k\}, \tag{7.12}$$

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

Proof. Consult [79], [78, Theorem 1.2], [113], 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 7.1. *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,*

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

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.

7.3 Summatory Functions For s-Power Free Integers

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

$$\mathcal{Q}_s = \{n \in \mathbb{Z} : \mu_s(n) \neq 0\} \tag{7.13}$$

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

$$\overline{\mathcal{Q}_s} = \{n \in \mathbb{Z} : \mu_s(n) = 0\}. \tag{7.14}$$

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

Lemma 7.6. *Given an integer $s \geq 2$, let $\mu_s(n)$ be the sth-Mobius function. Then, for any sufficiently large number $x \geq 1$,*

$$\sum_{n \leq x} \mu_s(n) = \frac{1}{\zeta(s)} x + O\left(x^{1/s}\right). \tag{7.15}$$

Proof. The basic sth-Mobius function μ_s is explained in Definition 3.5. This result is attributed to Gegenbauer, 1885. Recent proofs are provided in [64] and the literature. ■

Lemma 7.7. *Given an integer $s \geq 2$, let $\mu_s(n)$ be the sth-Mobius function. Then, for any sufficiently large number $x \geq 1$,*

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

Proof. Same as the proof of Lemma 7.2, mutatis mutandus. ■

Conjecture 7.2. *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 $x \geq 1$,*

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

7.4 Correlation Functions For s-Power Free Integers

Theorem 7.4. *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,*

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

where

$$\rho(p) = \begin{cases} 2 & \text{if } p^s \nmid a, \\ 1 & \text{if } p^s \mid a, \end{cases} \tag{7.16}$$

and

$$\alpha(p,a) = \frac{14}{7s+8} \tag{7.17}$$

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

Proof. Different proofs are given in [102], [4, 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

$$R_s(x) = \sum_{n \leq x} \mu_s(n) - \frac{1}{\zeta(2s)} x \tag{7.18}$$

in Theorem 7.4 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 [93]. 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 $a \geq 1$. A plausible result might have the form given below.

Conjecture 7.3. *Given a pair of integers $a \geq 1$ and $s \geq 2$. Let $x \geq 1$ be a large number, and let $\mu : \mathbb{Z} \longrightarrow \{-1, 0, 1\}$ be the Mobius function. If $a \geq 1$, and $q = O(\log^c x)$ with $c \geq 0$ constant, then,*

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

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

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

7.5 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 7.4. Specifically,

$$\prod_{q\geq 2}\left(1-\frac{2}{q^2}\right) = \left(\frac{6}{\pi^2}\right)^2\prod_{q\geq 2}\left(1+\frac{1}{q^2(q^2-2)}\right)^{-1} = 0.32269905424253557616148 3\ldots. \tag{7.19}$$

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

$$c_2(2) = \prod_{q\geq 2}\left(1+\frac{1}{q^2(q^2-2)}\right)^{-1} = 0.87298595344931361877174 5\ldots. \tag{7.20}$$

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 7.5. Specifically,

$$\prod_{q\geq 2}\left(1-\frac{3}{q^2}\right) = \left(\frac{6}{\pi^2}\right)^3\prod_{q\geq 2}\left(1+\frac{3q^2-1}{q^4(q^2-3)}\right)^{-1} = 0.12552487889682122018468 3\ldots. \tag{7.21}$$

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

$$c_2(3) = \prod_{q\geq 2}\left(1+\frac{3q^2-1}{q^4(q^2-3)}\right)^{-1} = 0.558526979127689105533330\ldots. \tag{7.22}$$

Accordingly, consecutive squarefree integers are highly correlated.

Chapter 8

Sets Of Smooth Integers

8.1 Smooth Integers

For an integer $n \in \mathbb{N}$, the largest prime divisor is denoted by $p = P(n)$. Let $x \geq 1$ be a real number, and let $B = x^{1/u}$, where $u > 0$. The subset of B-smooth integers is defined by

$$\mathcal{R}_{\mathcal{B}} = \{n \in \mathbb{N} : p = P(n)\}, \tag{8.1}$$

where $p = P(n) \leq B$ and is a prime.

Theorem 8.1. *The number of B-smooth integers has the aymptotic*

$$\Psi(x, B) = \rho(u)x + (1-\gamma)\frac{\rho(u-1)x}{\log x} + O\left(\frac{\rho(u)\log(u)^2u^2x}{(\log x)^2}\right),$$

where $\gamma = 0.5772\ldots$.

The density of B-smooth integers can be approximated as

$$\rho(u) = \begin{cases} 1 & \text{if } 0 < u \leq 1, \\ 1 - \log u & \text{if } 1 \leq u \leq 2, \\ u^{-u+o(1)} & \text{if } 2 \leq u \leq \infty. \end{cases} \tag{8.2}$$

The analytical formulas for small values $B \ll (\log x)^C$, where $C > 0$ is a arbitrary constant, are conditional on some standard conjectures.

8.2 Smooth And Nonsmooth Numbers In Short Intervals

For a large number $x \geq 1$, and $2 \leq z \leq x$, the subset of smooth numbers is defined by

$$\mathcal{S}(z) = \{n \geq 1 : P(n) \leq z\} \tag{8.3}$$

where $P(n) = \max\{p \,|\, n\}$ is the largest prime divisor of $n \geq 1$. The corresponding counting function is given by

$$\Psi(x, y) = \#\{n \leq x : P(n) \leq y\} \sim \rho x, \tag{8.4}$$

where $\rho(u) \geq 0$ is the density of smooth numbers. Some interesting applications of smooth numbers in short intervals call for estimates of the forms

$$\Psi(x + x^\beta, x^\alpha) - \Psi(x, x^\alpha) \sim \rho(1/\alpha)x^\beta, \tag{8.5}$$

with $1 \leq x^\alpha \leq x^\beta \leq x$, as $x \to \infty$, and $\alpha > 0$ and $\beta > 0$. A rich assortment of results for various ranges of the parameters x, y, z in $\Psi(x + y, z) - \Psi(x, z) > 0$ are proved in the literature.

For parameters of nonexponential sizes there are very few results, see [39, Conjecture 1]. Neither conditional nor unconditional results for the extreme cases

$$\Psi(x + \log^B x, \log^C x) - \Psi(x, \log^C x) \gg \log^D x, \tag{8.6}$$

where $B, C, D > 0$, are expected to be proved in the near future. The interested reader should refer to [**?**] for a comprehensive introduction to this topic.

Theorem 8.2. ([34]) *Let $x \geq 1$ be a large number, and let $\beta \geq \alpha > 0$. Then,*

$$\Psi(x + x^\beta, x^\alpha) - \Psi(x, x^\alpha) \leq \frac{1}{\alpha}x^\beta + c_0\pi_(x^\alpha).$$

as $x \to \infty$.

Theorem 8.3. ([39, Theorem 2.4]) *There exist nonnegative absolute constants ν and c such that*

$$\Psi(x, y) - \Psi(x - z, y) > cz$$

holds uniformly for all y, z such that

(i) *$y = x^\alpha$ with $1/2 - \nu \leq \alpha \leq 1 - \nu$;*

(ii) *$yz \geq x^{1-\nu}$ for all sufficiently large $x \geq 1$.*

A more recent result, which is basically a special case of the last theorem, has a fixed parameter $z = x^{1/2}$ for the size of the short interval.

Theorem 8.4. ([58]) *Let $\alpha > 1/4\sqrt{e}$. If $x \geq 1$ is sufficiently large then,*

$$\Psi(x + x^{1/2}, x^\alpha) - \Psi(x, x^\alpha) \gg x^{1/2}.$$

Lemma 8.1. *Let $\alpha > 1/4\sqrt{e}$. Then, there exists a constant $c_\alpha > 0$ such that*

$$\Psi(x + x^{1/2}, x^\alpha) - \Psi(x, x^\alpha) = c_\alpha x^{1/2} + o(x^{1/2})$$

for all sufficiently large $x \geq 1$.

Proof. Combining theorems 8.2 and 8.4 yield

$$x^{1/2} \ll \Psi(x + x^{1/2}, x^\alpha) - \Psi(x, x^\alpha) \leq \frac{1}{\alpha}x^{1/2} + c_0\pi_(x^\alpha). \tag{8.7}$$

This immediately implies the claim.

■

The counting function

$$\Theta(x,y,z) = \#\{n \le x : p \,|\, n \Rightarrow y \le p \le z\} \tag{8.8}$$

is studied in [38], and [87, p. 213]. In terms of the better known results it has the form

$$\begin{aligned} \Theta(x,x^\alpha,x^\beta) &= \Psi(x,x^\beta)\prod_{p\le x^\alpha}\left(1-\frac{1}{p}\right) \\ &\gg \frac{x^\beta}{\log x^\alpha}, \end{aligned} \tag{8.9}$$

see [40, Corollary 1]. For certain parameters such as $\alpha > 1/4\sqrt{e}$ and $\beta > \alpha$, this lower bound can be improved.

Lemma 8.2. *Let $x \ge 1$ be a large number, and let $x^\alpha < x^\beta$ with $1/4\sqrt{e} \le \alpha \le \beta < 1$. Then, interval $[x + x^{1/2}, x]$ contains*

$$\begin{aligned} \Theta(x,x^\alpha,x^\beta) &= \#\{x \le n \le x + x^{1/2} : p \,|\, n \Rightarrow x^\alpha \le p \le x^\beta\} \\ &= c(\alpha,\beta)x^{1/2} + o(x^{1/2}) \end{aligned}$$

nonsmooth integers $x \to \infty$, with $c(\alpha,\beta) > 0$ constant.

Proof. Fix the parameters $\alpha > 1/4\sqrt{e}$ and $\beta = 1-\varepsilon$, with $\varepsilon > 0$ an arbitrary small number. By Lemma 8.1 the short interval $[x, x + x^{1/2}]$ contains

$$\Psi(x + x^{1/2}, x^{1-\varepsilon}) - \Psi(x, x^{1-\varepsilon}) = c_\beta x^{1/2} + o(x^{1/2}), \tag{8.10}$$

$x^{1-\varepsilon}$-smooth integers, and

$$\Psi(x + x^{1/2}, x^{\alpha}) - \Psi(x, x^{\alpha}) = c_\alpha x^{1/2} + o(x^{1/2}), \tag{8.11}$$

x^{α}-smooth integers, respectively. Taking the difference yields

$$\#\{x \le n \le x + x^{1/2} : p \,|\, n \Rightarrow x^\alpha \le p \le x^\beta\} = c(\alpha,\beta)x^{1/2} + o(x^{1/2}), \tag{8.12}$$

where $c(\alpha,\beta) = c_\beta - c_\alpha > 0$ is a constant. ■

8.3 Correlation Functions For Twin Smooth Integers

The longest run of consecutive B-smooth integers

$$n, \quad n+1, \quad n+2, \quad \ldots, \quad n+k \tag{8.13}$$

such that $n + k \le x$, is believed to be $k + 1 = [\log x]$

Theorem 8.5. ([9, Theorem 1]) *Suppose that $u > 1$ is a fixed real number. Let*

$$k = [\log\log\log\log n/\log 3u].$$

Then, for infinitely many integers n, none of the prime factors of any of the k consecutive integers $n+1, n+2, \ldots, n+k$, exceed $n^{1/u}$.

The conjectured quantitative form

$$\sum_{n\leq x} \alpha_B(n)\alpha_B(n+1)\cdots\alpha_B(n+k) = a_k(u)\rho(u)^k x + O\left(\frac{t(u)x}{\log x}\right), \tag{8.14}$$

where $\alpha_B(n)$ is the characteristic function of B-smooth numbers, $a_k(u) > 0$ is a dependence correction factor, and $t(u) > 0$ is some function, is given in [45, Theorem 1.1].

Chapter 9

Prime Numbers Theorems

9.1 Primes And Almost Primes Indicator Functions

For $k \geq 1$, the Selberg function $\Lambda_k : \mathbb{N} \longrightarrow \mathbb{R}$ is defined by

$$\Lambda_k(n) = \begin{cases} (-1)^k \sum_{d|n} \mu(d) \log^k(n/d) & \text{if } \omega(n) \leq k, \\ 0 & \text{if } \omega(n) > k. \end{cases} \tag{9.1}$$

The subsets of integers $\mathbb{N}_k = \{n \in \mathbb{N} : \omega(n) \leq k\}$ is the support ofthis function. The selberg function generalizes the earlier special case for $k = 1$, known as the von-Mangoldt function. The vonMangoldt function, a weighted prime power indicator function, is defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^m, \\ 0 & \text{if } n \neq p^m. \end{cases} \tag{9.2}$$

The above notation $p^m \geq 2$, with $m \in \mathbb{N}$, denotes a prime power.

Lemma 9.1. *Given a fixed $k \geq 1$,and any integer $n \in \mathbb{N}$, the function $\Lambda_k(n)$ has the inverse Mobius pair*

$$\Lambda_k(n) = (-1)^k \sum_{d|n} \mu(d) \log^k(n/d) \qquad \textit{and} \qquad \log^k(n) = \sum_{d|n} \Lambda_k(d).$$

Proof. Use the inversion formula, [1, Theorem 2.9]. ■

Lemma 9.2. *Given a fixed $k \geq 1$,and any integer $n \in \mathbb{N}$, the function $\Lambda_k(n)$ satisfies the following properties.*

(i) $\Lambda_k(n) \geq 0$, *nonenegativity.*

(ii) $\Lambda_k(n) = 0$, *if and only if $\omega(n) > k$.*

(iii) $\Lambda_k(n) \leq \log^k x$. *polynomial growth.*

9.2 Partial Sums And Generating Functions

For a fixed $k \geq 1$, the partial sum of Selberg functions is defined by

$$\psi_k(x) = \sum_{n \leq x} \Lambda_k(n) \tag{9.3}$$

and the corresponding generting function is defined by

$$\sum_{n \geq 1} \frac{\Lambda_k(n)}{n^s} = (-1)^k \zeta^{(k)}(s) \cdot \frac{1}{\zeta(s)}. \tag{9.4}$$

Theorem 9.1. *If $k \geq 1$ is a fixed integer, and $x \geq 1$ is a large number, then*

$$\sum_{n \leq x} \Lambda_k(n) = x S_k(\log x) + O(x), \tag{9.5}$$

where $S_k(z) = kz^{k-1} + \cdots + a_1 z + a_0 \in \mathbb{R}[z]$ is a real polynomial.

There is a vast literature devoted to the case $k = 1$, known as the prime number theorem, and some literature devoted to the case $k = 2$, known as the elementary proof of the prime number theorem.

9.3 Counting Functions And Prime Numbers Theorems

The vonMangoldt function, a weighted prime power indicator function, is defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^m, \\ 0 & \text{if } n \neq p^m. \end{cases} \tag{9.6}$$

The above notation $p^m \geq 2$, with $m \in \mathbb{N}$, denotes a prime power.

Lemma 9.3. *For any integer $n \in \mathbb{N}$, the function $\Lambda(n)$ has the inverse Mobius pair*

$$\Lambda(n) = -\sum_{d|n} \mu(d) \log d \qquad \text{and} \qquad \log(n) = \sum_{d|n} \Lambda(d).$$

Proof. Use the inversion formula, [1, Theorem 2.9]. ■

The weighted primes counting functions, psi $\psi(x)$ and theta $\theta(x)$, are defined by

$$\theta(x) = \sum_{p \leq x} \log p \tag{9.7}$$

and

$$\psi(x) = \sum_{n \leq x} \Lambda(n) \tag{9.8}$$

respectively. The standard prime counting function is denoted by

$$\pi(x) = \#\{p \le x\} = \sum_{p \le x} 1. \tag{9.9}$$

This function is usually expressed in term of the logarithm integral $\mathrm{li}(x) = \int_2^x (\log t)^{-1} dt$.

Theorem 9.2. *Uniformly for $x \ge 2$ the psi and theta functions have the followings asymptotic formulae.*

(i) $\theta(x) = x + O\left(xe^{-c_0\sqrt{\log x}}\right)$, *unconditionally.*

(ii) $\theta(x) = x + \Omega_{\pm}\left(x^{1/2}\log\log\log x\right)$, *unconditional oscillation.*

(iii) $\theta(x) = x + O\left(x^{1/2}\log^2 x\right)$. *conditional on the RH.*

Proof. (ii) The oscillations form of the theta function is proved in [87, p. 479], ■

The same asymptotics hold for the function $\psi(x)$. Explicit estimates for both of these functions are given in [21], [105], [23, Theorem 5.2], and related literature.

Conjecture 9.1. *Assuming the RH and the LI conjecture, the suprema are*

$$\liminf_{x\to\infty} \frac{\psi(x)-x}{\sqrt{x}(\log\log x)^2} = \frac{-1}{\pi} \qquad \textit{and} \qquad \limsup_{x\to\infty} \frac{\psi(x)-x}{\sqrt{x}(\log\log x)^2} = \frac{1}{\pi}.$$

More details on the Linear Independence conjecture appear in [63], [29, Theorem 6.4], and recent literature. The LI conjecture asserts that the imaginary parts of the nontrivial zeros $\rho_n = 1/2 + i\gamma_n$ of the zeta function $\zeta(s)$ are linearly independent over the set $\{-1, 0, 1\}$. In short, the equations

$$\sum_{1\le n\le M} r_n\gamma_n = 0, \tag{9.10}$$

where $r_n \in \{-1, 0, 1\}$, have no nontrivial solutions.

Theorem 9.3. *Let $x \ge 1$ be a large number. Then*

(i) $\pi(x) = \mathrm{li}(x) + O\left(xe^{-c_0\sqrt{\log x}}\right)$, *unconditionally.*

(ii) $\pi(x) = \mathrm{li}(x) + \Omega_{\pm}\left(\dfrac{x^{1/2}\log\log\log x}{\log x}\right)$, *unconditional oscillation.*

(iii) $\pi(x) = \mathrm{li}(x) + O\left(x^{1/2}\log x\right)$, *conditional on the RH.*

Proof. (i) The unconditional part of the prime counting formula arises from the delaVallee Poussin form $\pi(x) = \mathrm{li}(x) + O\left(xe^{-c_0\sqrt{\log x}}\right)$ of the prime number theorem, see [87, p. 179]. Recent information on the constant $c_0 > 0$ and the sharper estimate

$$\pi(x) = \mathrm{li}(x) + O\left(xe^{-c_0\log x^{3/5}(\log\log x)^{-2/5}}\right) \tag{9.11}$$

appears in [35]. (ii) The unconditional oscillations part arises from the Littlewood form

$$\pi(x) = \mathrm{li}(x) + \Omega_{\pm}\left(x^{1/2}\log\log\log x/\log x\right) \tag{9.12}$$

of the prime number theorem, consult [64, p. 51], [87, p. 479], et cetera.

(iii) The conditional part arises from the Riemann form $\pi(x) = \mathrm{li}(x) + O\left(x^{1/2}\log^2 x\right)$ of the prime number theorem. ■

New explict estimates for the number of primes in arithmetic progressions are computed in [3].

Definition 9.1. Let $f : \mathbb{N} \longrightarrow \mathbb{C}$ be an arithmetic function, and let $x \geq 1$ be a real number. A level of distribution is a value $Q < x$ such that

$$\sum_{q<Q} \max_{\gcd(a,q)} \left| \sum_{\substack{n\leq x \\ n\equiv a \bmod q}} f(n) - \frac{1}{\varphi(q)} \sum_{\substack{n\leq x \\ \gcd(n,q)=1}} f(n) \right| \ll \left(\frac{x}{\log^C x}\right), \tag{9.13}$$

where $C > 0$ is a constant.

This compares the average orders over arithmetic progressions to the weigted average orders of the function. Recent develoments in this topic are discussed in [48]. The prime counting function $\pi(x, a, q)$ has the best known results for the level of distributions.

Result	Level Of Distribution
Bombieri-Vinogradov Theorem	$Q = x^{1/2}/\log^B x$
Friedlander- Granville Theorem, [37]	$Q < x/\log^B x$
Elliot-Halberstam Conjecture	$Q = x^{1-\varepsilon}$

Theorem 9.4. (Bombieri-Vinogradov theorem) *Let $C > 0$ be a constant. Then, there exists a constant $D > 1$ for which*

$$\sum_{q<x^{1/2}/\log^D x} \max_{\gcd(a,q)} \left|\pi(x,a,q) - \frac{1}{\varphi(q)}\mathrm{li}(x)\right| \ll \left(\frac{x}{\log^C x}\right),$$

as $x \to \infty$.

9.4 Sums Over The Primes

The most basic finite sum over the prime numbers is the prime harmonic sum $\sum_{p\leq x} 1/p$. The refined estimate of this finite sum, stated below, is a synthesis of various results due to various authors.

Lemma 9.4. *Let $x \geq 2$ be a large number, then*

(i) $$\sum_{p\leq x} \frac{1}{p} = \log\log x + B_1 + O\left(e^{-c_0\sqrt{\log x}}\right), \qquad \textit{unconditionally.}$$

(ii) $\displaystyle\sum_{p\leq x}\frac{1}{p}=\log\log x+B_1+\Omega_{\pm}\left(\frac{\log\log\log x}{x^{1/2}\log x}\right),$ *unconditional oscillation.*

(iii) $\displaystyle\sum_{p\leq x}\frac{1}{p}=\log\log x+B_1+O\left(\frac{\log x}{x^{1/2}}\right),$ *conditional on the RH.*

where $B_1=0.2614972128\ldots$, *is Mertens constant, and* $c_0>0$ *is an absolute constant.*

Proof. Replace the logarithm integral $\mathrm{li}(x)=\int_2^x(\log t)^{-1}dt$, and the appropriate prime counting measure $\pi(x)$ in Theorem 9.3 into the Stieltjes integral representation

$$\sum_{p\leq x}\frac{1}{p}=\int_2^x\frac{1}{t}d\pi(t) \tag{9.14}$$

and evaluate it.

(i) The unconditional part of the prime counting formula arises from the delaVallee Poussin form $\pi(x)=\mathrm{li}(x)+O\left(xe^{-c_0\sqrt{\log x}}\right)$ of the prime number theorem, see [87, p. 179].

(ii) The unconditional oscillations part arises from the Littlewood form $\pi(x)=\mathrm{li}(x)+\Omega_{\pm}\left(x^{1/2}\log\log\log x/\log x\right)$ of the prime number theorem, consult [64, p. 51], [87, p. 479], et cetera.

(iii) The conditional part arises from the Riemann form $\pi(x)=\mathrm{li}(x)+O\left(x^{1/2}\log^2 x\right)$ of the prime number theorem. ■

The asymptotic order $\sum_{p\leq x}1/p\sim\log\log x$ is due to Euler, confer [31, Chapter 15]. The earliest version including error term $\sum_{p\leq x}1/p=\log\log x+B_1+O(1/\log x)$ is due to Mertens, see [117]. The qualitative form of the oscillations of the differences

$$\sum_{p^k\leq x}\frac{1}{p^k}-(\log\log x+\gamma)\quad\text{and}\quad\sum_{p^k\leq x}\frac{\log p}{p^k}-(\log x+\gamma) \tag{9.15}$$

seems to be due to Phragmen, confer [89, p. 182].

The Euler constant and Mertens constant occur very frequently in analysis. The former is defined by, (twenty four digits accuracies),

$$\gamma=\lim_{x\to\infty}\left(\sum_{n\leq x}\frac{1}{n}-\log x\right)=0.577215664901532860606512\ldots, \tag{9.16}$$

and the later is defined by

$$B_1=\lim_{x\to\infty}\left(\sum_{p\leq x}\frac{1}{p-1}-\log\log x\right)=0.261497212847642783755426\ldots. \tag{9.17}$$

Other definitions of these constants are available in the literature, confer [**?**].

Lemma 9.5. *The constants γ and B_1 satisfy the linear relation*

$$B_1 = \gamma - \sum_{p\geq 2}\sum_{n\geq 2}\frac{1}{np^n}. \tag{9.18}$$

Proof. This relation stems from the power series expansion

$$B_1 - \gamma = \sum_{p\geq 2}\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right) \tag{9.19}$$

via the power series for $\log(1+z)$ with $|z|<1$. This leads to this identity, see [61, p. 466], [87, p. 182]. ■

Lemma 9.6. *Let $x \geq 2$ be a large number, then*

$$\sum_{p\leq x}\sum_{n\geq 2}\frac{1}{np^n} = \gamma - B_1 - \frac{1}{x\log x} + O\left(\frac{1}{x\log^2 x}\right).$$

Proof. Rearrange the power series expansion as

$$\sum_{p\leq x}\sum_{n\geq 2}\frac{1}{np^n} = \gamma - B_1 - \sum_{p>x}\sum_{n\geq 2}\frac{1}{np^n} = \gamma - B_1 - \frac{1}{x\log x} + O\left(\frac{1}{x\log^2 x}\right). \tag{9.20}$$

The estimate for the last two terms on the right follows from Lemma 9.7 computed below. ■

Lemma 9.7. *Let $x \geq 1$ be a large number, then*

$$\sum_{p>x}\sum_{n\geq 2}\frac{1}{np^n} = \frac{1}{x\log x} + O\left(\frac{1}{x\log^2 x}\right).$$

Proof. Split the infinite sum into two subsums:

$$\begin{aligned}\sum_{p>x}\sum_{n\geq 2}\frac{1}{np^n} &= \sum_{p>x}\frac{1}{2p^2} + \sum_{p>x}\sum_{n\geq 3}\frac{1}{np^n} \\ &= \sum_{p\geq x}\frac{1}{2p^2} + O\left(\frac{1}{x^2\log x}\right).\end{aligned} \tag{9.21}$$

Employ the prime counting measure $\pi(t) = \#\{p \leq t\}$ to evaluate the first subsum using the integral

$$\begin{aligned}\sum_{p\geq x}\frac{1}{p^2} &= \int_x^\infty \frac{1}{t^2}d\pi(t) \\ &= -\frac{\pi(x)}{x^2} + 2\int_x^\infty \frac{\pi(t)}{t^3}dt \\ &= \frac{1}{x\log x} + O\left(\frac{1}{x\log^2 x}\right).\end{aligned} \tag{9.22}$$

■

A generalized Mertens theorem to products of rational primes was recently proved by a few authors, see [96] and [112].

Theorem 9.5. *Let $x \geq 2$ be a large number, and let $k \geq 1$. Then,*

$$\sum_{p_1 p_2 \cdots p_k \leq x} \frac{1}{p_1 p_2 \cdots p_k} = P_k(\log\log x) + O\left(\frac{(\log\log x)^{k-1}}{\log x}\right),$$

where $P_k(z) \in \mathbb{R}[z]$ is a polynomial of degree $\deg P_k = k$.

The first two polynomials are these:

1. $P_1(z) = z + B$,
2. $P_2(z) = (z + B)^2 - \pi^2/6$,

where $B = B_1 = 0.26\ldots$ is Mertens constant. This results is very useful in the calculations of the moments of the prime counting function $\omega(n)$, the second moment is required in the proof of Theorem 2.1.

9.5 Products Over The Primes

The asymptotics for a variety of interesting products are simple applications of the results for prime harmonic sums in the previous section.

Lemma 9.8. *Let $x \geq 2$ be a large number, then*

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

(ii) $$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = e^{\gamma} \log x + \Omega\left(\frac{\log\log\log x}{x^{1/2}}\right), \qquad \textit{unconditional oscillation.}$$

(iii) $$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = e^{\gamma} \log x + O\left(\frac{\log x}{x^{1/2}}\right), \qquad \textit{conditional on the RH.}$$

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

The results for products over arithmetic progression are proved in [74], et alii.

Lemma 9.9. *Let $x \geq 2$ be a large number, then*

(i) $$\prod_{p \leq x} \left(1 + \frac{1}{p}\right) = \frac{6e^{\gamma}}{\pi^2} \log x + O\left(e^{-c_0\sqrt{\log x}}\right), \qquad \textit{unconditionally.}$$

(ii) $$\prod_{p \leq x} \left(1 + \frac{1}{p}\right) = \frac{6e^{\gamma}}{\pi^2} \log x + \Omega\left(\frac{\log\log\log x}{x^{1/2}\log x}\right), \qquad \textit{unconditional oscillation.}$$

(iii) $\displaystyle\prod_{p\leq x}\left(1+\frac{1}{p}\right)=\frac{6e^{\gamma}}{\pi^2}\log x+O\left(\frac{\log x}{x^{1/2}}\right),$ *conditional on the RH.*

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

Proof. (i) For a large real number $x\in\mathbb{R}$, rewrite the product as

$$\prod_{p\leq x}\left(1+\frac{1}{p}\right)=\prod_{p\leq x}\left(1+\frac{1}{p}\right)\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p}\right)^{-1}=\prod_{p\leq x}\left(1-\frac{1}{p^2}\right)\prod_{p\leq x}\left(1-\frac{1}{p}\right)^{-1}. \tag{9.23}$$

Replacing the completed product

$$\prod_{p\leq x}\left(1-\frac{1}{p^2}\right)=\prod_{p\geq 2}\left(1-\frac{1}{p^2}\right)+O\left(\frac{1}{x^c}\right)=\frac{6}{\pi^2}+O\left(\frac{1}{x^c}\right), \tag{9.24}$$

where $c\geq 1$ is a constant, in the first product on the right side of (**??**), and applying Lemma **??**? yield

$$\begin{aligned}\prod_{p\leq x}\left(1-\frac{1}{p^2}\right)\prod_{p\leq x}\left(1-\frac{1}{p}\right)^{-1} &= \left(\frac{6}{\pi^2}+O\left(\frac{1}{x^c}\right)\right)\prod_{p\leq x}\left(1-\frac{1}{p}\right)^{-1} \\ &= \left(\frac{6}{\pi^2}+O\left(\frac{1}{x^c}\right)\right)\left(e^{\gamma}\log x+O\left(e^{-c_0\sqrt{\log x}}\right)\right) \\ &= \frac{6e^{\gamma}}{\pi^2}\log x+O\left(e^{-c_0\sqrt{\log x}}\right).\end{aligned} \tag{9.25}$$

The verification of statements (ii) and (iii) are similar, mutatis mutandus.

■

The nonquantitative unconditional oscillations of the error of the product of primes is implied by the work of Phragmen, refer to equation (9.15), and [89, p. 182]. Since then, various authors have developed quantitative versions, see [103], [24], [71], [70], et alii. The specific quantitative form

$$\prod_{p\leq x}\left(1-\frac{1}{p}\right)^{-1}=e^{\gamma}\log x+\Omega_{\pm}\left(\frac{f(x)}{x^{1/2}}\right), \tag{9.26}$$

where $f(x)$ is a slowly increasing function, was proved in [24].

Theorem 9.6. (Martens, 1874) *The following asymptotic formulas hold:*

(i) $\displaystyle\lim_{x\to\infty}\frac{1}{\log x}\prod_{p\leq x}\left(1-\frac{1}{p}\right)^{-1}=e^{\gamma},$ *the product over the integers.*

(ii) $\displaystyle\lim_{x\to\infty}\frac{1}{\log x}\prod_{p\leq x}\left(1+\frac{1}{p}\right)^{-1}=\frac{6e^{\gamma}}{\pi^2}$ *the product over the squarefree integers.*

9.6 Correlation Functions For Twin Primes And Prime Pairs

The qualitative version of the prime pairs is attributed to dePolinac, see the survey in [94]. The heuristic for the quantitative prime pairs conjecture, based on the circle method, appears in [57, p. 42]. The precise statement is the following.

Conjecture 9.2. (Prime Pairs Conjecture) *There are infinitely many prime pairs $p, p+2k$ as the prime $p \to \infty$. Moreover, the counting function has the asymptotic formula*

$$\pi_{2k}(x) = 2\prod_{p|2k}\left(\frac{p-1}{p-2}\right)\prod_{p\nmid 2k}\left(1-\frac{1}{(p-1)^2}\right)\frac{x}{\log^2 x}+O\left(\frac{x}{\log^3 x}\right),$$

where $k \geq 1$ is a fixed integer, and $x \geq 1$ is a large number.

The constant arises from the singular series

$$\mathfrak{G}(2k) = \prod_{p\geq 2}\left(1-\frac{v_p(f)}{p}\right)\left(1-\frac{1}{p}\right)^{-2} = 2\prod_{p|2k}\left(\frac{p-1}{p-2}\right)\prod_{p\nmid 2k}\left(1-\frac{1}{(p-1)^2}\right), \quad (9.27)$$

where $v_p(f)$ is the number of root in the congruence $x(x+2k) \equiv 0 \bmod p$ for $p \geq 2$.

The heuristic based on probability, yields the Gaussian type analytic formula

$$\pi_{2k}(x) = C_{2k}\int_2^x \frac{1}{\log^2 t}dt + O\left(\frac{x}{\log^3 x}\right), \quad (9.28)$$

where C_{2k} is the same constant as above. The deterministic approach is based on the weighted prime pairs counting function

$$\sum_{n\leq x}\Lambda(n)\Lambda(n+m), \quad (9.29)$$

which is basically an extended version of the Chebyshev method for counting primes.

For an odd integer $m \geq 1$, the average order of the finite sum $\sum_{n\leq x}\Lambda(n)\Lambda(n+m)$ is very small, and the number of prime pairs $p, p+m$ is finite. Consequently, it is sufficient to consider even integer $m = 2k$. The best known case is for $k = 1$.

Conjecture 9.3. (Twin Prime Conjecture) *There are infinitely many twin prime $p, p+2$ as the prime $p \to \infty$. Moreover, the counting function has the asymptotic formula*

$$\pi_2(x) = 2\prod_{p\geq 3}\left(1-\frac{1}{(p-1)^2}\right)\frac{x}{\log^2 x}+O\left(\frac{x}{\log^3 x}\right),$$

asx $\to$ infty. The twin prime constant is

$$\mathfrak{G}(2) = 2\prod_{p\geq 3}\left(1-\frac{1}{(p-1)^2}\right) = 2(0.660161815846869573927812110014\ldots). \quad (9.30)$$

9.7 Arithmetic Functions Summation Formulas

Lemma 9.10. [118, Lemma 3.1] *Suppose that $f : \mathbb{N} \longrightarrow \mathbb{C}$ is a multiplicative function and nonnegative, and there is a number $\tau > 0$ such that*

$$\sum_{p \leq x} f(p) = (\tau + o(1)) = \frac{x}{\log x}$$

as $x \to \infty$. Then,

$$\sum_{n \leq x} \mu^2(n) f(n) = \left(\frac{e^{-\gamma \tau}}{\Gamma(\tau)} + o(1) \right) \frac{x}{\log x} \prod_{p \leq x} \left(1 + \frac{f(p)}{p} \right), \tag{9.31}$$

where $\gamma > 0$ is a Euler constant.

9.8 Problems

9.8.1 Constants Related Problems

Exercise 9.1. Show that Mertens constant is given by the series

$$B_1 = \gamma + \sum_{n\geq 2} \frac{\mu(n)}{n} \log \zeta(n).$$

Exercise 9.2. Show that if $a_1 > 0$ and $a_n \to 0$ as $n \to \infty$, then

$$\sum_{n\geq 2} \frac{\mu(n)}{n} \log\left(1 + a_n\right) > 0.$$

Exercise 9.3. Use the rapidly convergent property of the series linking the Euler and Mertens constants:

$$B_1 = \gamma - \sum_{p\geq 2} \sum_{n\geq 2} \frac{1}{np^n}$$

to prove or disprove that B_1 and γ are linearly independent over the rational numbers $\mathbb{Q}$.

Exercise 9.4. Let $\alpha \geq 0$ be a real number. Evaluate the finite sum

$$\sum_{n\geq 2} \frac{1}{n(\log n)^{1+\alpha}}.$$

Exercise 9.5. Let $x \geq 1$ be a large number. Show that

$$\prod_{p\leq x} \left(1 + \frac{p \pm 1}{p^2}\right) = \prod_{p\leq x} \left(1 + \frac{1}{p}\right) \left(\prod_{p\geq 2} \left(1 \pm \frac{1}{p(p+1)}\right) + O\left(\frac{1}{x \log x}\right)\right).$$

9.8.2 Primes Indicator Functions Problems

Let $1 \leq a < q$ be relatively prime integers. The indicator function of the sequence of primes $\{p \equiv a \bmod q\}$ is defined by

$$\beta(n, q, a) = \begin{cases} 1 & \text{if } n \equiv a \bmod q \text{ is prime,} \\ 0 & \text{if } n \equiv a \bmod q \text{ is not prime.} \end{cases}$$

Exercise 9.6. Let $\chi : \mathbb{N} \longrightarrow \{-1, 0, 1\}$ be the quadratic character modulo 4. Verify that the indicator function of the sequence of primes $\{p \equiv 1 \bmod 4\}$ is given by

$$\beta(n, 4, 1) = \frac{1}{2}\left(1 + \chi\left(n\right)\right) = \begin{cases} 1 & \text{if } n \equiv 1 \bmod 4 \text{ is prime,} \\ 0 & \text{if } n \equiv 1 \bmod 4 \text{ is not prime,} \end{cases}$$

Exercise 9.7. Let $\chi : \mathbb{N} \longrightarrow \{-1, 0, 1\}$ be the quadratic character modulo 4. Verify that the indicator function of the sequence of primes $\{p \equiv 3 \bmod 4\}$ is given by

$$\beta(n, 4, 3) = \frac{1}{2}\left(1 - \chi\left(n\right)\right) = \begin{cases} 1 & \text{if } n \equiv 3 \bmod 4 \text{ is prime,} \\ 0 & \text{if } n \equiv 3 \bmod 4 \text{ is not prime,} \end{cases}$$

Exercise 9.8. Verify that the indicator function of the sequence of primes $\{p \equiv 1 \bmod 4\}$ is given by

$$\beta(n,4,1) = \frac{1}{2}\left(1+\sin\left(\frac{\pi n}{2}\right)\right) = \begin{cases} 1 & \text{if } n \equiv 1 \bmod 4 \text{ is prime,} \\ 0 & \text{if } n \equiv 1 \bmod 4 \text{ is not prime,} \end{cases}$$

Exercise 9.9. Verify that the indicator function of the sequence of primes $\{p \equiv 3 \bmod 4\}$ is given by

$$\beta(n,4,3) = \frac{1}{2}\left(1-\sin\left(\frac{\pi n}{2}\right)\right) = \begin{cases} 1 & \text{if } n \equiv 3 \bmod 4 \text{ is prime,} \\ 0 & \text{if } n \equiv 3 \bmod 4 \text{ is not prime,} \end{cases}$$

Exercise 9.10. Let $\omega : \mathbb{N} \longrightarrow \mathbb{N}$ be the number of prime divisors function, and $[x] = x - \{x\}$ be the largest integer function. If $\alpha > 0$, and $n \geq 1$ is large, then the expression

$$\beta(n) = 1 + \left[\frac{1-\omega(n)}{n^{\alpha}}\right] = \begin{cases} 1 & \text{if } n \text{ is prime,} \\ 0 & \text{if } n \text{ is not prime,} \end{cases}$$

defines a prime indicator function.

Exercise 9.11. Let $d : \mathbb{N} \longrightarrow \mathbb{N}$ be the number of divisors function, and $[x] = x - \{x\}$ be the largest integer function. If $\alpha > 1/4$, and $n \geq 1$ is large, then the expression

$$\beta(n) = 1 + \left[\frac{2-d(n)}{n^{\alpha}}\right] = \begin{cases} 1 & \text{if } n \text{ is prime,} \\ 0 & \text{if } n \text{ is not prime,} \end{cases}$$

defines a prime indicator function.

Exercise 9.12. Let $\omega : \mathbb{N} \longrightarrow \mathbb{N}$ be the number of prime divisors function, and $[x] = x - \{x\}$ be the largest integer function. If $\alpha > 0$, and $n \geq 1$ is large, then the expression

$$\beta(n) = 1 + \left[\frac{\Lambda(n)-\log(n)}{n^{\alpha}}\right] = \begin{cases} 1 & \text{if } n \text{ is prime,} \\ 0 & \text{if } n \text{ is not prime,} \end{cases}$$

defines a prime indicator function.

Chapter 10

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 here.

10.1 Gauss Probabilistic Method

The basic Gauss probabilistic prime counting method for the number of primes generated by an arithmetic function $f : \mathbb{N} \longrightarrow \mathbb{N}$ has the shape

$$\pi_f(x) = \#\{p = f(n) \leq x\} = \sum_{f(n)\leq x} \frac{1}{\log f(n)} + O\left(\frac{x^{1/d}}{(\log x)^2}\right), \tag{10.1}$$

where f is a polynomial of degree $d = \deg f$. The conversion to an Stiejles integral realizes the equivalent asymptotic formulas

$$\pi_f(x) = \int_2^x \frac{1}{(\log f(t)} dt + O\left(\frac{x^{1/d}}{\log^{k+1} x}\right), \tag{10.2}$$

and

$$\sum_{f_i(n)\leq x} \Lambda(f_1(n)) \cdots \Lambda(f_k(n)) = s_f x^{1/d} + O\left(\frac{x^{1/d}}{\log^C x}\right),$$

with $d = d_1 + d_2 + \cdots + d_k$, and $C > 0$ is arbitrary. The Bateman-Horn conjecture is a refined version geared for a product $f(x) = f_1(x) \cdots f_k(x) \in \mathbb{Z}[x]$ of $k \geq 1$ irreducible polynomials $f_i(x)$ of degree $d_i = \deg f_i$.

10.2 Polynomials Primes Values Conjecture

The quantitative form of the qualitative Hypothesis H, [101, pp. 386–394], was formulated about fifty years ago in [2]. It states the followings.

Conjecture 10.1. (Bateman-Horn) *Let $f_1(x), f_2(x), \ldots, f_k(x) \in \mathbb{Z}[x]$ be relatively prime polynomials of degree $\deg(f_i) = d_i \geq 1$. Suppose that each polynomial $f_i(x)$ has the fixed divisor $\operatorname{div}(f_i) = 1$. Then, the number of simultaneously primes k-tuples*

$$f_1(n), f_2(n), \ldots, f_k(n),$$

as $n \leq x$ tends to infinity has the equivalent asymptotic formulas

$$\pi_f(x) = s_f \int_2^x \frac{1}{(\log t)^k} dt + O\left(\frac{x^{1/d}}{\log^{k+1} x}\right), \tag{10.3}$$

and

$$\sum_{f_i(n) \leq x} \Lambda(f_1(n)) \cdots \Lambda(f_k(n)) = s_f x^{1/d} + O\left(\frac{x^{1/d}}{\log^C x}\right),$$

with $d = d_1 + d_2 + \cdots + d_k$, and $C > 0$ is arbitrary. The density constant is defined by the product

$$s_f = \frac{1}{d_1 d_2 \cdots d_k} \prod_{p \geq 2} \left(1 - \frac{v_p(f)}{p}\right) \left(1 - \frac{1}{p}\right)^{-k}, \tag{10.4}$$

where the symbol $v_p(f) \geq 0$ denotes the number of solutions of the congruence

$$f_1(x) f_2(x) \cdots f_k(x) \equiv 0 \bmod p. \tag{10.5}$$

This generalization of prime values of polynomials appears in [2]. The constant, known as singular series

$$\mathfrak{G}(f) = \prod_{p \geq 2} \left(1 - \frac{v_p(f)}{p}\right) \left(1 - \frac{1}{p}\right)^{-k}, \tag{10.6}$$

can be derived by either the circle method, as done in [86, Chapter 10], [62, p. 167], [118] or by probabilistic means as explained in [94, p. 33], [101, p. 410], et alii. The convergence of the product is discussed in [2], [99], and other by authors.

The term

$$P_f(n) = \prod_{p \leq n} \left(1 - \frac{\nu(p)}{p}\right) \left(1 - \frac{1}{p}\right)^{-k}, \tag{10.7}$$

where $\nu(p) = \#\{n : f(n) \equiv 0 \bmod p\}$, is a correction factor accounting for some of the small primes dependence.

The Bateman-Horn conjecture was formulated in the 1960's, about half a century ago. A more recent result accounts for the irregularities and oscillations that can occur in the asymptotic formula as the polynomial is varied.

Theorem 10.1. ([36]) *Let $d \geq 1$ be a fixed integer, and let $B \geq 2$ be a real number. There exist infinitely many irreducible polynomials $f(x)$ of degree $\deg(f) = d$ with nonnegative integer coefficients, such that for some number $\delta_B > 0$ depending on B, and $x \geq \log^B |f(x)|$, the absolute difference*

$$\left|\pi_f(x) - C_f \frac{x}{\log |f(x)|}\right| > \delta_B C_f \frac{x}{\log |f(x)|}. \tag{10.8}$$

This result was proved for polynomials of large degrees, but it is claimed to hold for certain structured polynomials of small degrees $d \geq 1$.

10.3 Primorial Primes

The subset of primorial primes

$$\mathcal{A} = \{p = 2 \cdot 3 \cdot 5 \cdot 7 \cdots q + 1 : \text{ prime } q \geq 2\} \tag{10.9}$$

is studied in [11], and listed in OEIS A014545. A primorial prime has a highly composite totient $p - 1 = \varphi(p)$, the maximal numbers of prime divisors

$$\omega(p-1) \ll \log p / \log\log p, \tag{10.10}$$

see Lemma 2.1, and the minimal value

$$\frac{\varphi(p-1)}{p-1} = \prod_{q|p-1} \left(1 - \frac{1}{q}\right) \approx \frac{1}{\log\log p}, \tag{10.11}$$

where $r \leq q$ ranges over the primes, see Theorem 4.6. 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.

The standard heuristic for the number of primorial primes is based on the gaussian probabilistic method.

Conjecture 10.2. *As $x \to infty$, the number of prime pairs $p = n! + 1$ leqx has the asymptotic formula*

$$\pi_f(x) = \#\{p = n! + 1 \leq x : p \textit{ is prime } \} = e^\gamma \log x + o(\log x).$$

Heuristic 1: As $n \to \infty$, the asymptotic for the factorial function is $n! \approx n \log n$. Thus,

$$\begin{aligned} \pi_f(x) &= \#\{p = n! + 1 \leq x : p \text{ is prime } \} \\ &= \sum_{n \leq x} \prod_{p \leq n} \left(1 - \frac{1}{p}\right)^{-1} \frac{1}{\log(n! + 1)} \\ &\approx \sum_{n \leq x} e^\gamma \log n \cdot \frac{1}{n \log n} \\ &= e^\gamma \log x + o(\log x). \end{aligned} \tag{10.12}$$

It is not a standard practice, but a heuristic based on the Bate-Horn conjecture seems to predict an infinite number of primorial primes. To see this observe that the primorial primes are generated by the expression $f(n) = n! \pm 1$. Here, the factorial can be viewed as a product of n linear polynomials $f_k(x) = x - k$, actually this idea is used in p-adic analysis. Under this assumption, the Bate-Horn conjecture is applicable.

Heuristic 2: Let $f(x) = f_1(x)f_2(x)\cdots = x(x-1)(x-2)\cdots 2\cdot 1+1$. The congruence $f(n) \equiv 0 \bmod p$ has $\nu(p) = 0$ solutions for all primes $p \geq 2$. Hence,

$$\begin{aligned}
\pi_f(x) &= \#\{p = f(n) \leq x : p \text{ is prime } \} \qquad (10.13)\\
&\leq \sum_{p\leq x}\prod_{q\leq \log p}\left(1-\frac{1}{q}\right)^{-n}\left(1-\frac{\nu(p)}{p}\right)\frac{1}{\log(n!+1)}\\
&= \sum_{n\leq x}\prod_{p\leq n}\left(1-\frac{1}{p}\right)^{-n}\frac{1}{\log(n!+1)}\\
&\approx \sum_{n\leq x}\left(\frac{1}{e^{\gamma}\log n}\right)^{-n}\frac{1}{n\log n}\\
&= O\left(\frac{\log x}{\log\log x}\right).
\end{aligned}$$

Thus, the expected number is infinite.

10.4 Coprimorial Primes

The subset of coprimorial primes is defined by

$$\mathcal{B} = \{p = 3\cdot 5\cdot 7\cdots q+2 : \text{ prime } q \geq 2\}. \qquad (10.14)$$

The totient $p-1 = \varphi(p)$ of a coprimorial prime has very few prime divisors

$$\omega(p-1) \ll 1, \qquad (10.15)$$

and nearly maximal value

$$\frac{\varphi(p-1)}{p-1} = \prod_{q|p-1}\left(1-\frac{1}{q}\right) \approx \frac{1}{2}. \qquad (10.16)$$

The coprimorial primes have Germain primes type structure. The heuristic seems to show the existence of infinitely many coprimorial primes.

Conjecture 10.3. *As $x \to \infty$, the number of prime pairs $p = n!+1$ leqx has the asymptotic formula*

$$\pi_f(x) = \#\{p = n!/2+2 \leq x : p \textit{ is prime } \} = e^{\gamma}\log x + o(\log x).$$

Heuristic 1: Same as 10.2.
The collection of these primes is not a topic of research in the current literature.

10.5 Germain Primes

The subset of Germain primes is defined by

$$\mathcal{S} = \{p = 2^a\cdot q+1 : \text{ prime } q \geq 2 \text{ and } a \geq 1\}. \qquad (10.17)$$

The simplest sequence $p = 2q + 1$ is archived in OEIS A005384. 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

$$\omega(p-1) = 2, \tag{10.18}$$

and the nearly maximal value

$$\frac{\varphi(p-1)}{p-1} = \prod_{q|p-1} \left(1 - \frac{1}{q}\right) \approx \frac{1}{2}, \tag{10.19}$$

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

The expected number of Germain primes is derived from the Bate-Horn conjecture using the polynomials $f_1(x) = x$ and $f_2(x) = 2^a x + 1$.

Conjecture 10.4. *As $x \to \infty$, the number of prime pairs $p \leq x$ and $2^a p + 1 \leq x$ has the asymptotic formula*

$$\pi_f(x) = 2 \prod_{p \geq 3} \left(1 - \frac{1}{(p-1)^2}\right) \frac{x}{(\log x)^2} + O\left(\frac{x}{(\log x)^3}\right).$$

Heuristic: Let $f(x) = f_1(x) f_2(x) = x(2^a x + 1)$, with a small fixed integer $a \geq 1$. The congruence $f(n) \equiv 0 \bmod p$ has $\nu(p)$ solutions. Specifically,

$$\nu(p) = \begin{cases} 1 & \text{if } p = 2, \\ 2 & \text{if } p > 2. \end{cases} \tag{10.20}$$

Assembling these data yield

$$\begin{aligned} \pi_f(x) &= \#\{p \leq x : p \text{ and } 2^a p + 1 \text{ are primes } \} \\ &= 2 \sum_{n \leq x} \prod_{2 < p \leq x} \left(1 - \frac{1}{p}\right)^{-2} \left(1 - \frac{2}{p}\right) \frac{1}{\log(n) \log(2^a n + 1)} \\ &= 2 \prod_{2 < p \leq n} \left(1 - \frac{1}{(p-1)^2}\right) \sum_{n \leq x} \frac{1}{\log(n) \log(2^a n + 1)} \\ &= 2 \prod_{p \geq 3} \left(1 - \frac{1}{(p-1)^2}\right) \frac{x}{(\log x)^2} + O\left(\frac{x}{(\log x)^3}\right). \end{aligned} \tag{10.21}$$

The last line in (10.21) follows from the approximation

$$\sum_{n \leq x} \frac{1}{\log(n) \log(2^a n + 1)} \approx \sum_{n \leq x} \frac{1}{\log(n)^2} = \int_2^x \frac{1}{\log(t)^2} dt. \tag{10.22}$$

10.6 Fermat Primes

The subset of Fermat primes is defined by

$$\mathcal{S} = \{p = 2^{2^n} + 1 : n \geq\}. \tag{10.23}$$

The entire list of known has 5 primes, which are archived in OEIS A019434. The heuristic claims that there are finitely many Fermat primes. The totient $p-1 = \varphi(p)$ of a Fermat prime has one prime divisor

$$\omega(p-1) = 1, \tag{10.24}$$

and the maximal value

$$\frac{\varphi(p-1)}{p-1} = \prod_{q|p-1} \left(1 - \frac{1}{q}\right) = \frac{1}{2}. \tag{10.25}$$

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

Conjecture 10.5. *As $x \to \infty$, the number of primes $p = 2^{2^n} + 1 \leq x$ is finite.*

Heuristic: Let $p = f(n) = 2^{2^n} + 1$, and $x \geq 1$ be a large number. The calculation is based on the Gaussian probabilistic method. The Bate-Horn conjecture is not applicable to subset of primes generated by exponential functions. Specifically,

$$\begin{aligned} \pi_f(x) &= \#\{p = f(n) \leq x : p \text{ is prime } \} \\ &= \sum_{f(n)\leq x} \prod_{2<p\leq n} \left(1 - \frac{1}{p}\right)^{-1} \frac{1}{\log\left(2^{2^n}+1\right)} \\ &\leq \frac{e^{\gamma}}{\log(2)} \sum_{n \leq \log\log x} \frac{\log n}{2^n} \\ &= O(1). \end{aligned} \tag{10.26}$$

Thus, the expected number is finite, [61, p. 16].

Lemma 10.1. (Pepin test) *The number $p = 2^{2^n} + 1$ is prime if and only if the Legendre symbol*

$$\left(\frac{3}{p}\right) \equiv -1 \bmod p.$$

Proof. Use the quadratic reciprocity law. ■

10.7 Problems

Exercise 10.1. Determine whether or not the 26th Fermat number $F_n = 2^{2^{26}} + 1$ is composite or prime. Specifically, compute the quadratic symbol

$$\left(\frac{3}{2^{2^{26}}+1}\right) \equiv \pm 1 \bmod (2^{2^{26}} + 1).$$

If 3 is a quadratic nonresidue modulo F_n, then it is prime.

Exercise 10.2. Use an elementary argument to show that the largest prime divisor of the nth Fermat number F_n satisfies $P(F_n) > 2^{n+2} \geq \log F_n$.

Exercise 10.3. Prove whether or not the nth Fermat number F_n is squarefree.

Exercise 10.4. Use an elementary argument to show that the largest prime divisor of the nth Mersenne number $M_n = 2^n - 1$ satisfies $P(M_n) > n \geq \log M_n$.

Exercise 10.5. Prove whether or not the nth Mersenne number M_n is squarefree-it is sufficient to use prime values $n = p$.

Exercise 10.6. Let p_k be the kth prime in increasing order. Prove whether or not the subset of primorial primes $p = 2 \cdot 3 \cdots p_k \pm 1$ is finite.

Chapter 11

Finite Cyclic Groups

Let $n = p_1^{v_1} p_2^{v_2} \cdots p_t^{v_t}$ be an arbitrary integer, and let $\mathbb{Z}/n\mathbb{Z}$ be a finite ring. Some properties of the group of units of the finite ring

$$(\mathbb{Z}/n\mathbb{Z})^\times = U(p^{v_1}) \times U(p^{v_2}) \times \cdots \times U(p^{v_t}), \tag{11.1}$$

where $U(n)$ is a cyclic group of order $\#U(n) = \varphi(n)$ are investigated here.

11.1 Multiplicative Orders

Definition 11.1. The *order* of an element $v \in G$ in a cyclic group G is defined by $\operatorname{ord}_G(v) = \min\{n : v^n \equiv 1 \bmod G\}$, and the index is defined by $\operatorname{ind}_G(v) = \#G/\operatorname{ord}_G(v)$.

Definition 11.2. A subset of integers $\mathcal{B} \subset \mathbb{Z}$ with respect to a fixed base $v \geq 2$ if the order and the index are nearly equal: $\operatorname{ord}_n(v) \approx \operatorname{ind}_n(v) \approx \sqrt{n}$ for each $n \in \mathcal{B}$.

The order function maps the multiplicative group onto the the set of divisors of an integer. The diagram below specifies the basic assignments.

$$\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & \mathcal{D}(m) = \{d \mid m\}, \\ u & \longrightarrow & \operatorname{ord}_n(u) = d. \end{array} \tag{11.2}$$

where $m = \lambda(n)$, and $d \mid m$.

Lemma 11.1. *The order* $\operatorname{ord} : G \longrightarrow \mathbb{N}$ *is multiplicative function on a multiplicative subgroup* G *of cardinality* $\#G = \lambda(n)$ *in* $\mathbb{Z}/n\mathbb{Z}$*, and it has the followings properties.*

(i) $\operatorname{ord}_n(u \cdot v) = \operatorname{ord}_n(u) \operatorname{ord}_n(v)$, *if* $\gcd(\operatorname{ord}_n(u), \operatorname{ord}_n(v)) = 1$.
(ii) $\operatorname{ord}_n(u^k) = \operatorname{ord}_n(u)/\gcd(k, n)$, *for any pair of integers* $k, n \geq 1$.

The Carmichael function specifies the maximal order of a cyclic subgroup G of the finite ring $\mathbb{Z}/n\mathbb{Z}$, and the maximal order $\lambda(n) = \max\{m \geq 1 : v^m \equiv 1 \bmod n\}$ of the elements in a finite cyclic group G.

Definition 11.3. An integer $u \in \mathbb{Z}$ is called a *primitive root* mod n if the least exponent $\min\{m \in \mathbb{N} : u^m \equiv 1 \bmod n\} = \lambda(n)$.

In synopsis, primitive elements in a cyclic group have the maximal orders $\mathrm{ord}_G(v) = \#G$, and minimal indices $\mathrm{ind}_G(v) = 1$.

Lemma 11.2. (Primitive root test) *Let $p \geq 3$ be a prime, and let $a \geq 2$ be an integer such* $\gcd(a, p) = 1$. *Then,*
the integer a is a primitive root if and only if

$$a^{(p-1)/q} - 1 \not\equiv 0 \bmod p \tag{11.3}$$

for every prime divisor $q \mid p - 1$.

Proof. This is a restricted version of the Pocklington primality test, see [16, p. 175]. ■

Lemma 11.3. *For any integer $n \geq 1$, and the group $\mathbb{Z}/n\mathbb{Z}$, the followings hold.*

(i) *The group of units $(\mathbb{Z}/n\mathbb{Z})^\times$ has $\varphi(n)$ units.*

(ii) *The number of primitive root is given by*

$$\varphi(\varphi(n)) = \varphi(n) \prod_{p \mid \varphi(n)} \left(1 - \frac{1}{p^{m(p)}}\right), \tag{11.4}$$

where $m(p) \geq 1$ is the number of invariant factor associate with p.

The Euler totient function and the more general Carmichael totient function over the finite ring $\mathbb{Z}/n\mathbb{Z}$ are seamlessly linked by the Fermat-Euler Theorem.

Lemma 11.4. (Fermat-Euler) *If $a \in \mathbb{Z}$ is an integer such that* $\gcd(a, n) = 1$, *then* $a^{\varphi(n)} \equiv 1 \bmod n$.

The improvement provides the least exponent $\lambda(n) \mid \varphi(n)$ such that $a^{\lambda(n)} \equiv (1 \bmod n)$.

Lemma 11.5. ([18]) *Let $n \in \mathbb{N}$ be any given integer. Then*

(i) *The congruence $a^{\lambda(n)} \equiv 1 \bmod n$ is satisfied by every integer $a \geq 1$ relatively prime to n, that is* $\gcd(a, n) = 1$.

(ii) *In every congruence $x^{\lambda(n)} \equiv 1 \bmod n$, a solution $x = u$ exists which is a primitive root* mod n, *and for any such solution u, there are $\varphi(\lambda(n))$ primitive roots congruent to powers of u.*

Proof. (i) The number $\lambda(n)$ is a multiple of every $\lambda(p^v) = \varphi(p^v)$ such that $p^v \mid n$. Ergo, for any relatively prime integer $a \geq 2$, the system of congruences

$$a^{\lambda(n)} \equiv 1 \bmod p_1^{v_1}, \quad a^{\lambda(n)} \equiv 1 \bmod p_2^{v_2}, \quad \ldots, \quad a^{\lambda(n)} \equiv 1 \bmod p_t^{v_t}, \tag{11.5}$$

where $t = \omega(n)$ is the number of prime divisors in n, is valid. ■

Properties of the Discrete Logarithm Function
The discrete logarithm function, with respect to the fixed primitive element $\log_\tau$, maps the multiplicative group into a cyclic group. The diagram below specifies the basic assignments.

$$\begin{array}{rcl} (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & \mathbb{Z}/m\mathbb{Z}, \\ u = \tau^k & \longrightarrow & \log_\tau(u) = k. \end{array} \tag{11.6}$$

where $m = \lambda(n)$, and $k \leq m$.

Lemma 11.6. *Let $m, n \in \mathbb{Z}$ be integers, and let τ be a primitive root modulo n. Then, for any nonzero elements $u, v \in (\mathbb{Z}/n\mathbb{Z})^\times$ in the multiplicative group modulo n, the followings hold.*

(i) $\log_\tau(u) \equiv \log_\tau(v)$, *then* $u \equiv v \bmod \lambda(n)$.

(ii) $\log_\tau(uv) \equiv \log_\tau(u) + \log_\tau(v) \bmod \lambda(n)$.

(iii) $\log_\tau(u^m) \equiv m \log_\tau(u) \bmod \lambda(n)$.

11.2 Maximal Cyclic Subgroups

The multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ has $\xi(n) = \varphi(n)/\lambda(n)$ maximal cyclic subgroups

$$G_1 \cup G_2 \cup \cdots \cup G_t = (\mathbb{Z}/n\mathbb{Z})^\times \tag{11.7}$$

of order $\#G_i = \lambda(n)$, and $G_i \cap G_j = \{1\}$ for $i \neq j$ with $1 \leq i, j \leq t = \xi(n)$. Each maximal subgroup G_i has a unique subset
of $\varphi(\lambda(n))$ primitive roots. The optimal case $G_1 = (\mathbb{Z}/n\mathbb{Z})^\times$ for $\xi(n) = 1$ occurs on a
subset of integers of zero density, the next lemma is the best known result, see also Lemma 4.5.

Lemma 11.7. (Gauss) *Let $p \geq 3$ be a prime, and let $n \geq 1$ be an integer. Then, the multiplicative groups has the following properties.*

(i) $(\mathbb{Z}/p^n\mathbb{Z})^\times$ *is cyclic of order $\varphi(p^n)$, and there exists a primitive root of the same order.*

(ii) $(\mathbb{Z}/2p^n\mathbb{Z})^\times$ *is cyclic of order $\varphi(2p^n)$, and there exists a primitive root of the same order.*

Proof. The proof and additional information appear in [1, Theorem 10.7], and [98, Theorem 2.6]. ■

Lemma 11.8. *Let $n \geq 2$ be an integer. Then, the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic of order $\varphi(n)$ if and only if $\varphi(n) = \lambda(n)$.*

Proof. Try to prove this as an exercise. ■

Extensive details on this topic appear in [17].

Lemma 11.9. *Let p and q be primes, and let $n = pq \geq 2$. Then, the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is cyclic of order $\varphi(n)/2$ if and only if the totients $p-1$ and $q-1$ are squarefree and relatively prime.*

Proof. The Carmichael function is maximal if and only if $\gcd(p-1, q-1) = 2$. Under this condition, $\lambda(n) = \lambda(pq) = (p-1)(q-1)/2 = \varphi(n)/2$. ■

Given a $p-1$ squarefree totient, it is natural to expect that the occurrence of another squarefree and relatively totient $q-1$ is a dependent event. The numerical parameter $c_s \geq 0$, referred to as the prime dependence correction factor, is used to adjust and account for this phenomenon.

Theorem 11.1. *Let $p, q, r \geq 2$ be primes, and let $x \geq 1$ be a large number. Suppose that $p-1 > 2$, $q-1 > 2$, and $r-1 > 2$ are squarefree, and relatively prime totients. Then, the following average orders of pairs and triples of squarefree totients are true.*

(i) $$N(p,q) = \frac{3c_2}{4} \prod_{p \geq 3} \left(1 - \frac{1}{(p-1)^2}\right) \frac{x^2}{(\log x)^2} \left(1 + O\left(\frac{1}{(\log x)^3}\right)\right),$$

where $p, q \leq x$ and $c_2 \geq 0$ is a prime dependence correction factor.

(ii) $$N(p,q,r) = \frac{7c_3}{8} \prod_{p \geq 3} \left(1 - \frac{1}{(p-1)^3}\right) \frac{x^3}{(\log x)^3} \left(1 + O\left(\frac{1}{(\log x)^4}\right)\right),$$

where $p, q, r \leq x$ and $c_3 \geq 0$ is a prime dependence correction factor.

Proof. (i) Simultaneous squarefree and relatively prime totients means that the indicator function, written in term of Mobious function, is

$$\sum_{\substack{d|(p-1)/2 \\ d|(q-1)/2}} \mu(d) = \begin{cases} 1 & \gcd((p-1)/2, (q-1)/2) = 1, \\ 0 & \gcd((p-1)/2, (q-1)/2) \neq 1, \end{cases} \tag{11.8}$$

Summing over all the prime pairs $p, q \leq x$, and reversing the order of summation, returns

$$\begin{aligned} \sum_{p,q \leq x} \sum_{\substack{d|(p-1)/2 \\ d|(q-1)/2}} \mu(d) &= c_2 \sum_{d \leq x} \mu(d) \sum_{\substack{p \leq x \\ p \equiv 1 \bmod 2d,}} 1 \sum_{\substack{q \leq x \\ q \equiv 1 \bmod 2d}} 1 \\ &= c_2 \sum_{d \leq x} \mu(d) \cdot \pi(x, 2d, 1)^2, \end{aligned} \tag{11.9}$$

where $c_2 \geq 0$ is a prime dependence correction factor. Assume the restriction to $d \leq (\log x)^B$, where $B > 0$ is a constant, and apply the Siegel-Walfisz theorem.

After some simplification, it yields

$$\begin{aligned} c_2 \sum_{d\le x} \mu(d)\cdot \pi(x,2d,1)^2 &= c_2 \sum_{d\le (\log x)^B} \mu(d)\cdot \pi(x,2d,1)^2 + c_2 \sum_{d>(\log x)^B} \mu(d)\cdot \pi(x,2d,1)^2 \\ &= c_2 \sum_{d\le (\log x)^B} \mu(d)\cdot \left(\frac{x}{\varphi(2d)\log x} + O\left(\frac{x}{(\log x)^C}\right)\right)^2 \\ &\qquad + O\left(\sum_{d>(\log x)^B} \left(\frac{x}{d}\right)^2\right) \\ &= c_2 \sum_{d\ge 1} \frac{\mu(d)}{\varphi(2d)^2}\frac{x^2}{(\log x)^2} + O\left(\frac{x^2}{(\log x)^B}\right). \end{aligned} \tag{11.10}$$

This is nontrivial for $B > 2$, and $C > 2$. The density constant is

$$c_2 \sum_{d\ge 1} \frac{\mu(d)}{\varphi(2d)^2} = \frac{3c_2}{4}\prod_{p\ge 3}\left(1-\frac{1}{(p-1)^2}\right). \tag{11.11}$$

(ii) Given a prime triple p, q, r, use the indicator function

$$\sum_{\substack{d\mid (p-1)/2\\ d\mid (q-1)/2\\ d\mid (r-1)/2}} \mu(d) = \begin{cases} 1 & \gcd((p-1)/2,(q-1)/2,(r-1)/2) = 1,\\ 0 & \gcd((p-1)/2,(q-1)/2,(r-1)/2) \ne 1, \end{cases} \tag{11.12}$$

and take the sum over all the prime triples $p, q, r \le x$. Continue as in the previous case, mutatis mutandis. ■

The determination of the actual value of the prime dependence correction factor $c_2 \ge 0$ could be a difficult problem in algebraic number theory. Obviously, if the prime pairs are $p \le x$ and $q \le x$ independent, then $c_2 = 1$.

11.3 Basic Primitive Roots Properties

Properties of the Order Function

The order function maps the multiplicative group $\mathbb{F}_p^\times$ onto the the set of divisors of $p-1$. The diagram below specifies the basic assignments.

$$\begin{array}{ccc} \mathbb{F}_p^\times & \longrightarrow & \mathcal{D}(p-1) = \{d \mid p-1\}, \\ u & \longrightarrow & \mathrm{ord}_p(u) = d, \end{array} \tag{11.13}$$

where $d \mid p-1$.

Lemma 11.10. *Let $k, m, n \in \mathbb{Z}$ be integers. Then, for any nonzero elements $u, v \in \mathbb{F}_p^\times$ in the multiplicative group modulo p, the followings hold.*

(i) *If* $\mathrm{ord}_p(u) = k$, *then* $k \mid p-1$.

(ii) *If* $\mathrm{ord}_p(u) = k$, *then* $\mathrm{ord}_p(u^m) = \frac{k}{\gcd(k,m)}$.

(iii) $\mathrm{ord}_p(u^m) = \frac{p-1}{\gcd(m,n)}$.

(iv) *If* $\mathrm{ord}_p(u) = k$, *and* $\mathrm{ord}_p(v) = m$, *then* $\mathrm{ord}_p(uv) = \frac{km}{\gcd(k,m)}$.

Properties of the Discrete Logarithm Function
The discrete logarithm function, with respect to the fixed primitive element $\log_\tau$, maps the multiplicative group into a cyclic group $\mathbb{F}_p^\times$. The diagram below specifies the basic assignments.

$$\begin{array}{rcl} \mathbb{F}_p^\times & \longrightarrow & \mathbb{Z}/(p-1)\mathbb{Z}, \\ u = \tau^k & \longrightarrow & \log_\tau(u) = k. \end{array} \tag{11.14}$$

where $k \leq p-1$.

Lemma 11.11. *Let $m, n \in \mathbb{Z}$ be integers, and let τ be a primitive root modulo n. Then, for any nonzero elements $u, v \in \mathbb{F}_p^\times$ in the multiplicative group, the followings hold.*

(i) $\log_\tau(u) \equiv \log_\tau(v)$, *then* $u \equiv v \bmod (p-1)$.

(ii) $\log_\tau(uv) \equiv \log_\tau(u) + \log_\tau(v) \bmod (p-1)$.

(iii) $\log_\tau(u^m) \equiv m \log_\tau(u) \bmod (p-1)$.

11.4 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 11.4. The order $\min\{k \in \mathbb{N} : u^k \equiv 1 \bmod p\}$ of an element $u \in \mathbb{F}_p$ is denoted by $\mathrm{ord}_p(u)$. An element is a *primitive root* if and only if $\mathrm{ord}_p(u) = p-1$.

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

Lemma 11.12. (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 11.13. (Primitive root test) *An integer $u \in \mathbb{Z}$ is a primitive root modulo an integer $n \in \mathbb{N}$ if and only if*

$$u^{\varphi(n)/p} - 1 \not\equiv 0 \mod n \tag{11.15}$$

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

The primitive root test is a special case of the Lucas primality test, introduced in [72, p. 302]. A more recent version appears in [16, Theorem 4.1.1], and similar sources.

Lemma 11.14. (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 [111, Chapter 11]. By [15, 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 $\varepsilon > 0$. ■

11.5 Mean Average Multiplicative Order

The *multiplicative order* of an element u in a finite group G of cardinality $n = \#G$ is defined by $\operatorname{ord}_n u = \min\{m : u^m \equiv 1 \bmod n\}$. The definition of the average multiplicative order in a fixed finite group has a very useful analytic formulation.

Definition 11.5. Let G be a cyclic group of order $n = \#G$. The average multiplicative order of the elements $u \in G$ is defined by

$$A(n) = \frac{1}{n}\sum_{u\in G} \operatorname{ord}_n u = \frac{1}{n}\sum_{d|n} d\varphi(d). \tag{11.16}$$

Lemma 11.15. *The mean average order* $\overline{A(n)}$ *of the elements in a finite cyclic group of order* $n\#G$, $n \le x$ *is*

$$\overline{A(n)} = a_0 x + O(\log x),$$

where the constant is

$$a_0 = \zeta(3)/2\zeta(2) = 0.365381484700719249363018365653857\ldots.$$

Proof. Taking the mean value of the average multiplicative order gives

$$\begin{aligned} \frac{1}{x}\sum_{n\le x} A(n) &= \frac{1}{x}\sum_{n\le x}\frac{1}{n}\sum_{d|n} d\varphi(d) \\ &= \frac{1}{x}\sum_{m\le x}\frac{1}{m}\sum_{d\le x/m}\varphi(d). \end{aligned} \tag{11.17}$$

The condition $d \mid n$ was used to cancel the d term in the inner sum. Applying Theorem 4.1 leads to

$$\begin{aligned} \frac{1}{x}\sum_{n\le x} A(n) &= \frac{1}{x}\sum_{m\le x}\frac{1}{m}\left(\frac{1}{2\zeta(2)}\left(\frac{x}{m}\right)^2 + O\left(\frac{x}{m}\log(x/m)\right)\right) \\ &= \frac{x}{2\zeta(2)}\sum_{m\le x}\frac{1}{m^3} + O\left((\log x)\sum_{m\le x}\frac{1}{m}\right) \\ &= \frac{\zeta(3)}{2\zeta(2)}x + O\left(\log x\right). \end{aligned} \tag{11.18}$$

■

The double averaging accounts for the small error term. Moreover, since the mean average order $\overline{A(n)}$ is almost the same magnitute as the largest groups $\#G = n \approx x$, this result shows that the generators of the cyclic group, elements of maximal multiplicative orders, contribute the sheer bulk of the of the mean average order. A slightly more difficult proof appears in [119, Theorem 3.1].

Almost every element in a random finite cyclic group G of cardinality $n = \#G \le x$ has a large order bounded below by $\operatorname{ord}_n u \gg n/\log n$.

Theorem 11.2. ([67, Theorem 6]) *Assume GRH. Let* x *be a large number, and let* G *be finite cyclic group of cardinality* $n = \#G \le x$. *Then, almost every element* $u \in G$ *has large multiplicative order* $\operatorname{ord}_n u \gg n/\log x$.

11.6 Problems

11.6.1 Cyclic Groups Related Problems

Exercise 11.1. *Show that the multiplicative groups* $(\mathbb{Z}/4p\mathbb{Z})^\times$ *and* $(\mathbb{Z}/pq\mathbb{Z})^\times$ *of the rings of integers modulo* $n = 4p$ *or* $n = pq$ *have the maximal order* $\lambda(n) = \varphi(n)/2$ *if* $p - 1 > 2$ *and* $q - 1 > 2$ *are squarefree, and relatively prime.*

Exercise 11.2. *Let* $n = pq \leq x^2$*, and* $2 < p - 1 \leq x$ *and* $2 < q - 1 \leq x$ *are squarefree, and relatively prime. Show that average probability of a nonzero element* u *of being a primitive root in the multiplicative group* $(\mathbb{Z}/pq\mathbb{Z})^\times$ *is*

$$P(\mathrm{ord}(u) = \lambda(n)) \asymp \frac{1}{(\log x)^2}$$

.

11.6.2 Primitive Roots Related Problems

Exercise 11.3. (Gauss) Given an integer $n \geq 2$, show that

$$\prod_{\substack{1 \leq a \leq n \\ \gcd(a,n)=1}} a = \begin{cases} -1 & \text{if } n \text{ has a primitive root,} \\ 1 & \text{if } n \text{ does not have a primitive root.} \end{cases}$$

Exercise 11.4. Let $n \geq 2$ and $a \geq 1$ be a pair of integers, and define the function $f(a, n) = \sum_{d|n} a^d \mu(n/d)$.

(a) Prove that $f(a, n) \equiv 0 \bmod n$.

(b) If $p = 2$ is prime and $a < p$, then $f(a, n) \equiv 0 \bmod n$ is equivalent to the Fermat little theorem $a^{p-1} \equiv 1 \bmod p$

(c) If $n = pq$, p, q primes, then $f(a, n)$ reduces to $a^p + q^q \equiv a^n + a \bmod n$.

11.6.3 Algorithm Problems

Exercise 11.5. 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 11.6. 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.

Exercise 11.7. Develop a divisor-free primitive root test. The standard primitive root test is totally dependent on the divisors of $p - 1$.

11.6.4 Open Problems

Exercise 11.8. (Sarkozy conjecture) Let $\mathcal{R} = \mathcal{R}_p$ be the set of primitive roots modulo p. Prove that there is an additive partition of disjoint subsets

$$\mathcal{R} = \mathcal{A} + \mathcal{B}.$$

Chapter 12

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.

12.1 Simple Characters Sums

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

$$\chi(u) = e^{i2\pi k \log(u)/d}, \tag{12.1}$$

where $v = \log u$ is the discrete logarithm of $u \neq 0$ with respect to some primitive root, and for some integer $k \in \mathbb{Z}$, see [75, p. 187], [87, p. 118], and [62, p. 271]. The principal character $\chi_0 = 1 \bmod q$ has order $d = 1$, and it is defined by the relation

$$\chi_0(n) = \begin{cases} 1 & \text{if } \gcd(n, q) = 1, \\ 0 & \text{if } \gcd(n, q) \neq 1. \end{cases} \tag{12.2}$$

And the nonprincipal character $\chi \neq 1 \bmod q$ of order $\text{ord}(\chi) = d > 1$ is defined by the relation

$$\chi(n) = \begin{cases} \omega^{\log n} & \text{if } \gcd(n, q) = 1, \\ 0 & \text{if } \gcd(n, q) \neq 1, \end{cases} \tag{12.3}$$

where $\omega \in \mathbb{C}$ is a dth root of unity.

Lemma 12.1. *For a fixed integer $u \neq 0$, and an integer $q \in \mathbb{N}$, let $\chi \neq 1$ be nonprincipal character mod q, then*

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

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

12.2 Divisors Dependent Characteristic Function

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

Lemma 12.2. *Let G be a finite cyclic group of order $p-1 = \#G$, and let $0 \neq u \in G$ be an invertible element of the group. Then*

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

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

$$\sum_{\mathrm{ord}(\psi)=q} \chi(u) = \sum_{\mathrm{ord}(\psi)=q} \chi(\tau^{qm}) = \sum_{\mathrm{ord}(\psi)=q} \chi(\tau^m)^q = \varphi(q) = q-1, \tag{12.4}$$

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

$$\begin{aligned} \frac{\phi(p-1)}{p-1} \sum_{d|p-1} \frac{\mu(d)}{\varphi(d)} \sum_{\mathrm{ord}(\chi)=d} \chi(u) &= \frac{\phi(p-1)}{p-1} \prod_{q|p-1} \left(1 - \frac{\sum_{\mathrm{ord}(\chi)=q} \chi(u)}{q-1}\right) \\ &= \frac{\phi(p-1)}{p-1} \prod_{q|p-1} \left(1 - \frac{q-1}{q-1}\right) = 0. \end{aligned} \tag{12.5}$$

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

$$\sum_{\mathrm{ord}(\psi)=q} \chi(u) = \sum_{\mathrm{ord}(\psi)=q} \chi(\tau^m) = -1. \tag{12.6}$$

Replacing this information into the product

$$\begin{aligned} \frac{\phi(p-1)}{p-1} \sum_{d|p-1} \frac{\mu(d)}{\varphi(d)} \sum_{\mathrm{ord}(\chi)=d} \chi(u) &= \frac{\phi(p-1)}{p-1} \prod_{q|p-1} \left(1 - \frac{\sum_{\mathrm{ord}(\chi)=q} \chi(u)}{q-1}\right) \\ &= \frac{\phi(p-1)}{p-1} \prod_{q|p-1} \left(1 - \frac{-1}{q-1}\right) = 1. \end{aligned} \tag{12.7}$$

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

The works in [22], and [121] attribute this formula to Vinogradov. The proof and other details on the characteristic function are given in [33, p. 863], [75, p. 258], [82, p. 18]. The characteristic function for multiple primitive roots is used in [20, p. 146] to study consecutive primitive roots. In [28] it is used to study the gap between primitive roots with respect to the Hamming metric. And in [121] it is used to prove the existence of primitive roots in certain small subsets $A \subset \mathbb{F}_p$. In [22] 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 [92] using this formula.

12.3 Divisors Free Characteristic Function

It often difficult to derive any meaningful result using the usual divisors dependent characteristic function of primitive elements given in Lemma 12.2. This difficulty is due to the large number of terms that can be generated by the divisors, for example, $d \mid p-1$, involved in the calculations, see [33], [28] for typical applications and [81, 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 12.2, 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 12.3, 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 12.3. *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*

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

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

$$\tau^n - u = 0 \tag{12.8}$$

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

$$\Psi(u) = \sum_{\gcd(n,p-1)=1} \frac{1}{p} \sum_{0 \leq m \leq p-1} e^{i2\pi(\tau^n - u)m/p} = \begin{cases} 1 & \text{if } \operatorname{ord}_p(u) = p-1, \\ 0 & \text{if } \operatorname{ord}_p(u) \neq p-1. \end{cases} \tag{12.9}$$

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

12.4 Smooth Integer Characteristic Function

For an integer $n \geq 1$, the largest prime divisor function has the usual formula $P(n) = \max\{p \mid n\} = p$, the radical is given by the product $rad(n) = \prod_{p|n} p$. Further, set $Q(z) = \prod_{p \leq z} p$.

Lemma 12.4. *Let $p \geq 2$ be a prime, and let $B \geq 1$ be a real parameter. The indicator function of B-smooth integers has the form*

$$\mathcal{S}_B(n) = \frac{1}{p} \sum_{0 \leq a \leq p-1} e^{\frac{i2\pi Q(n)a}{rad(n)}} = \begin{cases} 1 & \text{if } P(n) \leq B, \\ 0 & \text{if } P(n) \not\leq B. \end{cases}$$

Proof. Routine exercise. ■

12.5 Arbitrary Subset Characteristic Function

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

Lemma 12.5. *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,*

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

Proof. Consider the equation

$$x - u = 0 \tag{12.10}$$

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

12.6 Characteristic Functions For Quadratic Residues

The standard characteristic function of quadratic residues and quadratic nonresidues are induced by the quadratic symbol.

Lemma 12.6. *Let $p \geq 2$ be a prime, and let $(x \,|\, p)$ be the quadratic character mod p. Then,*

(i) $$\Psi_2(u) = \frac{1}{2}\left(1 + \left(\frac{u}{p}\right)\right) = \begin{cases} 1 & \text{if } u^{(p-1)/2} \equiv 1 \bmod p, \\ 0 & \text{if } u^{(p-1)/2} \equiv -1 \bmod p. \end{cases}$$

(ii) $$\overline{\Psi}_2(u) = \frac{1}{2}\left(1 - \left(\frac{u}{p}\right)\right) = \begin{cases} 1 & \text{if } u^{(p-1)/2} \equiv -1 \bmod p, \\ 0 & \text{if } u^{(p-1)/2} \equiv 1 \bmod p. \end{cases}$$

are the characteristic functions for quadratic residues and quadratic non residues modulo p respectively in the finite field $\mathbb{F}_p$.

A new representation of the characteristic function for quadratic residues and quadratic nonresidues are introduced below.

Lemma 12.7. *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, then*

$$\text{(i)}\ \ \Psi_2(u) = \sum_{0 \leq n < (p-1)/2} \frac{1}{p} \sum_{0 \leq m \leq p-1} e^{i2\pi\left(\tau^{2n}-u\right)m/p} = \begin{cases} 1 & \text{if } n^{(p-1)/2} \equiv 1 \bmod p, \\ 0 & \text{if } n^{(p-1)/2} \equiv -1 \bmod p. \end{cases}$$

$$\text{(ii)}\ \ \overline{\Psi}_2(u) = \sum_{0 \leq n < (p-1)/2} \frac{1}{p} \sum_{0 \leq m \leq p-1} e^{i2\pi\left(\tau^{2n+1}-u\right)m/p} = \begin{cases} 1 & \text{if } n^{(p-1)/2} \equiv -1 \bmod p, \\ 0 & \text{if } n^{(p-1)/2} \equiv 1 \bmod p. \end{cases}$$

Proof. (i) The finite field $\mathbb{F}_p$ equation

$$\tau^{2n} - u = 0 \tag{12.11}$$

has a unique solution $n = n_0 \in \{0, 1, 2, \ldots (p-1)/2 - 1\}$ if and only if $u \neq 0$ is a quadratic residue modulo p. This, in turns, implies that the inner exponential sum collapses to p. Otherwise, $\tau^{2n} - u \neq 0$, which implies that the inner exponential sum vanishes. ■

12.7 Characteristic Functions Modulo Prime Powers

The standard method for constructing characteristic function for primitive elements are discussed in [98, Corollary 3.5], [75, p. 258], and some characteristic functions for finite rings are discussed in [65]. These type of characteristic functions detect the orders of the elements $v \in (\mathbb{Z}/p^2\mathbb{Z})^\times$ by means of the divisors of $\varphi(p^2) = \#G$. A new method for constructing characteristic functions for certain elements in cyclic groups is developed here. These type of characteristic functions detect the orders of the elements $v \in (\mathbb{Z}/p^2\mathbb{Z})^\times$ by means of the solutions of the equation $\tau^{pn} - v \equiv 0 \bmod p^2$, where v, τ are constants, and n is a variable such that $1 \leq n < p-1$, and $\gcd(n, p-1) = 1$. The formula $\varphi(n) = \prod_{p|n}(1 - 1/p)$ denotes the Euler totient function.

Lemma 12.8. *Let $p \geq 3$ be a prime, and let τ be a primitive root* $\bmod p^2$. *Let $v \in (\mathbb{Z}/p^2\mathbb{Z})^\times$ be a nonzero element. Then*

$$\Psi_v(p^2) = \sum_{\substack{1 \leq n < p-1 \\ \gcd(n,p-1)=1}} \frac{1}{\varphi(p^2)} \sum_{0 \leq m < \varphi(p^2)} e^{\frac{i2\pi(\tau^{pn}-v)m}{\varphi(p^2)}} = \begin{cases} 1 & \text{if } \operatorname{ord}_{p^2}(v) = p-1, \\ 0 & \text{if } \operatorname{ord}_{p^2}(v) \neq p-1. \end{cases}$$

Proof. Let $\tau \in (\mathbb{Z}/p^2\mathbb{Z})^\times$ be a fixed primitive root of order $p(p-1) = \varphi(p^2)$. As the index $n \geq 1$ ranges over the integers relatively prime to $p-1$, the element $\tau^{pn} \in (\mathbb{Z}/p^2\mathbb{Z})^\times$ ranges over the elements of order $\operatorname{ord}_{p^2}(\tau^{pn}) = p-1$. Hence, the equation

$$\tau^{pn} - v = 0 \tag{12.12}$$

has a solution if and only if the fixed element $(\mathbb{Z}/p^2\mathbb{Z})^\times$ is an elements of order $\mathrm{ord}_{p^2}(v) = p-1$. Setting $w = e^{i2\pi(\tau^{pn}-v)/\varphi(p^2)}$ and summing the inner sum yield

$$\sum_{\gcd(n,p-1)=1} \frac{1}{\varphi(p^2)} \sum_{0\le m<\varphi(p^2)} w^m = \begin{cases} 1 & \text{if } \mathrm{ord}_{p^2}(v) = p-1, \\ 0 & \text{if } \mathrm{ord}_{p^2}(v) \neq p-1. \end{cases} \tag{12.13}$$

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

The characteristic function for any element $v \ge 2$ of order $\mathrm{ord}_{p^2}(v) = d \mid p-1$ in the cyclic group $(\mathbb{Z}/p^2\mathbb{Z})^\times$ is a sum of characteristic functions.

Lemma 12.9. *Let Let $v \ge 2$ be a fixed base, let $p \ge 3$ be a prime, and let τ be a primitive root* $\bmod p^2$*. The indicator function for the subset of primes such that $v^{p-1} - 1 \equiv 0 \bmod p^2$ is given by*

$$\begin{aligned} \Psi_0(p^2) &= \sum_{d\mid p-1} \sum_{\substack{1\le n<p-1 \\ \gcd(n,(p-1)/d)=1}} \frac{1}{\varphi(p^2)} \sum_{0\le m<\varphi(p^2)} e^{\frac{i2\pi(\tau^{dpn}-v)m}{\varphi(p^2)}} \\ &= \begin{cases} 1 & \textit{if } \mathrm{ord}_{p^2}(v) \mid p-1, \\ 0 & \textit{if } \mathrm{ord}_{p^2}(v) \nmid p-1. \end{cases} \end{aligned} \tag{12.14}$$

Proof. Suppose that $\mathrm{ord}_{p^2}(v) = p-1$. Then, there is a unique pair $d \mid p-1$ and $n \ge 1$ with $\gcd(n,(p-1)/d) = 1$ such that $\tau^{dpn} - v \equiv 0 \bmod p^2$. Otherwise, $\tau^{dpn} - v \not\equiv 0 \bmod p^2$ for all pairs $d \mid p-1$ and $\gcd(n,(p-1)/d) = 1$. Proceed as in the proof of Lemma 12.8. ■

Lemma 12.10. *Let $p \ge 3$ be a prime, and let τ be a primitive root* $\bmod p^k$*. Let $v \in \left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$ be a nonzero element. Then*

$$\Psi_v(p^k) = \sum_{\substack{1\le n<p-1 \\ \gcd(n,p-1)=1}} \frac{1}{\varphi(p^k)} \sum_{0\le m<\varphi(p^k)} e^{\frac{i2\pi(\tau^{p^{k-1}n}-v)m}{\varphi(p^k)}} = \begin{cases} 1 & \textit{if } \mathrm{ord}_{p^k}(v) = p-1, \\ 0 & \textit{if } \mathrm{ord}_{p^k}(v) \neq p-1. \end{cases}$$

Proof. Modify the proof of Lemma 12.8 to fit the finite ring $\mathbb{Z}/p^k\mathbb{Z}$. ■

12.8 Characteristic Functions Modulo n

The indicator function for primitive root in a maximal cyclic group $G \subset \mathbb{Z}/n\mathbb{Z}$ is simpler than the indicator function for primitive root in $\mathbb{Z}/n\mathbb{Z}$, which is a sum of indicator functions for its maximal cyclic groups $G_1, G_2, \ldots, G_e$, with $e \ge 1$.

Lemma 12.11. *Let $n \ge 3$ be an integer, and let $\tau \in G$ be a primitive root* $\bmod n$ *in a maximal cyclic subgroup $G \subset (\mathbb{Z}/n\mathbb{Z})^\times$. If $v \neq \pm u^2$ is an integer, then*

$$\Psi_v(G) = \sum_{\substack{1\le m<\lambda(n) \\ \gcd(m,\lambda(n))=1}} \frac{1}{\varphi(n)} \sum_{0\le r<\varphi(n)} e^{\frac{i2\pi(\tau^m-v)r}{\varphi(n)}} = \begin{cases} 1 & \textit{if } \mathrm{ord}_n(v) = \lambda(n), \\ 0 & \textit{if } \mathrm{ord}_n(v) \neq \lambda(n). \end{cases}$$

Proof. Let $\tau \in G$ be a fixed primitive root of order $\lambda(n)$, see Lemma 11.7. As the index $m \geq 1$ ranges over the integers relatively prime to $\lambda(n)$, the element $\tau^m \in G$ ranges over the elements of order $\mathrm{ord}_n(\tau^m) = \lambda(n)$. Hence, the equation

$$\tau^m - v = 0 \tag{12.15}$$

has a solution if and only if the fixed element $v \in G$ is an element of order $\mathrm{ord}_n(v) = \lambda(n)$. Next, let $w = e^{i2\pi(\tau^m - v)/\varphi(n)}$. Summing the inner sum yields

$$\sum_{\gcd(m,\lambda(n))=1} \frac{1}{\varphi(n)} \sum_{0 \leq r < \varphi(n)} e^{\frac{i2\pi(\tau^m - v)r}{\varphi(n)}} = \begin{cases} 1 & \text{if } \mathrm{ord}_n(v) = \lambda(n), \\ 0 & \text{if } \mathrm{ord}_n(v) \neq \lambda(n). \end{cases} \tag{12.16}$$

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

Lemma 12.12. *Let $n \geq 3$ be an integer, and let $\xi(n) = \varphi(n)/\lambda(n)$. Let $\tau_i \in G_i$ be a primitive root* mod$n$ *in a maximal cyclic subgroup $G_i \subset (\mathbb{Z}/n\mathbb{Z})^\times$. If $v \neq \pm u^2$ is an integer, then*

$$\Psi_1(n) = \sum_{1 \leq i \leq \xi(n)} \sum_{\substack{1 \leq m < \lambda(n) \\ \gcd(m,\lambda(n))=1}} \frac{1}{\varphi(n)} \sum_{0 \leq r < \varphi(n)} e^{\frac{i2\pi(\tau_i^m - v)r}{\varphi(n)}} = \begin{cases} 1 & \textit{if } \mathrm{ord}_n(v) = \lambda(n), \\ 0 & \textit{if } \mathrm{ord}_n(v) \neq \lambda(n). \end{cases}$$

Proof. This is a sum of $\xi(n) \geq 1$ copies of the indicator function proved in Lemma 12.11. ■

The last one considered is the indicator function for elements of order $\mathrm{ord}_{n^2}(v) \mid \lambda(n)$ in $\mathbb{Z}/n^2\mathbb{Z}$. This amounts to a double sum of indicator functions for its maximal cyclic groups $G_1, G_2, \ldots, G_e$, with $e \geq 1$.

Lemma 12.13. *Let $n \geq 3$ be an integer, and let $\xi(n) = \varphi(n)/\lambda(n)$. Let $\tau_i \in G_i$ be a primitive root* mod$n$ *in a maximal cyclic subgroup $G_i \subset (\mathbb{Z}/n^2\mathbb{Z})^\times$. If $v \neq \pm u^2$ is an integer, then*

$$\begin{aligned} \Psi_0(n^2) &= \sum_{1 \leq i \leq \xi(n)} \sum_{d \mid \lambda(n)} \sum_{\substack{1 \leq m < \lambda(n) \\ \gcd(m,\lambda(n)/d)=1}} \frac{1}{\varphi(n^2)} \sum_{0 \leq r < \varphi(n^2)} e^{\frac{i2\pi(\tau_i^{dm} - v)r}{\varphi(n^2)}} \\ &= \begin{cases} 1 & \textit{if } \mathrm{ord}_{n^2}(v) \mid \lambda(n), \\ 0 & \textit{if } \mathrm{ord}_{n^2}(v) \nmid \lambda(n). \end{cases} \end{aligned} \tag{12.17}$$

Proof. For each divisor $d \mid \lambda(n)$, this is a sum of $\xi(n) \geq 1$ copies of the indicator function proved in Lemma 12.11. ■

12.9 Problems

12.9.1 Indicator Functions Related Problems

Exercise 12.1. 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 12.2. Let $s \in \mathbb{Z}$ be a fixed integer, and let $p \geq 1$ be a prime. Evaluate the finite sum

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

.

Exercise 12.3. Let $p \geq 3$ be a prime. Show that the characteristic function of quadratic nonresidue in the finite ring $(\mathbb{Z}/p^2\mathbb{Z})^{\times}$ is

$$\Psi_{v^2}(p^2) = \sum_{\substack{1 \leq n < \varphi(p^2) \\ \gcd(2,n)=1}} \frac{1}{\varphi(p^2)} \sum_{0 \leq m < \varphi(p^2)} e^{\frac{i2\pi(\tau \frac{p(p-1)}{2} n - v)m}{\varphi(p^2)}} = \begin{cases} 1 & \text{if } \operatorname{ord}_{p^2}(v) = 2, \\ 0 & \text{if } \operatorname{ord}_{p^2}(v) \neq 2. \end{cases}$$

Exercise 12.4. Let $p = 3a+1 \geq 7$ be a prime. Show that the characteristic function of cubic nonresidue in the finite ring $(\mathbb{Z}/p^2\mathbb{Z})^{\times}$ is

$$\Psi_{v^3}(p^2) = \sum_{\substack{1 \leq n < \varphi(p^2) \\ \gcd(3,n)=1}} \frac{1}{\varphi(p^2)} \sum_{0 \leq m < \varphi(p^2)} e^{\frac{i2\pi(\tau \frac{p(p-1)}{3} n - v)m}{\varphi(p^2)}} = \begin{cases} 1 & \text{if } \operatorname{ord}_{p^2}(v) = 3, \\ 0 & \text{if } \operatorname{ord}_{p^2}(v) \neq 3. \end{cases}$$

12.9.2 Square Integers Indicator Functions Problems

Exercise 12.5. Let $[\cdot] : \mathbb{R} \longrightarrow \mathbb{Z}$ be the largest integer function defined by $[x] = x - \{x\}$. If $n \geq 1$ is an integer, then the expression

$$\varrho(n) = \left[\sqrt{n}\right] - \left[\sqrt{n-1}\right] = \begin{cases} 1 & \text{if } n = m^2 \text{ is a square,} \\ 0 & \text{if } n \neq m^2 \text{ is not a square,} \end{cases}$$

defines a square integer indicator function.

Exercise 12.6. Let $\lambda : \mathbb{N} \longrightarrow \{-1, 1\}$ be the Louiville function. If $n \geq 1$ is an integer, then the expression

$$\varrho(n) = \sum_{d|n} \lambda(n) = \begin{cases} 1 & \text{if } n = m^2 \text{ is a square,} \\ 0 & \text{if } n \neq m^2 \text{ is not a square,} \end{cases}$$

defines a square integer indicator function.

12.9.3 Integers Powers Indicator Functions Problems

Exercise 12.7. Let $[\cdot] : \mathbb{R} \longrightarrow \mathbb{Z}$ be the largest integer function defined by $[x] = x - \{x\}$. If $k \geq 2$ is a fixed integer, and $n \geq 1$ is an integer, then the expression

$$\varrho_k(n) = \left[\sqrt[k]{n}\right] - \left[\sqrt[k]{n-1}\right] = \begin{cases} 1 & \text{if } n = m^k \text{ is a } k \text{ power,} \\ 0 & \text{if } n \neq m^k \text{ is not a } k \text{ power,} \end{cases}$$

defines an integer k power indicator function.

Chapter 13

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 13.2, and to show that

$$\sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} = \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} + E(p), \tag{13.1}$$

where $E(p)$ is an error term, this is proved in Lemma 13.1. These are indirectly implied by the equidistribution of the subsets

$$\{\tau^n : \gcd(n, p-1) = 1\} = \{b\tau^n : \gcd(n, p-1) = 1\} \subset \mathbb{F}_p, \tag{13.2}$$

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

13.1 Incomplete And Complete Exponential Sums

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

$$\hat{f}(t) = \frac{1}{q} \sum_{0 \leq s \leq q-1} e^{i\pi st/q} \tag{13.3}$$

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

Definition 13.1. Let p and q be primes, and let $\omega = e^{i2\pi/q}$, and $\zeta = e^{i2\pi/p}$ be roots of unity. The *finite summation kernel* is defined by the finite Fourier transform identity

$$\mathcal{K}(f(n)) = \frac{1}{q} \sum_{0 \leq t \leq q-1,\, 0 \leq s \leq p-1} \omega^{t(n-s)} f(s) = f(n). \tag{13.4}$$

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

$$\sum_{n \leq x} f(n) = \sum_{n \leq x} \mathcal{K}(f(n)), \tag{13.5}$$

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

Theorem 13.1. ([108], [83]) *Let $p \geq 2$ be a large prime, and let $\tau \in \mathbb{F}_p$ be an element of large multiplicative order $\mathrm{ord}_p(\tau) \mid p-1$. Then, for any $b \in [1, p-1]$, and $x \leq p-1$,*

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

Proof. Let $q = p + o(p)$ be a large prime, and let $f(n) = e^{i2\pi b\tau^n/p}$, where τ is a primitive root modulo p. Applying the finite summation kernel in Definition 13.1, yields

$$\sum_{n \leq x} e^{i2\pi b\tau^n/p} = \sum_{n \leq x} \frac{1}{q} \sum_{0 \leq t \leq q-1,\ 1 \leq s \leq p-1} \omega^{t(n-s)} e^{i2\pi b\tau^s/p}. \tag{13.6}$$

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

$$\begin{aligned} \sum_{n \leq x} e^{i2\pi b\tau^n/p} &= \frac{1}{q} \sum_{n \leq x,\ 1 \leq t \leq q-1,\ 1 \leq s \leq p-1} \omega^{t(n-s)} e^{i2\pi b\tau^s/p} - \frac{x}{q} \\ &= \frac{1}{q} \sum_{1 \leq t \leq q-1} \left(\sum_{1 \leq s \leq p-1} \omega^{-ts} e^{i2\pi b\tau^s/p} \right) \left(\sum_{n \leq x} \omega^{tn} \right) - \frac{x}{q}. \end{aligned} \tag{13.7}$$

Taking absolute value, and applying Lemma 13.2, and Lemma 13.4, yield

$$\begin{aligned} \left| \sum_{n \leq x} e^{i2\pi b\tau^n/p} \right| &\leq \frac{1}{q} \sum_{1 \leq t \leq q-1} \left| \sum_{0 \leq s \leq p-1} \omega^{-ts} e^{i2\pi b\tau^s/p} \right| \cdot \left| \sum_{n \leq x} \omega^{tn} \right| + \frac{x}{q} \\ &\ll \frac{1}{q} \sum_{1 \leq t \leq q-1} \left(2q^{1/2} \log q \right) \cdot \left(\frac{2q}{\pi t} \right) + \frac{x}{q} \\ &\ll p^{1/2} \log^2 p. \end{aligned} \tag{13.8}$$

The last summation in (13.8) uses the estimate

$$\sum_{1 \leq t \leq q-1} \frac{1}{t} \ll \log q \ll \log p \tag{13.9}$$

since $q = p + o(p)$, and $x/q \leq 1$. ∎

This appears to be the best possible upper bound. The above proof generalizes the sum of resolvents method used in [83]. Here, it is reformulated as a finite Fourier transform method, which is applicable to a wide range of functions. A similar upper bound for composite moduli $p = m$ is also proved, [op. cit., equation (2.29)].

Theorem 13.2. *Let $p \geq 2$ be a large prime, and let τ be a primitive root modulo p. Then,*

$$\sum_{\gcd(n, p-1)=1} e^{i2\pi b\tau^n/p} \ll p^{1-\varepsilon} \tag{13.10}$$

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

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

$$\sum_{\gcd(n,p-1)=1} e^{\frac{i2\pi b\tau^n}{p}} = \sum_{\gcd(n,p-1)=1} \frac{1}{q} \sum_{0\le t\le q-1,} \sum_{1\le s\le p-1} \omega^{t(n-s)} e^{\frac{i2\pi b\tau^s}{p}}, \tag{13.11}$$

see Definition 13.1. Use the inclusion exclusion principle to rewrite the exponential sum as

$$\sum_{\gcd(n,p-1)=1} e^{\frac{i2\pi b\tau^n}{p}} = \sum_{n\le p-1} \frac{1}{q} \sum_{0\le t\le q-1,} \sum_{1\le s\le p-1} \omega^{t(n-s)} e^{\frac{i2\pi b\tau^s}{p}} \sum_{\substack{d|p-1\\ d|n}} \mu(d). \tag{13.12}$$

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

$$\begin{aligned} &\sum_{\gcd(n,p-1)=1} e^{\frac{i2\pi b\tau^n}{p}} \qquad (13.13)\\ &= \sum_{n\le p-1} \frac{1}{q} \sum_{1\le t\le q-1,} \sum_{1\le s\le p-1} \omega^{t(n-s)} e^{\frac{i2\pi b\tau^s}{p}} \sum_{\substack{d|p-1\\ d|n}} \mu(d) - \frac{\varphi(p)}{q}\\ &= \frac{1}{q} \sum_{1\le t\le q-1} \left(\sum_{1\le s\le p-1} \omega^{-ts} e^{\frac{i2\pi b\tau^s}{p}} \right) \left(\sum_{d|p-1} \mu(d) \sum_{\substack{n\le p-1,\\ d|n}} \omega^{tn} \right) - \frac{\varphi(p)}{q}. \end{aligned}$$

Taking absolute value, and applying Lemma 13.3, and Lemma 13.4, yield

$$\begin{aligned} &\left| \sum_{\gcd(n,p-1)=1} e^{\frac{i2\pi b\tau^n}{p}} \right| \qquad (13.14)\\ &\le \frac{1}{q} \sum_{1\le t\le q-1} \left| \sum_{1\le s\le p-1} \omega^{-ts} e^{i2\pi b\tau^s/p} \right| \cdot \left| \sum_{d|p-1} \mu(d) \sum_{\substack{n\le p-1,\\ d|n}} \omega^{tn} \right| + \frac{\varphi(p)}{q}\\ &\ll \frac{1}{q} \sum_{1\le t\le q-1} \left(2q^{1/2}\log q\right) \cdot \left(\frac{4q\log\log p}{\pi t} \right) + \frac{\varphi(p)}{q}\\ &\ll p^{1/2}\log^3 p. \end{aligned}$$

The last summation in (13.14) uses the estimate

$$\sum_{1\le t\le q-1} \frac{1}{t} \ll \log q \ll \log p \tag{13.15}$$

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

The upper bound given in Theorem 13.1 seems to be optimum. A different proof, which has a weaker upper bound, appears in [44, Theorem 6], and related results are given in [10], [43], [50], and [51, Theorem 1].

13.2 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

$$\{\tau^n : \gcd(n, p-1) = 1\} \quad \text{and} \quad \{b\tau^n : \gcd(n, p-1) = 1\} \subset \mathbb{F}_p \tag{13.16}$$

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

$$\sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} \quad \text{and} \quad \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p}, \tag{13.17}$$

have the same upper bound up to an error term. An asymptotic relation for the exponential sums (13.17) is provided in Lemma 13.1. This result expresses the first exponential sum in (13.17) as a sum of simpler exponential sum and an error term.

Lemma 13.1. *Let $p \geq 2$ be a large primes. If τ be a primitive root modulo p, then,*

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

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

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

$$\begin{aligned} &\sum_{\gcd(n,p-1)=1} e^{\frac{i2\pi b\tau^n}{p}} \qquad (13.18)\\ &= \frac{1}{q}\sum_{1\leq t\leq q-1}\left(\sum_{1\leq s\leq p-1}\omega^{-ts}e^{\frac{i2\pi b\tau^s}{p}}\right)\left(\sum_{d|p-1}\mu(d)\sum_{\substack{n\leq p-1,\\ d|n}}\omega^{tn}\right) - \frac{\varphi(p)}{q}, \end{aligned}$$

confer equation (13.13) for details. And, for $b = 1$,

$$\begin{aligned} &\sum_{\gcd(n,p-1)=1} e^{\frac{i2\pi\tau^n}{p}} \qquad (13.19)\\ &= \frac{1}{q}\sum_{1\leq t\leq q-1}\left(\sum_{1\leq s\leq p-1}\omega^{-ts}e^{\frac{i2\pi\tau^s}{p}}\right)\left(\sum_{d|p-1}\mu(d)\sum_{\substack{n\leq p-1,\\ d|n}}\omega^{tn}\right) - \frac{\varphi(p)}{q}, \end{aligned}$$

respectively, see (13.13). Differencing (13.18) and (13.19) produces

$$\begin{aligned} &\sum_{\gcd(n,p-1)=1} e^{i2\pi b\tau^n/p} - \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} \qquad (13.20)\\ &= \frac{1}{q}\sum_{0\leq t\leq q-1}\left(\sum_{1\leq s\leq p-1}\omega^{-ts}e^{\frac{i2\pi b\tau^s}{p}} - \sum_{1\leq s\leq p-1}\omega^{-ts}e^{\frac{i2\pi\tau^s}{p}}\right)\\ &\quad\times\left(\sum_{d|p-1}\mu(d)\sum_{\substack{n\leq p-1,\\ d|n}}\omega^{tn}\right). \end{aligned}$$

By Lemma 13.3, the relatively prime summation kernel is bounded by

$$\begin{aligned}\left|\sum_{d|p-1}\mu(d)\sum_{\substack{n\le p-1,\\ d|n}}\omega^{tn}\right| &= \left|\sum_{\gcd(n,p-1)=1}\omega^{tn}\right| \\ &\le \frac{4q\log\log p}{\pi t}, \end{aligned} \tag{13.21}$$

and by Lemma 13.4, the difference of two Gauss sums is bounded by

$$\begin{aligned}&\left|\sum_{1\le s\le p-1}\omega^{-ts}e^{\frac{i2\pi b\tau^s}{p}}-\sum_{1\le s\le p-1}\omega^{-ts}e^{\frac{i2\pi\tau^s}{p}}\right| \\ =\ &\left|\sum_{1\le s\le p-1}\chi(s)\psi_b(s)-\sum_{1\le s\le p-1}\chi(s)\psi_1(s)\right| \\ \le\ & 4p^{1/2}\log p, \end{aligned} \tag{13.22}$$

where $\chi(s)=e^{i\pi st/p}$, and $\psi_b(s)=e^{i2\pi b\tau^s/p}$. Taking absolute value in (13.20) and replacing (13.21), and (13.22), return

$$\begin{aligned}&\left|\sum_{\gcd(n,p-1)=1}e^{i2\pi b\tau^n/p}-\sum_{\gcd(n,p-1)=1}e^{i2\pi\tau^n/p}\right| \\ \le\ & \frac{1}{q}\sum_{0\le t\le q-1}\left(4q^{1/2}\log q\right)\cdot\left(\frac{4q\log\log p}{t}\right) \\ \le\ & 16q^{1/2}(\log q)(\log q)(\log\log p) \\ \le\ & 16p^{1/2}\log^3 p, \end{aligned} \tag{13.23}$$

where $q=p+o(p)$. ■

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

$$\sum_{n\in\mathcal{A}}e^{i2\pi b\tau^n/p}=\sum_{n\in\mathcal{A}}e^{i2\pi\tau^n/p}+O(p^{1/2}\log^c p), \tag{13.24}$$

for some constant $c>0$.

13.3 Finite Summation Kernels And Gaussian Sums

Lemma 13.2. *Let $p\ge 2$ and $q=p+o(p)>p$ be large primes. Let $\omega=e^{i2\pi/q}$ be a qth root of unity, and let $t\in[1,p-1]$. Then,*

(i) $$\sum_{n\le p-1}\omega^{tn}=\frac{\omega^t-\omega^{tp}}{1-\omega^t},$$

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

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

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

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

$$\left|\frac{\omega^t - \omega^{tp}}{1-\omega^t}\right| \leq \left|\frac{2}{\sin(\pi t/q)}\right| \leq \frac{2q}{\pi t}. \tag{13.25}$$

■

Lemma 13.3. *Let $p \geq 2$ and $q = p + o(p) > p$ be large primes, and let $\omega = e^{i2\pi/q}$ be a qth root of unity. Then,*

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

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

where $\mu(k)$ is the Mobius function, for any fixed pair $d \mid p-1$ and $t \in [1, p-1]$.

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

$$\begin{aligned}
\sum_{\gcd(n,p-1)=1} \omega^{tn} &= \sum_{n\leq p-1} \omega^{tn} \sum_{\substack{d|p-1\\ d|n}} \mu(d) \\
&= \sum_{d|p-1} \mu(d) \sum_{\substack{n\leq p-1\\ d|n}} \omega^{tn} \\
&= \sum_{d|p-1} \mu(d) \sum_{m\leq (p-1)/d} \omega^{dtm} \\
&= \sum_{d|p-1} \mu(d) \frac{\omega^{dt} - \omega^{dt((p-1)/d+1)}}{1-\omega^{dt}}.
\end{aligned} \tag{13.26}$$

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

$$\left|\frac{\omega^{dt} - \omega^{dtp}}{1-\omega^{dt}}\right| \leq \left|\frac{2}{\sin(\pi dt/q)}\right| \leq \frac{2q}{\pi dt} \tag{13.27}$$

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

$$\begin{aligned} \left| \sum_{d|p-1} \mu(d) \frac{\omega^{dt} - \omega^{dt((p-1)/d+1)}}{1-\omega^{dt}} \right| &\leq \frac{2q}{\pi t} \sum_{d|p-1} \frac{1}{d} \\ &\leq \frac{4q \log\log p}{\pi t}. \end{aligned} \tag{13.28}$$

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

Lemma 13.4. (Gauss sums) *Let $p \geq 2$ and q be large primes. Let $\chi(t) = e^{i2\pi t/q}$ and $\psi(t) = e^{i2\pi\tau^t/p}$ be a pair of characters. Then, the Gaussian sum has the upper bound*

$$\left| \sum_{1 \leq t \leq q-1} \chi(t)\psi(t) \right| \leq 2q^{1/2} \log q. \tag{13.29}$$

.

Chapter 14

Asymptotic Formulas For The Main Terms

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

Lemma 14.1. *Let $p \geq 2$ be a large prime, let $k \ll \log p$, and let φ be the totient function. Then,*

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

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

$$\begin{aligned} M(k,p) &= \sum_{n \in \mathbb{F}_p} \prod_{0 \leq i \leq k} \left(\frac{1}{p} \sum_{\gcd(n_i, p-1)=1} 1 \right) \\ &= \left(\frac{\varphi(p-1)}{p} \right)^{k+1} \sum_{n \in \mathbb{F}_p} 1 \qquad (14.1) \\ &= \left(\frac{\varphi(p-1)}{p} \right)^{k+1} p. \end{aligned}$$

Last, but not least use the readjustment

$$\frac{\varphi(p-1)}{p} = \frac{\varphi(p-1)}{p-1} \left(1 - \frac{1}{p} \right) \qquad (14.2)$$

to obtain the standard form of the main term. ∎

14.2 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 7.1.

Lemma 14.2. *Let $p \geq 2$ be a large prime, let $k \ll \log p$, and let φ be the totient function. Then,*

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

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,

$$\begin{aligned} M(k,p) &= \sum_{n\in\mathbb{F}_p}\left(\frac{\mu(n+a_0)^2}{p}\sum_{\gcd(n_0,p-1)=1}1\cdots\frac{\mu(n+a_k)^2}{p}\sum_{\gcd(n_k,p-1)=1}1\right)\\ &= \left(\frac{\varphi(p-1)}{p}\right)^{k+1}\sum_{n\in\mathbb{F}_p}\mu(n+a_0)^2\cdots\mu(n+a_k)^2 \qquad (14.3)\\ &= \prod_{q\geq 2}\left(1-\frac{\omega(q)}{q^2}\right)\left(\frac{\varphi(p-1)}{p-1}\right)^{k+1}p+O\left(x^{2/3+\varepsilon}\right). \end{aligned}$$

The last line follows from Theorem 7.3 applied to the correlation function, and $\varepsilon > 0$ is an arbitrarily small number. Now, use the readjustment

$$\frac{\varphi(p-1)}{p}=\frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \qquad (14.4)$$

to obtain the standard form of the main term. ■

14.3 Main Term For Squarefree Twin Primitive Roots

Lemma 14.3. *Let $p \geq 2$ be a large prime, let φ be the totient function, and let μ be the Mobius function. Then,*

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

Proof. Rearrange it and simplify it as

$$\begin{aligned} M_2(2,p) &= \sum_{n\in\mathbb{F}_p}\left(\frac{\mu^2(n)}{p}\sum_{\gcd(n_0,p-1)=1}1\right)\left(\frac{\mu^2(n+1)}{p}\sum_{\gcd(n_1,p-1)=1}1\right) \\ &= \left(\frac{\varphi(p-1)}{p}\right)^2\sum_{n\in\mathbb{F}_p}\mu^2(n)\mu^2(n+1) \qquad (14.5) \\ &= \left(\frac{\varphi(p-1)}{p}\right)^2\left(\prod_{q\geq 2}\left(1-\frac{2}{q^2}\right)p+O\left(p^{2/3}\right)\right) \end{aligned}$$

The last line follows from Lemma 7.4 or Theorem 7.3 applied to the correlation function. Lastly, use the readjustment

$$\frac{\varphi(p-1)}{p}=\frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \qquad (14.6)$$

to obtain the standard form of the main term. ■

14.4 Main Term For Squarefree Triple Primitive Roots

Lemma 14.4. *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*

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

Proof. Rearrange it and simplify it as

$$\begin{aligned} M_2(3,p) &= \sum_{n\in\mathbb{F}_p}\left(\frac{\mu^2(n)}{p}\sum_{\gcd(n_0,p-1)=1}1\right)\left(\frac{\mu^2(n+1)}{p}\sum_{\gcd(n_1,p-1)=1}1\right) \\ &\quad\times\left(\frac{\mu^2(n+2)}{p}\sum_{\gcd(n_2,p-1)=1}1\right) \\ &= \left(\frac{\varphi(p-1)}{p}\right)^3\sum_{n\in\mathbb{F}_p}\mu^2(n)\mu^2(n+1)\mu^2(n+2) \qquad (14.7) \\ &= \left(\frac{\varphi(p-1)}{p}\right)^3\left(\prod_{q\geq 2}\left(1-\frac{3}{q^2}\right)p+O\left(p^{2/3}\right)\right) \end{aligned}$$

The last line follows from Lemma 7.5 or Theorem 7.3 applied to the correlation function. Lastly, use the readjustment

$$\frac{\varphi(p-1)}{p} = \frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \tag{14.8}$$

to obtain the standard form of the main term. ■

14.5 Main Term For s-Power Free Primitive Roots

Lemma 14.5. *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,*

$$\sum_{n\in\mathbb{F}_p} \frac{\mu_s(n)}{p} \sum_{\gcd(m,p-1)=1} 1 = \frac{1}{\zeta(s)}\frac{\varphi(p-1)}{p-1}p + O\left(p^{1/s}\right). \tag{14.9}$$

Proof. Simplify the double sum:

$$\frac{1}{p}\sum_{n\in\mathbb{F}_p}\mu_s(n) \sum_{\gcd(m,p-1)=1} 1 = \frac{\varphi(p-1)}{p}\sum_{n\in\mathbb{F}_p}\mu_s(n). \tag{14.10}$$

Replace the characteristic function for s-power free integers, see Lemma 3.4, and reverse the order of summation:

$$\begin{aligned}
\frac{\varphi(p-1)}{p}\sum_{n\in\mathbb{F}_p}\mu_s(n) &= \frac{\varphi(p-1)}{p}\sum_{n\in\mathbb{F}_p}\sum_{d^s|n}\mu(d) \\
&= \frac{\varphi(p-1)}{p}\sum_{d\leq p^{1/s}}\mu(d)\sum_{\substack{n\in\mathbb{F}_p \\ d^s|n}} 1 \\
&= \frac{\varphi(p-1)}{p}\sum_{d\leq p^{1/s}}\mu(d)\left(\frac{p}{d^s}+O(1)\right) \\
&= \frac{1}{\zeta(s)}\frac{\varphi(p-1)}{p}p + O\left(p^{1/s}\right),
\end{aligned} \tag{14.11}$$

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

$$\frac{\varphi(p-1)}{p} = \frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \tag{14.12}$$

to obtain the standard form of the main term. ■

14.6 Main Term For s-Power Free Twin Primitive Roots

Lemma 14.6. *Let $p \geq 2$ be a large prime, let $a_0 \neq a_1$ and $s \geq 2$ be small integers. Let μ_s be the s-power free characteristic function. Then,*

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

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

Proof. Rearrange it and simplify it as

$$\begin{aligned}M_2(2,p) &= \sum_{n\in\mathbb{F}_p}\left(\frac{\mu_s(n)}{p}\sum_{\gcd(n_0,p-1)=1}1\right)\left(\frac{\mu_s(n+a)}{p}\sum_{\gcd(n_1,p-1)=1}1\right)\\ &= \left(\frac{\varphi(p-1)}{p}\right)^2\sum_{n\in\mathbb{F}_p}\mu_s(n)\mu_s(n+a) \qquad (14.13)\\ &= \left(\frac{\varphi(p-1)}{p}\right)^2\left(\prod_{q\geq 2}\left(1-\frac{\rho(s)}{q^s}\right)p+O\left(p^{\alpha(s)+\varepsilon}\right)\right)\end{aligned}$$

The last line follows from Theorem 7.4 applied to the correlation function. Lastly, use the readjustment

$$\frac{\varphi(p-1)}{p}=\frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \qquad (14.14)$$

to obtain the standard form of the main term. ■

14.7 Main Term For Relatively Prime Primitive Roots

Lemma 14.7. *Let $p \geq 2$ be a large prime, and let $q \leq p-1$ be a fixed integer. Then,*

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

Proof. Simplify the double sum:

$$\begin{aligned}M_r(p,q) &= \frac{1}{p}\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1}}\sum_{\gcd(m,p-1)=1}1 \qquad (14.15)\\ &= \frac{\varphi(p-1)}{p}\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1}}1.\end{aligned}$$

Replace the characteristic function for relatively prime numbers, see Definition 3.6, and rearrange the order of summation:

$$\begin{aligned}\frac{\varphi(p-1)}{p}\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1}}1 &= \frac{\varphi(p-1)}{p}\sum_{n\in\mathbb{F}_p}\sum_{\substack{d|n\\ d|q}}\mu(d)\\ &= \frac{\varphi(p-1)}{p}\sum_{d|q}\mu(d)\sum_{\substack{n\in\mathbb{F}_p\\ d|n}}1\\ &= p\frac{\varphi(p-1)}{p}\sum_{d|q}\frac{\mu(d)}{d}\\ &= \frac{\varphi(q)}{q}\frac{\varphi(p-1)}{p-1}p,\end{aligned} \tag{14.16}$$

where $\varphi(n)/n=\sum_{d|n}\mu(d)/d$, see Section 4.9. Lastly, use the readjustment

$$\frac{\varphi(p-1)}{p}=\frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \tag{14.17}$$

to obtain the standard form of the main term. ■

14.8 Main Term For Relatively Prime Twin Primitive Roots

The identity $\varphi(n)=\sum_{\gcd(d,n)=1}1$, and the estimate $\sum_{d|q}|\mu(d)|=O\left(q^{\delta}\right)$ for $\delta>0$ is a small number, see Section 3.1, are used within the proofs.

Lemma 14.8. *If $p\geq 2$ is a large prime, let $a\geq 1$ and $q\leq p-1$ be a pair of fixed integers. Then,*

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

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

Proof. Simplify the double sum:

$$\frac{1}{p}\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1\\ \gcd(n+a,q)=1}}\sum_{\gcd(m,p-1)=1}1=\frac{\varphi(p-1)}{p}\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1\\ \gcd(n+a,q)=1}}1. \tag{14.18}$$

Replace the characteristic function for relatively prime numbers, see Definition 3.6,

and rearrange the order of summation:

$$\begin{aligned}\frac{\varphi(p-1)}{p}\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1\\ \gcd(n+a,q)=1}} 1 &= \frac{\varphi(p-1)}{p}\sum_{n\in\mathbb{F}_p}\sum_{\substack{d\mid n\\ d\mid q}}\mu(d)\sum_{\substack{e\mid n+a\\ e\mid q}}\mu(e) \\ &= \frac{\varphi(p-1)}{p}\sum_{d\mid q}\mu(d)\sum_{e\mid q}\mu(e)\sum_{\substack{n\in\mathbb{F}_p\\ d\mid n\\ e\mid n+1}} 1 \\ &= \frac{\varphi(p-1)}{p}\sum_{d\mid q}\mu(d)\sum_{e\mid q}\mu(e)\left(c_2(q,a)\frac{p}{de}+O(1)\right),\end{aligned} \tag{14.19}$$

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

$$\begin{aligned}&\frac{\varphi(p-1)}{p}\sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1\,\gcd(n+a,q)=1}} 1 \\ &= c_2(q,a)p\frac{\varphi(p-1)}{p}\sum_{d\mid q}\frac{\mu(d)}{d}\sum_{e\mid q}\frac{\mu(e)}{e}+O\left(\sum_{d\mid q}|\mu(d)|\sum_{e\mid q}|\mu(e)|\right) \\ &= c_2(q,a)\left(\frac{\varphi(q)}{q}\right)^2\frac{\varphi(p-1)}{p}p+O\left(q^{2\delta}\right),\end{aligned} \tag{14.20}$$

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

$$\frac{\varphi(p-1)}{p}=\frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \tag{14.21}$$

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 (14.19). It simply includes a dependence correction constant $c_2(q)>0$.

14.9 Main Term For Squarefree And Relatively Prime Primitive Roots

Lemma 14.9. *Let $p\geq 2$ be a large prime, and let $q=O(\log p)$ be a fixed integer. Then,*

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

Proof. Simplify the double sum:

$$\begin{aligned} M_r(p,q) &= \frac{1}{p} \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1}} \sum_{\gcd(m,p-1)=1} \mu(n)^2 \\ &= \frac{\varphi(p-1)}{p} \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1}} \mu(n)^2. \end{aligned} \tag{14.22}$$

Apply Lemma 7.3 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

$$\frac{\varphi(p-1)}{p} = \frac{\varphi(p-1)}{p-1} \left(1 - \frac{1}{p}\right) \tag{14.23}$$

to obtain the standard form of the main term. ■

14.10 Main Term For Squarefree And Relatively Prime Twin Primitive Roots

Lemma 14.10. *Assume conjecture* 7.1. *If $p \geq 2$ is a large prime, let $a \geq 1$ and $q \leq p-1$ be a pair of fixed integers. Then,*

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

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

Proof. Simplify the double sum:

$$\frac{1}{p^2} \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1 \\ \gcd(n+a,q)=1}} \sum_{\substack{\gcd(m_0,p-1)=1 \\ \gcd(m_1,p-1)=1}} \mu(n)^2 \mu(n+a)^2 = \left(\frac{\varphi(p-1)}{p}\right)^2 \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1 \\ \gcd(n+a,q)=1}} \mu(n)^2 \mu(n+a)^2. \tag{14.24}$$

Set $x = p$, and apply Conjecture 7.1 to the inner finite sum:

$$\begin{aligned} M_{sr}(2,p,q) &= \left(\frac{\varphi(p-1)}{p}\right)^2 \sum_{\substack{n\in\mathbb{F}_p \\ \gcd(n,q)=1 \\ \gcd(n+a,q)=1}} \mu(n)^2\mu(n+a)^2 \qquad (14.25) \\ &= \left(\frac{\varphi(p-1)}{p}\right)^2 \left(c_2(q,a)\prod_{p\nmid q}\left(1+\frac{1}{p}\right)^{-2}\prod_{p\geq 2}\left(1-\frac{2}{p^2}\right)p + O\left(p^{1-\delta}\right)\right) \\ &= c_2(q,a)\prod_{p\nmid q}\left(1+\frac{1}{p}\right)^{-2}\prod_{p\geq 2}\left(1-\frac{2}{p^2}\right)\left(\frac{\varphi(p-1)}{p}\right)^2 p + O\left(p^{1-\delta}\right), \end{aligned}$$

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

$$\frac{\varphi(p-1)}{p} = \frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \qquad (14.26)$$

to obtain the standard form of the main term. ■

14.11 Main Term For Smooth Primitive Roots

Lemma 14.11. *Let $p \geq 2$ be a large prime, let $B = p^{1/u}$ be a parameter, with $u > 0$, and let α_B be the characteristic function of B-smooth integers. Then,*

$$\sum_{n\in\mathbb{F}_p}\frac{\alpha_B(n)}{p}\sum_{\gcd(m,p-1)=1} 1 = \rho(u)\frac{\varphi(p-1)}{p-1}p + O\left(\rho(u-1)\frac{p}{\log p}\right).$$

Proof. Simplify the double sum:

$$\sum_{n\in\mathbb{F}_p}\frac{\alpha_B(n)}{p}\sum_{\gcd(m,p-1)=1} 1 = \frac{\varphi(p-1)}{p}\sum_{n\in\mathbb{F}_p}\alpha_B(n). \qquad (14.27)$$

Applying Theorem 8.1 yields

$$\begin{aligned} \frac{\varphi(p-1)}{p}\sum_{n\in\mathbb{F}_p}\alpha_B(n) &= \frac{\varphi(p-1)}{p}\left(\rho(u)p + O\left(\rho(u-1)\frac{p}{\log p}\right)\right) \qquad (14.28) \\ &= \rho(u)\frac{\varphi(p-1)}{p}p + O\left(\rho(u-1)\frac{p}{\log p}\right). \end{aligned}$$

The density $\rho(u)$ is specified in (8.2). Lastly, use the readjustment

$$\frac{\varphi(p-1)}{p} = \frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \qquad (14.29)$$

to obtain the standard form of the main term. ■

14.12 Main Term For B-Smooth Twin Primitive Roots

Lemma 14.12. *Let $p \geq 2$ be a large prime, let $B = p^{1/u}$ be a parameter, with $u > 0$, and let α_B be the characteristic function of B-smooth integers. Then,*

$$\begin{aligned} & \sum_{n \in \mathbb{F}_p} \left(\frac{\alpha_B(n)}{p} \sum_{\gcd(n_0, p-1)=1} 1 \right) \left(\frac{\alpha_B(n+1)}{p} \sum_{\gcd(n_1, p-1)=1} 1 \right) \\ = \; & a_2(u) \rho(u)^2 \left(\frac{\varphi(p-1)}{p-1} \right)^2 p + O\left(\frac{t(u)p}{\log p} \right), \end{aligned}$$

where $\rho(u) > 0$ is the density, and $s_2(u) > 0$ is a dependence correction factor.

Proof. Rearrange it and simplify it as

$$\begin{aligned} M_2(u,p) &= \sum_{n \in \mathbb{F}_p} \left(\frac{\alpha_B(n)}{p} \sum_{\gcd(n_0, p-1)=1} 1 \right) \left(\frac{\alpha_B(n+1)}{p} \sum_{\gcd(n_1, p-1)=1} 1 \right) \\ &= \left(\frac{\varphi(p-1)}{p} \right)^2 \sum_{n \in \mathbb{F}_p} \alpha_B(n) \alpha_B(n+1) \qquad (14.30) \\ &= \left(\frac{\varphi(p-1)}{p} \right)^2 \left(a_2(u) \rho(u)^2 p + O\left(\frac{t(u)p}{\log p} \right) \right) \end{aligned}$$

The last line follows from Theorem 8.5 applied to the correlation function. Lastly, use the readjustment

$$\frac{\varphi(p-1)}{p} = \frac{\varphi(p-1)}{p-1} \left(1 - \frac{1}{p} \right) \qquad (14.31)$$

to obtain the standard form of the main term. ■

14.13 Main Term For Prime Primitive Roots

Lemma 14.13. *Let $p \geq 2$ be a large prime, and let $\Lambda(n)/\log n$ be the characteristic function of prime power integers. Then,*

$$\sum_{n \in \mathbb{F}_p} \frac{1}{p} \frac{\Lambda(n)}{\log n} \sum_{\gcd(m, p-1)=1} 1 = \frac{\varphi(p-1)}{p-1} \frac{p}{\log p} + O\left(\frac{p}{\log^2 p} \right).$$

Proof. Simplify the double sum:

$$\sum_{n \in \mathbb{F}_p} \frac{1}{p} \frac{\Lambda(n)}{\log n} \sum_{\gcd(m, p-1)=1} 1 = \frac{\varphi(p-1)}{p} \sum_{n \in \mathbb{F}_p} \frac{\Lambda(n)}{\log n}. \qquad (14.32)$$

Applying the Prime Number Theorem 9.3 yields

$$\frac{\varphi(p-1)}{p} \sum_{n \in \mathbb{F}_p} \frac{\Lambda(n)}{\log n} = \frac{\varphi(p-1)}{p} \left(\frac{p}{\log p} + O\left(\frac{p}{\log^2 p} \right) \right).$$

Lastly, use the readjustment

$$\frac{\varphi(p-1)}{p} = \frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \tag{14.33}$$

to obtain the standard form of the main term. ■

14.14 Main Term For Twin Primes Primitive Roots

Lemma 14.14. *Assume Conjecture* 9.3. *If $p \geq 2$ is a large prime, then,*

$$\begin{aligned} & \sum_{n\in\mathbb{F}_p}\left(\frac{1}{p}\frac{\Lambda(n)}{\log n}\sum_{\gcd(n_0,p-1)=1}1\right)\left(\frac{1}{p}\frac{\Lambda(n+2)}{\log(n+2)}\sum_{\gcd(n_1,p-1)=1}1\right) \\ = \; & \mathfrak{G}(2)\left(\frac{\varphi(p-1)}{p-1}\right)^2\frac{p}{\log^2 p}+O\left(\frac{p}{\log^3 p}\right). \end{aligned}$$

Proof. Rearrange it and simplify it as

$$\begin{aligned} M_0(u,p) &= \sum_{n\in\mathbb{F}_p}\left(\frac{1}{p}\frac{\Lambda(n)}{\log n}\sum_{\gcd(n_0,p-1)=1}1\right)\left(\frac{1}{p}\frac{\Lambda(n+2)}{\log(n+2)}\sum_{\gcd(n_1,p-1)=1}1\right) \\ &= \left(\frac{\varphi(p-1)}{p}\right)^2\sum_{n\in\mathbb{F}_p}\frac{\Lambda(n)}{\log(n)}\frac{\Lambda(n+2)}{\log(n+2)} \\ &= \mathfrak{G}(2)\left(\frac{\varphi(p-1)}{p}\right)^2\left(\frac{p}{\log^2 p}+O\left(\frac{p}{\log^3 p}\right)\right) \end{aligned} \tag{14.34}$$

The last line follows from Conjecture 9.3 applied to the correlation function. Lastly, use the readjustment

$$\frac{\varphi(p-1)}{p} = \frac{\varphi(p-1)}{p-1}\left(1-\frac{1}{p}\right) \tag{14.35}$$

to obtain the standard form of the main term. ■

Chapter 15

The Estimates Varius The Error Terms

The upper bounds for exponential sums over subsets of elements in finite fields $\mathbb{F}_p$ studied in Section 8.2 are used to estimate the error terms for the different configurations of consecutive primitive roots in Theorem 1.2 and the other results.

15.1 The Estimates For The Error Terms

Lemma 15.1. *Let $p \geq 2$ be a large prime, and let τ be a primitive root mod p. If the element $u \neq 0, \pm 1, v^2$ is not a primitive root, then,*

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

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

$$\begin{aligned} S_1 &= \sum_{u \in \mathbb{F}_p} \frac{1}{p} \sum_{\gcd(n,p-1)=1,\ 0<m\leq p-1} \sum e^{i2\pi((\tau^n-u)m)} \qquad (15.1) \\ &= \frac{1}{p} \sum_{u \in \mathbb{F}_p} \left(\sum_{0<m\leq p-1,} e^{-i2\pi um/p} \right) \left(\sum_{\gcd(n,p-1)=1} e^{i2\pi m\tau^n/p} \right) \\ &= \frac{1}{p} \sum_{u \in \mathbb{F}_p} \left(\sum_{0<m\leq p-1,} e^{-i2\pi um/p} \right) \left(\sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} + O(p^{1/2}\log^3 p) \right) \\ &= \frac{1}{p} \sum_{u \in \mathbb{F}_p} U_p \cdot V_p. \end{aligned}$$

The third line in equation (15.1) follows from Lemma 13.1. The first exponential

sum U_p has the exact evaluation

$$|U_p| = \left| \sum_{0<m\leq p-1} e^{-i2\pi um/p} \right| = 1, \tag{15.2}$$

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

$$\begin{aligned} |V_p| &= \left| \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} + O\left(p^{1/2}\log^3 p\right) \right| \\ &\ll \left| \sum_{\gcd(n,p-1)=1} e^{i2\pi\tau^n/p} \right| + p^{1/2}\log^3 p \\ &\ll p^{1-\varepsilon}, \end{aligned} \tag{15.3}$$

where $\varepsilon < 1/2$ is an arbitrarily small number, see Theorem 13.2. Taking absolute value in (15.1), and replacing the estimates (15.2) and (15.3) return

$$\begin{aligned} |S_1| &\leq \frac{1}{p}\sum_{u\in\mathbb{F}_p} |U_p|\cdot|V_p| \\ &\ll \frac{1}{p}\sum_{u\in\mathbb{F}_p} (1)\cdot p^{1-\varepsilon} \\ &\ll \frac{1}{p^{\varepsilon}}\sum_{u\in\mathbb{F}_p} 1 \\ &\ll p^{1-\varepsilon}. \end{aligned} \tag{15.4}$$

■

No effort was made to optimize the error term in Lemma 15.1. However, it should be noted that the best possible is $p^{1/2+\varepsilon}$, see Theorem 13.2.

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

Lemma 15.2. *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,*

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

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

$$|S_1| \ll p^{1-\varepsilon}, \tag{15.5}$$

see Lemma 15.1. The product of the remaining sums indexed by m_i and n_i, $i \in \{1, 2, \dots k-1\}$ have the trivial upper bound

$$\begin{aligned} |S_2| &\leq \left| \frac{1}{p} \sum_{\substack{\gcd(n_1, p-1)=1 \\ 0<m_1 \leq p-1}} e^{i2\pi((\tau^{n_1} - n - a_1)m_1)} \right| \dots \left| \frac{1}{p} \sum_{\substack{\gcd(n_k, p-1)=1 \\ 0<m_k \leq p-1}} e^{i2\pi((\tau^{n_k} - n - a_k)m_k)} \right| \\ &\leq \frac{\varphi(p-1)}{p} \dots \frac{\varphi(p-1)}{p} \\ &\leq \left(\frac{\varphi(p-1)}{p} \right)^k. \end{aligned} \tag{15.6}$$

Merging (15.5) and (15.6) returns

$$\begin{aligned} |E(p, \tau)| &\leq |S_1|\,|S_2| \\ &\leq \left(p^{1-\varepsilon}\right) \times \left(\frac{\varphi(p-1)}{p} \right)^k \\ &\leq p^{1-\varepsilon}. \end{aligned} \tag{15.7}$$

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

15.3 Error Term For s-Power Free Primitive Roots

Lemma 15.3. *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,*

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

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

Proof. Same as Lemma 15.1, mutatis mutandus. ■

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

Lemma 15.4. *Let $p \geq 2$ be a large prime, let $0 \leq a_0, a_1, a_2, \dots, a_k$ 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,

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

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

Proof. Same as Lemma 15.2, mutatis mutandus. ■

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

Lemma 15.5. *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,*

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

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 15.2, mutatis mutandus. ■

Chapter 16

Lengths Of Consecutive Primitive Roots

16.1 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 Section 10.3.

(2) The average primes $p \geq 2$. The average totients $p-1=\varphi(p)$ have the mean numbers of prime divisors, Section 2.1.

(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 10.5.

Lemma 16.1. *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

$$p\left(\frac{\varphi(p-1)}{p-1}\right)^{k+1} \gg p^{1-\varepsilon} \tag{16.1}$$

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

$$k \ll \frac{\varepsilon \log p}{\log\left(\frac{p-1}{\varphi(p-1)}\right)} \ll \frac{\varepsilon \log p}{\log \omega(p-1)}. \tag{16.2}$$

Substituting the estimates for the three different cases

1. $\dfrac{p-1}{\varphi(p-1)} \approx \log\log p,$
2. $\dfrac{p-1}{\varphi(p-1)} \approx \log\log\log p,$
3. $\dfrac{p-1}{\varphi(p-1)} \approx 2,$

respectively, complete the proof. ■

Definition 16.1. 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,[46].

Example 16.1. 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 16.1 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 16.2. 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 16.1: 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 16.2: 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

16.2 Problems

Exercise 16.1. 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 16.1.

Exercise 16.2. Compute a table of the length merit factor $m = k/\log p$ indexed by the primes $p \leq 1000$. .

Exercise 16.3. Compute a table of the length merit factor $m = k/\log p$ indexed by the length $k \leq 50$.

Chapter 17

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 [12] using a counting technique based on Lemma 12.2. A new proof and counting technique based on Lemma 12.3 is given here.

17.1 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

$$\tau^{n_0} = n + a_0, \quad \tau^{n_1} = n + a_1, \quad \tau^{n_2} = n + a_2, \quad \ldots, \quad \tau^{n_k} = n + a_k, \tag{17.1}$$

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

$$N(k,p) = \#\left\{n \in \mathbb{F}_p : \mathrm{ord}_p(n + a_i) = p - 1\right\} \tag{17.2}$$

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 12.3, as

$$\begin{aligned} N(k,p) &= \sum_{n \in \mathbb{F}_p} \Psi(n+a_0)\,\Psi(n+a_1)\cdots\Psi(n+a_k) \qquad (17.3)\\ &= \sum_{n \in \mathbb{F}_p} \prod_{0 \leq i \leq k} \left(\frac{1}{p} \sum_{\substack{\gcd(n_i, p-1)=1 \\ 0 \leq u_i \leq p-1}} \psi\left((\tau^{n_i} - n - a_i)u_i\right)\right) \\ &= M(k,p) + E(k,p). \end{aligned}$$

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

$$M(k,p) = \sum_{n \in \mathbb{F}_p} \prod_{0 \leq i \leq k} \left(\frac{1}{p} \sum_{\gcd(n_i, p-1)=1} 1 \right), \tag{17.4}$$

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

$$E(k,p) = \sum_{n \in \mathbb{F}_p} \prod_{0 \leq i \leq k} \left(\frac{1}{p} \sum_{\substack{\gcd(n_i, p-1)=1 \\ 1 \leq u_i \leq p-1}} \psi\left((\tau^{n_i} - n - a_i)u_i\right) \right). \tag{17.5}$$

Applying Lemma 14.1 to the main term and Lemma 15.2 to the error term, yield

$$\begin{aligned} N(k,p) &= M(k,p) + E(k,p) \\ &= \left(\frac{\varphi(p-1)}{p-1} \right)^{k+1} p + O(\log^2 p) + O(p^{1-\varepsilon}) \\ &= \left(\frac{\varphi(p-1)}{p-1} \right)^{k+1} p + O(p^{1-\varepsilon}) \\ &> 0, \end{aligned} \tag{17.6}$$

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

■

Lemma 17.1. *Let $x \geq 1$ be a large number, let $p \leq x$ be a large prime, and let $k \geq 1$ be an integer. Then, the average number of $(k+1)$ consecutive primitive roots modulo p has the asymptotic*

$$\frac{1}{x} \sum_{p \leq x} \left(\frac{\varphi(p-1)}{p-1} \right)^k p = a_k \frac{x}{2 \log x} + O\left(\frac{x}{\log^2 x} \right), \tag{17.7}$$

where $a_k > 0$ is a constant.

Proof. The value of the constant and a proof appear in Lemma 4.7. ■

17.2 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 17.1. The probability of primitive roots in a finite field $\mathbb{F}_p$ is defined by

$$P\left(\operatorname{ord}_p(X) = p-1\right) = \frac{\varphi(p-1)}{p-1} + O\left(\frac{1}{p^{\varepsilon}} \right), \tag{17.8}$$

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 17.1. A random $(k+1)$-tuple of consecutive primitive roots is denoted by

$$Z_k = (X_0, X_1, \ldots, X_k), \tag{17.9}$$

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

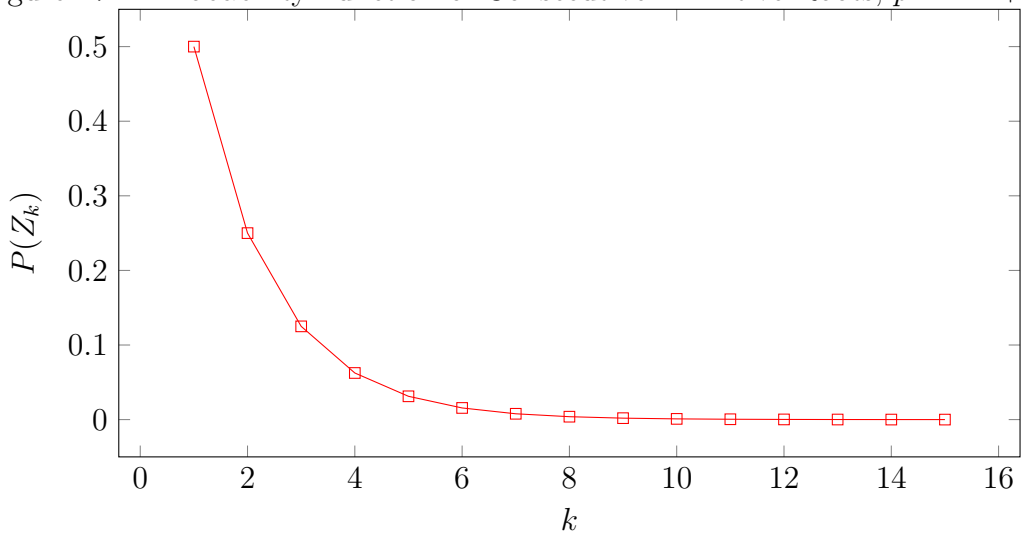
$$P(Z_k) = \left(\frac{\varphi(p-1)}{p-1}\right)^{k+1} = \left(\frac{1}{2} - \frac{1}{2q}\right)^{k+1}, \tag{17.10}$$

Table 16.1 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
$q \geq 3$ is prime, is

$$P(Z_k) = \left(\frac{\varphi(p-1)}{p-1}\right)^{k+1} = \prod_{r \leq q} \left(1 - \frac{1}{q}\right)^{k+1}, \tag{17.11}$$

where $r \leq q$ ranges over the primes. Some numerical data are displayed in Figure 17.1 and Figure 17.2.

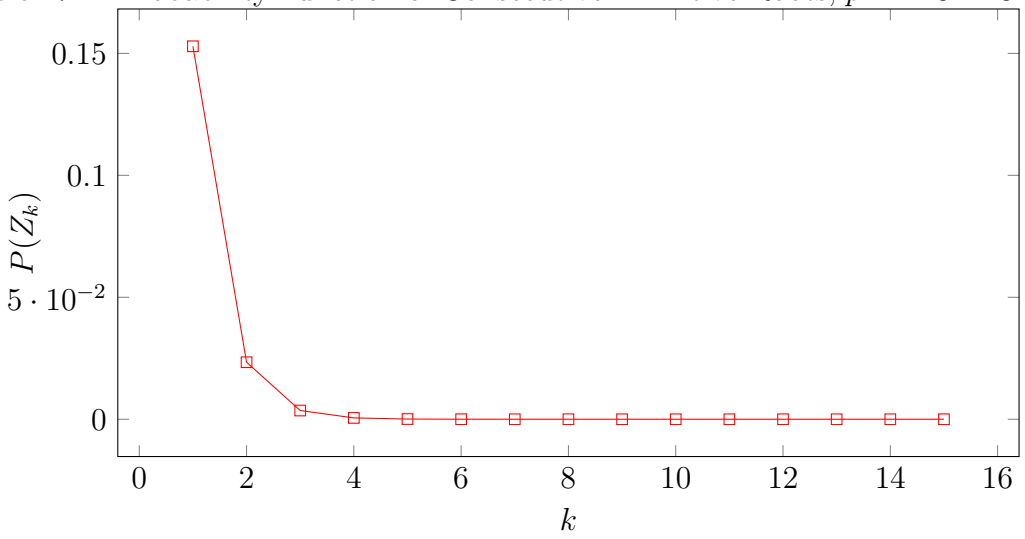
Figure 17.1: Probability Function of Consecutive Primitive Roots, $p = 2^{16} + 1$



17.3 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:

Figure 17.2: Probability Function of Consecutive Primitive Roots, $p = 2 \cdot 3 \cdots 31 + 1$



1. $\tau^{n_0} = n + a_0, \quad \tau^{n_1} = n + a_1, \quad \ldots, \quad \tau^{n_k} = n + a_k,$
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

$$N_2(k,p) = \#\left\{n \in \mathbb{F}_p : \mathrm{ord}_p(n + a_i) = p - 1, \mu^2(n + a_i) = 1\right\} \tag{17.12}$$

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

17.4 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 12.3, and the characteristic function for squarefree integers, see Lemma 3.4, as

$$\begin{aligned} N_2(k,p) &= \sum_{n \in \mathbb{F}_p} \prod_{0 \le i \le k} \Psi\left(n + a_i\right) \mu^2(n + a_i) \qquad (17.13) \\ &= \sum_{n \in \mathbb{F}_p} \prod_{0 \le i \le k} \left(\frac{1}{p} \sum_{\substack{\gcd(n_i, p-1) = 1 \\ 0 \le u_i \le p-1}} \psi\left((\tau^{n_i} - n - a_i) u_i\right) \right) \\ &= M_2(k,p) + E_2(k,p). \end{aligned}$$

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

$$M_2(k,p) = \sum_{n\in\mathbb{F}_p} \prod_{0\le i\le k} \left(\frac{\mu^2(n+a_i)}{p} \sum_{\gcd(n_i,p-1)=1} 1 \right), \tag{17.14}$$

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

$$E_2(k,p) = \sum_{n\in\mathbb{F}_p} \prod_{0\le i\le k} \left(\frac{\mu^2(n+a_i)}{p} \sum_{\substack{\gcd(n_i,p-1)=1 \\ 1\le u_i\le p-1}} \psi\left((\tau^{n_i} - n - a_i)u_i\right) \right). \tag{17.15}$$

Applying Lemma 14.2 to the main term and Lemma 15.4 to the error term, yield

$$\begin{aligned} N_2(k,p) &= M_2(k,p) + E_2(k,p) \qquad (17.16)\\ &= \prod_{q\ge 2} \left(1 - \frac{\omega(q)}{q^2}\right) \left(\frac{\varphi(p-1)}{p-1}\right)^{k+1} p + O\left(p^{2/3}\right) + O(p^{1-\varepsilon}) \\ &= \prod_{q\ge 2} \left(1 - \frac{\omega(q)}{q^2}\right) \left(\frac{\varphi(p-1)}{p-1}\right)^{k+1} p + O(p^{1-\varepsilon}) \\ &> 0, \end{aligned}$$

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

17.5 Problems

Exercise 17.1. 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 17.2. 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?

Chapter 18

Squarefree Primitive Roots

18.1 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

$$\tau^m = n \quad \text{and} \quad \mu^2(n) = 1, \tag{18.1}$$

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

$$N_2(p) = \#\left\{n \in \mathbb{F}_p : \operatorname{ord}_p(n) = p-1 \text{ and } \mu^2(n) = 1\right\} \tag{18.2}$$

denotes the number of solutions.

Theorem 18.1. *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*

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

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 12.3, and the characteristic function for squarefree integers, see Lemma 3.4, as

$$\begin{aligned} \sum_{n \in \mathbb{F}_p} \Psi(n)\, \mu^2(n) &= \sum_{n \in \mathbb{F}_p} \left(\frac{\mu^2(n)}{p} \sum_{\substack{\gcd(m,p-1)=1 \\ 0 \leq u \leq p-1}} \psi\left((\tau^m - n)u\right) \right) \\ &= M_2(p) + E_2(p). \end{aligned} \tag{18.3}$$

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 14.5 to the main term and

Lemma 15.4 to the error term, yield

$$\begin{aligned} N_2(p) &= M_2(p) + E_2(p) \\ &= \prod_{q\geq 2}\left(1-\frac{1}{q^2}\right)\left(\frac{\varphi(p-1)}{p}\right)p + O\left(p^{1/2}\right) + O(p^{1-\varepsilon}) \\ &= \prod_{q\geq 2}\left(1-\frac{1}{q^2}\right)\left(\frac{\varphi(p-1)}{p}\right)p + O(p^{1-\varepsilon}) \\ &> 0, \end{aligned} \tag{18.4}$$

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

18.2 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

$$N_2(2,p) = \#\left\{n \in \mathbb{F}_p : \mathrm{ord}_p(n + a_i) = p - 1, \text{ and } \mu^2(n + a_i) = 1\right\} \tag{18.5}$$

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

Theorem 18.2. *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*

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

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 12.3, and the characteristic function for squarefree integers, see Lemma 3.4, as

$$\begin{aligned} \mathbb{N}_2(2,p) &= sum_{n\in\mathbb{F}_p}\Psi\left(n+a_0\right)\Psi\left(n+a_1\right)\mu^2(n+a_0)\mu^2(n+a_1) \\ &= \sum_{n\in\mathbb{F}_p}\left(\frac{\mu^2(n+a_0)}{p}\sum_{\substack{\gcd(n_0,p-1)=1\\ 0\leq u_0\leq p-1}}\psi\left((\tau^{n_0}-n-a_0)u_0\right)\right) \\ &\quad\times\left(\frac{\mu^2(n+a_1)}{p}\sum_{\substack{\gcd(n_1,p-1)=1\\ 0\leq u_1\leq p-1}}\psi\left((\tau^{n_1}-n-a_1)u_1\right)\right) \\ &= M_2(2,p) + E_2(2,p). \end{aligned} \tag{18.6}$$

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 14.3 to the main term and Lemma 15.4 to the error term, yield

$$\begin{aligned} N_2(2,p) &= M_2(2,p) + E_2(2,p) \\ &= \prod_{q\geq 2}\left(1-\frac{2}{q^2}\right)\left(\frac{\varphi(p-1)}{p-1}\right)^2 p + O\left(p^{2/3}\right) + O(p^{1-\varepsilon}) \\ &= \prod_{q\geq 2}\left(1-\frac{2}{q^2}\right)\left(\frac{\varphi(p-1)}{p-1}\right)^2 p + O(p^{1-\varepsilon}) \\ &> 0, \end{aligned} \tag{18.7}$$

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

18.3 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

$$N_2(3,p) = \#\left\{n \in \mathbb{F}_p : \operatorname{ord}_p(n + a_i) = p - 1, \text{ and } \mu^2(n + a_i) = 1\right\} \tag{18.8}$$

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

Theorem 18.3. *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*

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

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 12.3,

and the characteristic function for squarefree integers, see Lemma 3.4, as

$$\begin{aligned} N_2(3,p) &= \sum_{n\in\mathbb{F}_p} \Psi(n)\,\Psi(n+1)\,\Psi(n+2)\,\mu^2(n)\mu^2(n+1)\mu^2(n+2) \qquad (18.9)\\ &= \sum_{n\in\mathbb{F}_p} \left(\frac{\mu^2(n)}{p} \sum_{\substack{\gcd(n_0,p-1)=1\\ 0\le u_0\le p-1}} \psi\left((\tau^{n_0}-n)u_0\right) \right)\\ &\quad \times \left(\frac{\mu^2(n+1)}{p} \sum_{\substack{\gcd(n_1,p-1)=1\\ 0\le u_1\le p-1}} \psi\left((\tau^{n_1}-n-1)u_1\right) \right)\\ &\quad \times \left(\frac{\mu^2(n+1)}{p} \sum_{\substack{\gcd(n_2,p-1)=1\\ 0\le u_2\le p-1}} \psi\left((\tau^{n_2}-n-2)u_2\right) \right)\\ &= M_2(3,p)+E_2(3,p). \qquad (18.10) \end{aligned}$$

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 14.4 to the main term and Lemma 15.4 to the error term, yield

$$\begin{aligned} N_2(3,p) &= M_2(3,p)+E_2(3,p) \qquad (18.11)\\ &= \prod_{q\ge 2}\left(1-\frac{3}{q^2}\right)\left(\frac{\varphi(p-1)}{p-1}\right)^3 p + O\left(p^{2/3}\right)+O(p^{1-\varepsilon})\\ &= \prod_{q\ge 2}\left(1-\frac{3}{q^2}\right)\left(\frac{\varphi(p-1)}{p-1}\right)^3 p + O(p^{1-\varepsilon})\\ &> 0, \end{aligned}$$

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

18.4 Problems

Exercise 18.1. 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 18.2. 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 18.3. 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 $n \geq 1$.

Chapter 19

Consecutive s-Power Free Primitive Roots

19.1 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

$$\tau^m = n \quad \text{and} \quad \mu_s(n) = 1, \tag{19.1}$$

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

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

see Lemma 3.4, denotes the number of solutions.

Theorem 19.1. *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*

$$N_s(p) = \prod_{q \geq 2}\left(1 - \frac{1}{q^s}\right)\left(\frac{\varphi(p-1)}{p-1}\right)p + O(p^{1-\varepsilon}), \tag{19.2}$$

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 12.3, and the characteristic function for s-power free integers, see Lemma 3.4, as

$$\begin{aligned}\sum_{n \in \mathbb{F}_p}\Psi(n)\,\mu_s(n) &= \sum_{n \in \mathbb{F}_p}\left(\frac{\mu_s(n)}{p}\sum_{\substack{\gcd(n,p-1)=1\\ 0 \leq u \leq p-1}}\psi\left((\tau^n - n)u\right)\right)\\ &= M_s(p) + E_s(p).\end{aligned} \tag{19.3}$$

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 14.5 to the main term and

Lemma 15.4 to the error term, yield

$$\begin{aligned} N_s(p) &= M_s(p) + E_s(p) \\ &= \prod_{q\geq 2}\left(1-\frac{1}{q^s}\right)\left(\frac{\varphi(p-1)}{p-1}\right)p + O\left(p^{1/s}\right) + O(p^{1-\varepsilon}) \\ &= \prod_{q\geq 2}\left(1-\frac{1}{q^s}\right)\left(\frac{\varphi(p-1)}{p-1}\right)p + O(p^{1-\varepsilon}) \\ &> 0, \end{aligned} \tag{19.4}$$

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

19.2 s-Power Free Twin Primitive Roots

Given a triple of small integers $a_0 \neq a_1$ and $s \geq 2$. Let $p \geq 2$ 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

$$N_s(2, p, a) = \#\left\{n \in \mathbb{F}_p : \mathrm{ord}_p(n + a_i) = p - 1, \text{ and } \mu_s(n + a_i) = \pm 1\right\}, \tag{19.5}$$

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 12.3, and the characteristic function for squarefree integers, see Lemma 3.4, as

$$\begin{aligned} N_s(2, p) &= \sum_{n\in\mathbb{F}_p} \Psi\left(n + a_0\right)\Psi\left(n + a_1\right)\mu_s(n + a_0)\mu_s(n + a_1) \\ &= \sum_{n\in\mathbb{F}_p}\left(\frac{\mu_s(n + a_0)}{p}\sum_{\substack{\gcd(n_0,p-1)=1\\ 0\leq u_0\leq p-1}}\psi\left((\tau^{n_0} - n - a_0)u_0\right)\right) \\ &\quad \times\left(\frac{\mu_s(n + a)}{p}\sum_{\substack{\gcd(n_1,p-1)=1\\ 0\leq u_1\leq p-1}}\psi\left((\tau^{n_1} - n - a_1)u_1\right)\right) \\ &= M_s(2, p) + E_s(2, p). \end{aligned} \tag{19.6}$$

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 14.6 to the main term and Lemma 15.4 to the error term, yield

$$\begin{aligned} N_s(2,p) &= M_s(2,p) + E_s(2,p) \qquad (19.7) \\ &= \prod_{q\geq 2}\left(1-\frac{\rho(s)}{q^s}\right)\left(\frac{\varphi(p-1)}{p-1}\right)^2 p + O\left(p^{\alpha(s)-\varepsilon}\right) + O(p^{1-\varepsilon}) \\ &= \prod_{q\geq 2}\left(1-\frac{\rho(s)}{q^s}\right)\left(\frac{\varphi(p-1)}{p-1}\right)^2 p + O(p^{1-\varepsilon}) \\ &> 0, \end{aligned}$$

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

Chapter 20

Relatively Prime Primitive Roots

The first proof based on Lemma **??** and restricted to $q = p - 1$ was given in [60]. A new proof based on Lemma **??**, 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.

20.1 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

$$N_r(p,q) = \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1}} \Psi(n). \tag{20.1}$$

In terms of characteristic function for primitive roots, see Lemma 12.3, this is written as

$$\begin{aligned} N_r(p,q) &= \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1}} \Psi(n) \\ &= \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1}} \left(\frac{1}{p} \sum_{\gcd(m,p-1)=1,\ 0 \leq u \leq p-1} \psi\left((\tau^m - n)u\right) \right) \qquad (20.2) \\ &= \frac{1}{p} \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1}} \sum_{\gcd(m,p-1)=1} 1 + \frac{1}{p} \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1}} \sum_{\gcd(m,p-1)=1,\ 0 < u \leq p-1} \psi\left((\tau^m - n)u\right) \\ &= M_r(p,q) + E_r(p,q). \end{aligned}$$

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 14.7 to the main

term and Lemma 15.1 to the error term, yield

$$\begin{aligned} N_r(p,q) &= M_r(p,q) + E_r(p,q) \\ &= \frac{\varphi(q)}{q}\frac{\varphi(p-1)}{p-1}p + O(\log^2 p) + O(p^{1-\varepsilon}) \\ &= \frac{\varphi(q)}{q}\frac{\varphi(p-1)}{p-1}p + O(p^{1-\varepsilon}) \\ &> 0, \end{aligned} \tag{20.3}$$

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

20.2 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:

$$c_2(q,a) \begin{cases} > 0 & \text{if } a = 2b+1, \text{ and } q = 2c+1, \text{ with } b \geq 0, c \geq 0, \\ = 0 & \text{if } a = 2b+1, \text{ and } q = 2c, \text{ with } b \geq 0, c \geq 1, \\ > 0 & \text{if } a = 2b, \text{ and } q \geq 1, \text{ with } b \geq 1. \end{cases} \tag{20.4}$$

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

$$N_r(2,p,q) = \#\left\{n \in \mathbb{F}_p : \operatorname{ord}_p(n) = \operatorname{ord}_p(n+a) = p-1, \gcd(n,q) = \gcd(n+1,q) = 1\right\} \tag{20.5}$$

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

$$N_r(2,p,q) = \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1 \\ \gcd(n+a,q)=1}} \Psi(n)\Psi(n+a). \tag{20.6}$$

In terms of characteristic function for primitive roots, see Lemma 12.3, this is written as

$$\begin{aligned} N_r(2,p,q) &= \sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1\\ \gcd(n+a,q)=1}} \left(\frac{1}{p}\sum_{\substack{0\le u\le p-1\\ \gcd(c,p-1)=1}} \psi\left((\tau^c-n)u\right)\right)\left(\frac{1}{p}\sum_{\substack{0\le v\le p-1\\ \gcd(d,p-1)=1}} \psi\left((\tau^d-n-a)v\right)\right)\\ &= M_r(2,p,q)+E_r(2,p,q). \end{aligned} \tag{20.7}$$

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

$$M_s(2,p,q) = \sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1\\ \gcd(n+a,q)=1}} \left(\frac{1}{p}\sum_{\substack{0\le u\le p-1\\ \gcd(c,p-1)=1}} 1\right)\left(\frac{1}{p}\sum_{\substack{0\le v\le p-1\\ \gcd(d,p-1)=1}} 1\right), \tag{20.8}$$

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

$$E_r(2,p,q) = \sum_{\substack{n\in\mathbb{F}_p\\ \gcd(n,q)=1\\ \gcd(n+a,q)=1}} \left(\frac{1}{p}\sum_{\substack{1\le u\le p-1\\ \gcd(c,p-1)=1}} \psi\left((\tau^c-n)u\right)\right)\left(\frac{1}{p}\sum_{\substack{1\le v\le p-1\\ \gcd(d,p-1)=1}} \psi\left((\tau^d-n-a)v\right)\right). \tag{20.9}$$

Applying Lemma 14.8 to the main term and Lemma 15.2 to the error term, yield

$$\begin{aligned} N_r(2,p,q) &= M_r(2,p,q)+E_r(2,p,q) \qquad (20.10)\\ &= c_2(q,a)\left(\frac{\varphi(q)}{q}\right)^2\frac{\varphi(p-1)}{p-1}p+O(p^{\varepsilon})+O(p^{1-\varepsilon})\\ &= c_2(q,a)\left(\frac{\varphi(q)}{q}\right)^2\frac{\varphi(p-1)}{p-1}p+O(p^{1-\varepsilon})\\ &> 0, \end{aligned}$$

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

Chapter 21

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 7.1, is a new result in the literature.

21.1 Squarefree And Relatively Prime Primitive Roots

Theorem 21.1. *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*

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

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

$$N_{sr}(p,q) = \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1}} \Psi(n)\mu(n)^2. \tag{21.1}$$

In terms of characteristic function for primitive roots, see Lemma 12.3, this is written

as

$$\begin{aligned} N_r(p,q) &= \sum_{\substack{n\in\mathbb{F}_p \\ \gcd(n,q)=1}} \Psi(n)\mu(n)^2 \qquad (21.2)\\ &= \sum_{\substack{n\in\mathbb{F}_p \\ \gcd(n,q)=1}} \left(\frac{\mu(n)^2}{p} \sum_{\gcd(m,p-1)=1,\ 0\le u\le p-1} \sum \psi\left((\tau^m - n)u\right) \right) \\ &= \frac{1}{p} \sum_{\substack{n\in\mathbb{F}_p \\ \gcd(n,q)=1}} \sum_{\gcd(m,p-1)=1} \mu(n)^2 \\ &\qquad + \sum_{\substack{n\in\mathbb{F}_p \\ \gcd(n,q)=1}} \frac{\mu(n)^2}{p} \sum_{\gcd(m,p-1)=1,\ 0<u\le p-1} \sum \psi\left((\tau^m - n)u\right) \\ &= M_{sr}(p,q) + E_{sr}(p,q). \end{aligned}$$

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 14.9 to the main term and Lemma 15.3 or Lemma 15.5 to the error term, yield

$$\begin{aligned} N_{sr}(p,q) &= M_{sr}(p,q) + E_{sr}(p,q) \qquad (21.3)\\ &= \frac{6}{\pi^2} \prod_{p\nmid q} \left(1+\frac{1}{p}\right)^{-1} \frac{\varphi(p-1)}{p-1} p + O(p^{1/2}) + O(p^{1-\varepsilon}) \\ &= \frac{6}{\pi^2} \prod_{p\nmid q} \left(1+\frac{1}{p}\right)^{-1} \frac{\varphi(p-1)}{p-1} p + O(p^{1-\varepsilon}) \\ &> 0, \end{aligned}$$

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

21.2 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:

$$c_2(q,a) \begin{cases} > 0 & \text{if } a = 2b+1, \text{ and } q = 2c+1, \text{ with } b \geq 0, c \geq 0, \\ = 0 & \text{if } a = 2b+1, \text{ and } q = 2c, \text{ with } b \geq 0, c \geq 1, \\ > 0 & \text{if } a = 2b, \text{ and } q \geq 1, \text{ with } b \geq 1. \end{cases} \qquad (21.4)$$

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

$$N_{sr}(2, p, q) = \#\{n \in \mathbb{F}_p : \text{Conditions 1, 2, and 3 are satisfied.}\} \tag{21.5}$$

denotes the number of solutions.

Theorem 21.2. *Assume Conjecture* 7.1. *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*

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

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

$$N_{sr}(2, p, q) = \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1 \\ \gcd(n+a,q)=1}} \Psi(n)\Psi(n+a)\mu(n)^2\mu(n+a)^2. \tag{21.6}$$

In terms of characteristic function for primitive roots, see Lemma 12.3, this is written as

$$\begin{aligned} N_{sr}(2, p, q) &= \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1 \\ \gcd(n+a,q)=1}} \left(\frac{\mu(n)^2}{p} \sum_{\substack{0 \leq u \leq p-1 \\ \gcd(c,p-1)=1}} \psi\left((\tau^c - n)u\right) \right) \\ &\quad \times \left(\frac{\mu(n+a)^2}{p} \sum_{\substack{0 \leq v \leq p-1 \\ \gcd(d,p-1)=1}} \psi\left((\tau^d - n - a)v\right) \right) \\ &= M_{sr}(2, p, q) + E_{sr}(2, p, q). \end{aligned} \tag{21.7}$$

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

$$M_s(2, p, q) = \sum_{\substack{n \in \mathbb{F}_p \\ \gcd(n,q)=1 \\ \gcd(n+a,q)=1}} \left(\frac{1}{p} \sum_{\substack{0 \leq u \leq p-1 \\ \gcd(c,p-1)=1}} \mu(n)^2 \right) \left(\frac{1}{p} \sum_{\substack{0 \leq v \leq p-1 \\ \gcd(d,p-1)=1}} \mu(n+a)^2 \right), \tag{21.8}$$

and the error term $E_{sr}(2,p,q)$ is determined by the indices $u \neq 0, v \neq 0$, and has the form as (21.7). Applying Lemma 14.10 to the main term and Lemma 15.5 to the error term, yield

$$\begin{aligned} N_{sr}(2,p,q) &= M_{sr}(2,p,q) + E_{sr}(2,p,q) \qquad (21.9) \\ &= c_2(q,a) \prod_{p \nmid q} \left(1+\frac{1}{p}\right)^{-2} \prod_{p \geq 2} \left(1-\frac{2}{p^2}\right) \left(\frac{\varphi(p-1)}{p}\right)^2 p \\ &\qquad + O\left(p^{1-\delta}\right) + O(p^{1-\varepsilon}) \\ &= c_2(q,a) \prod_{p \nmid q} \left(1+\frac{1}{p}\right)^{-2} \prod_{p \geq 2} \left(1-\frac{2}{p^2}\right) \left(\frac{\varphi(p-1)}{p}\right)^2 p + O(p^{1-\varepsilon}) \\ &> 0, \end{aligned}$$

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

21.3 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

$$P\left(\mathrm{ord}_p\left(X\right) = p-1 \text{ and } \mu(X)^2 \neq 0\right) = \frac{\varphi(p-1)}{p-1} \prod_{q \geq 2} \left(1-\frac{1}{q^2}\right) + O\left(\frac{1}{p^{\varepsilon}}\right), \quad (21.10)$$

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 $p \geq 2$ 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*

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

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

Proof. The density constant in the main term of Theorem 18.2 is the probability of having two consecutive squafree primitive roots. Next, use a series of steps to reduces to a simpler product:

$$\begin{aligned}\left(\frac{\varphi(p-1)}{p-1}\right)^2\prod_{q\geq 2}\left(1-\frac{2}{q^2}\right) &= \left(\frac{\varphi(p-1)}{p-1}\right)^2\prod_{q\geq 2}\left(1-\frac{1}{q^2}\right)^2\left(1+\frac{1}{q^2(q^2-2)}\right)^{-1}\\ &< \left(\frac{\varphi(p-1)}{p-1}\right)^2\prod_{q\geq 2}\left(1-\frac{1}{q^2}\right)^2. \qquad (21.11)\end{aligned}$$

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

$$c_2(2)=\prod_{q\geq 2}\left(1+\frac{1}{q^2(q^2-2)}\right)^{-1}=0.87298595344931361877174511\ldots. \qquad (21.12)$$

■

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*

$$\begin{aligned}P(X_0,X_1,X_2) &= P\begin{pmatrix}\operatorname{ord}(X_0)=\operatorname{ord}(X_1)=\operatorname{ord}(X_2)=p-1,\\ \mu(X_0)=\pm 1,\mu(X_1)=\pm 1,\mu(X_2)=\pm 1\end{pmatrix} \qquad (21.13)\\ &= \left(\frac{\varphi(p-1)}{p-1}\right)^3\prod_{q\geq 2}\left(1-\frac{3}{q^2}\right)+O\left(\frac{1}{p^{\varepsilon}}\right),\end{aligned}$$

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

Proof. The density constant in the main term of Theorem 18.2 is the probability of having two consecutive squafree primitive roots. Next, use a series of steps to reduces to a simpler product:

$$\begin{aligned}\left(\frac{\varphi(p-1)}{p-1}\right)^3\prod_{q\geq 2}\left(1-\frac{3}{q^2}\right) &= \left(\frac{\varphi(p-1)}{p-1}\right)^3\prod_{q\geq 2}\left(1-\frac{1}{q^2}\right)^3\left(1+\frac{3q^2-1}{q^4(q^2-3)}\right)^{-1}\\ &< \left(\frac{\varphi(p-1)}{p-1}\right)^3\prod_{q\geq 2}\left(1-\frac{1}{q^2}\right)^3. \qquad (21.14)\end{aligned}$$

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

$$c_2(3)=\prod_{q\geq 2}\left(1+\frac{3q^2-1}{q^4(q^2-3)}\right)^{-1}=0.55852697912768910553333 0\ldots. \qquad (21.15)$$

■

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 $q=2$.

21.4 Problems

Exercise 21.1. 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 21.2. 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 21.3. 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.

Chapter 22

B-Smooth Primitive Roots

22.1 B-Smooth Primitive Roots

Let $p \geq 2$ be a large prime, let $B = p^{1/u}$, with $u > 0$, and let $\tau \in \mathbb{F}_p$ be a primitive root. A B-smooth primitive root $n \in \mathbb{F}_p$ exists if and only if the system of equations

$$\tau^m = n \quad \text{and} \quad \alpha_B(n) = 1, \tag{22.1}$$

where $\mathcal{S}_B(n)$ is the characteristic function of B-smooth number, 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

$$N_u(p) = \#\left\{n \in \mathbb{F}_p : \operatorname{ord}_p(n) = p-1 \text{ and } \mathcal{S}_B(n) = 1\right\} \tag{22.2}$$

denotes the number of solutions.

Theorem 22.1. *For any large prime $p \geq 2$, and let $B = p^{1/u}$ with $u > 0$. Then, the finite field $\mathbb{F}_p$ contains B-smooth primitive roots. Furthermore, the total number has the asymptotic formula*

$$N_u(p) = \rho(u)\left(\frac{\varphi(p-1)}{p}\right)p + O\left(\frac{\rho(u-1)p}{\log p}\right),$$

where $\rho(u) > 0$ is the density of smooth numbers.

Proof. The total number of solutions is written in terms of characteristic function for primitive roots, see Lemma 12.3, and the characteristic function for B-smooth integers, see Lemma 12.4, as

$$\begin{aligned}\sum_{n\in\mathbb{F}_p}\Psi(n)\,\mathcal{S}_B(n) &= \sum_{n\in\mathbb{F}_p}\left(\frac{\mathcal{S}_B(n)}{p}\sum_{\substack{\gcd(m,p-1)=1\\0\leq a\leq p-1}}\psi\left((\tau^m-n)a\right)\right)\\ &= M_2(p)+E_2(p).\end{aligned} \tag{22.3}$$

The main term $M_u(p)$ is determined by the index $a = 0$, and the error term $E_u(p)$ is determined by the index $a \neq 0$. Applying Lemma 14.11 to the main term and

Lemma 15.4 to the error term, yield

$$\begin{aligned} N_u(p) &= M_u(p) + E_u(p) \\ &= \rho(u)\left(\frac{\varphi(p-1)}{p}\right)p + O\left(\frac{\rho(u-1)p}{\log p}\right) + O(p^{1-\varepsilon}) \\ &= \rho(u)\left(\frac{\varphi(p-1)}{p}\right)p + O\left(\frac{\rho(u-1)p}{\log p}\right) \\ &> 0, \end{aligned} \tag{22.4}$$

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

22.2 B-Smooth Twin Primitive Roots

Let $p \geq 2$ be a large prime, let $B = p^{1/u}$, and let $\tau \in \mathbb{F}_p$ be a primitive root. Each B-Smooth twin primitive roots n and $n+1$ is a solution of the systems of equations

1. $\tau^{n_0} = n, \quad \tau^{n_1} = n+1,$ the primitive root condition.

2. $\mathcal{S}_B(n) = 1, \quad \mathcal{S}_B(n+1) = 1,$ the smoothness 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

$$N_u(2,p) = \#\left\{n \in \mathbb{F}_p : \operatorname{ord}_p(n+a_i) = p-1, \text{ and } \mathcal{S}_B(n+a_i) = 1\right\} \tag{22.5}$$

for $i = 0, 1$, and $a_0 = 0$ and $a_1 = 1$, denotes the number of solutions.

Theorem 22.2. *For any large prime $p \geq 2$, let $B = p^{1/u}$, with $u > 0$. Then, the finite field $\mathbb{F}_p$ contains 2 consecutive B-Smooth primitive roots. Furthermore, the number of pairs has the asymptotic formula*

$$N_u(2,p) = a_2(u)\rho(u)^2\left(\frac{\varphi(p-1)}{p-1}\right)^2 p + O\left(\frac{t(u)p}{\log p}\right),$$

where $a_2(u) > 0$ is a dependence correction factor, $\rho(u) > 0$ is the density of smooth numbers, and $t(u)$ is some function of $u > 0$.

Proof. The total number of solutions is written in terms of characteristic function for primitive roots, see Lemma 12.3, and the characteristic function $\mathcal{S}_B(n)$ for B-smooth

integers, see Lemma 12.4, as

$$\begin{aligned}
\mathbb{N}_u(2,p) &= \sum_{n\in\mathbb{F}_p} \Psi\left(n+a_0\right)\Psi\left(n+a_1\right)\mathcal{S}_B(n+a_0)\mathcal{S}_B(n+a_1) \qquad (22.6)\\
&= \sum_{n\in\mathbb{F}_p}\left(\frac{\mathcal{S}_B(n+a_0)}{p}\sum_{\substack{\gcd(n_0,p-1)=1\\0\le u_0\le p-1}}\psi\left((\tau^{n_0}-n-a_0)u_0\right)\right)\\
&\qquad\qquad\times\left(\frac{\mathcal{S}_B(n+a_1)}{p}\sum_{\substack{\gcd(n_1,p-1)=1\\0\le u_1\le p-1}}\psi\left((\tau^{n_1}-n-a_1)u_1\right)\right)\\
&= M_u(2,p)+E_u(2,p).
\end{aligned}$$

The main term $M_u(2,p)$ is determined by the indices $u_0=u_1=0$, and the error term $E_u(2,p)$ is determined by the indices $u_0\neq 0, u_1\neq 0$. Applying Lemma 14.12 to the main term and Lemma 15.4 to the error term, yield

$$\begin{aligned}
N_u(2,p) &= M_u(2,p)+E_u(2,p) \qquad (22.7)\\
&= a_2(u)\rho(u)^2\left(\frac{\varphi(p-1)}{p-1}\right)^2 p+O\left(\frac{t(u)p}{\log p}\right)+O(p^{1-\varepsilon})\\
&= a_2(u)\rho(u)^2\left(\frac{\varphi(p-1)}{p-1}\right)^2 p+O\left(\frac{t(u)p}{\log p}\right)\\
&> 0,
\end{aligned}$$

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

Chapter 23

Prime And Twin Primitive Roots

23.1 Prime Primitive Roots

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

$$\tau^m = n \quad \text{and} \quad \Lambda(n)/\log n = 1, \tag{23.1}$$

where $\Lambda(n)/\log n$ is the characteristic function of prime power number, 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

$$N_0(p) = \#\left\{n \in \mathbb{F}_p : \operatorname{ord}_p(n) = p-1 \text{ and } \Lambda(n)/\log n = 1\right\} \tag{23.2}$$

denotes the number of solutions.

Theorem 23.1. *For any large prime $p \geq 2$, the finite field $\mathbb{F}_p$ contains prime primitive roots. Furthermore, the total number has the asymptotic formula*

$$N_0(p) = \left(\frac{\varphi(p-1)}{p}\right)\frac{p}{\log p} + O\left(\frac{p}{\log^2 p}\right).$$

Proof. The total number of solutions is written in terms of characteristic function for primitive roots, see Lemma 12.3, and the characteristic function for prime power integers, see Section 9.3, as

$$\begin{aligned}\sum_{n\in\mathbb{F}_p} \Psi(n)\frac{\Lambda(n)}{\log n} &= \frac{1}{p}\sum_{n\in\mathbb{F}_p}\left(\frac{\Lambda(n)}{\log n}\sum_{\substack{\gcd(m,p-1)=1\\0\leq a\leq p-1}}\psi\left((\tau^m-n)a\right)\right)\\ &= M_0(p) + E_0(p).\end{aligned} \tag{23.3}$$

The main term $M_0(p)$ is determined by the index $a = 0$, and the error term $E_0(p)$ is determined by the index $a \neq 0$. Applying Lemma 14.13 to the main term and

Lemma 15.4 to the error term, yield

$$\begin{aligned} N_0(p) &= M_0(p) + E_0(p) \\ &= \left(\frac{\varphi(p-1)}{p}\right)\frac{p}{\log p} + O\left(\frac{p}{\log^2 p}\right) + O(p^{1-\varepsilon}) \\ &= \left(\frac{\varphi(p-1)}{p}\right)\frac{p}{\log p} + O\left(\frac{p}{\log^2 p}\right) \\ &> 0, \end{aligned} \tag{23.4}$$

for all sufficently large primes $p \geq 2$. ■

23.2 Twin Primes Primitive Roots

Let $p \geq 2$ be a large prime, and let $\tau \in \mathbb{F}_p$ be a primitive root. Each twin prime primitive roots n and $n+1$ is a solution of the systems of equations

1. $\tau^{n_0} = n, \quad \tau^{n_1} = n+1,$ the primitive root condition.

2. $\dfrac{\Lambda(n)}{\log n} = 1, \quad \dfrac{\Lambda(n+2)}{\log(n+2)} = 1,$ the twin primes 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

$$N_0(2,p) = \#\left\{n \in \mathbb{F}_p : \operatorname{ord}_p(n+a_i) = p-1, \text{ and } \frac{\Lambda(n+a_i)}{\log(n+a_i)} = 1\right\} \tag{23.5}$$

for $i = 0, 1$, and $a_0 = 0$ and $a_1 = 1$, denotes the number of solutions.

Theorem 23.2. *Assume Conjecture* 9.3. *For any large prime $p \geq 2$, the finite field $\mathbb{F}_p$ contains twin primes primitive roots. Furthermore, the number of pairs has the asymptotic formula*

$$N_0(2,p) = \mathfrak{G}(2)\left(\frac{\varphi(p-1)}{p-1}\right)^2 \frac{p}{\log^2 p} + O\left(\frac{p}{\log^3 p}\right),$$

where $\mathfrak{G}(2) > 0$ is the twin prime constant.

Proof. The total number of solutions is written in terms of characteristic function for primitive roots, see Lemma 12.3, and the characteristic function for twin prime

integers, see Section 9.3, as

$$\begin{aligned}
\mathbb{N}_0(2,p) &= \sum_{n\in\mathbb{F}_p} \Psi(n)\,\frac{\Lambda(n)}{\log(n)}\cdot\Psi(n+2)\,\frac{\Lambda(n+2)}{\log(n+2)} \qquad (23.6)\\
&= \sum_{n\in\mathbb{F}_p}\left(\frac{1}{p}\frac{\Lambda(n)}{\log(n)}\sum_{\substack{\gcd(n_0,p-1)=1\\ 0\le u_0\le p-1}}\psi\left((\tau^{n_0}-n)u_0\right)\right)\\
&\qquad\times\left(\frac{1}{p}\frac{\Lambda(n+2)}{\log(n+2)}\sum_{\substack{\gcd(n_1,p-1)=1\\ 0\le u_1\le p-1}}\psi\left((\tau^{n_1}-n-2)u_1\right)\right)\\
&= M_0(2,p)+E_0(2,p).
\end{aligned}$$

The main term $M_0(2,p)$ is determined by the indices $u_0 = u_1 = 0$, and the error term $E_0(2,p)$ is determined by the indices $u_0 \neq 0, u_1 \neq 0$. Applying Lemma 14.14 to the main term and Lemma 15.4 to the error term, yield

$$\begin{aligned}
N_0(2,p) &= M_0(2,p)+E_0(2,p) \qquad (23.7)\\
&= \mathfrak{G}(2)\left(\frac{\varphi(p-1)}{p-1}\right)^2\frac{p}{\log^2 p}+O\left(p\log^2 p\right)+O(p^{1-\varepsilon})\\
&= \mathfrak{G}(2)\left(\frac{\varphi(p-1)}{p-1}\right)^2\frac{p}{\log^2 p}+O\left(p\log^2 p\right)\\
&> 0,
\end{aligned}$$

for all sufficently large primes $p \geq 2$. ■

Chapter 24

The Order Series

The Romanoff problem is concerned with the evaluation of the series $\sum_{n\geq 2} 1/(n \operatorname{ord}(2))$. This seris occurs in the calculation of the density of the binary additive problem $n = p + 2^k$. Much more general versions of this series are used in similar additive problems.

24.1 Order Series Over The Integers

Theorem 24.1. ([85]) *Let $f_v(n) = \operatorname{ord}_n(v)$. Then*

(i) *If $\varepsilon > 0$ is an arbitrary small number, then there is an absolute constant c_2 for which,*

$$\sum_{n\geq 2} \frac{1}{nf_v(n)^{\varepsilon}} \leq e^{\gamma} \left(\log\log v + \varepsilon^{-1} + c_2\right). \tag{24.1}$$

(ii) *If $\varepsilon > 0$ is an arbitrary small number, let $x \geq 2$, and let $v = 1+\operatorname{lcm}[1, 2, \ldots, x]$, then*

$$\sum_{n\geq 2} \frac{1}{nf_v(n)^{\varepsilon}} \geq e^{\gamma} \log\log v + O\left(\log\log\log v\right). \tag{24.2}$$

24.2 Order Series Over Subsets Of Integers

Let $q \geq 2$ be a prime power, and let $v \geq$ be a fixed integer. The asymptotic formulas for the restrictions to relatively primes subsets of integers $\mathcal{A} = \{n \geq 1 : \gcd(\operatorname{ord}_n(v), q) = 1\}$ are considered in this section. These results are based on the counting function $A(x) = \{n \leq x : n \in \mathcal{A}\}$.

Theorem 24.2. ([77, Theorem 4]) *For a prime power $q \geq 2$, and a large number $x \geq 1$, the counting function $A(x)$ has the asymptotic foirmula*

$$\sum_{\substack{n\leq x \\ \gcd(\operatorname{ord}_n(v),q)=1}} 1 = a(q,v)\frac{x}{\log^{c(q,v)} x}\left(1 + O_q\left(\frac{(\log\log x)^5}{(\log x)^{c(q,v)+1}}\right)\right),$$

where $a(q,v) > 0$ and $c(q,v) > 0$ are constants.

Theorem 24.3. *For any prime power $q \geq 2$, and fixed integer let $v \geq$, the order series converges:*

$$\sum_{\substack{n \leq x \\ \gcd(\mathrm{ord}_n(v),q)=1}} \frac{1}{n \,\mathrm{ord}_n(v)} < \infty. \tag{24.3}$$

Proof. Let $\mathcal{A} = \{n \geq 1 : \gcd(\mathrm{ord}_n(v), q) = 1\}$ and let $A(x) = \{n \leq x : n \in \mathcal{A}\}$ be the corresponding the counting function. The series has an integral representation as

$$\sum_{\substack{n \leq x \\ \gcd(\mathrm{ord}_n(v),q)=1}} \frac{1}{n \,\mathrm{ord}_n(v)} = \int_1^\infty \frac{1}{t \,\mathrm{ord}_t(v)} dA(t). \tag{24.4}$$

Use the bounds of the order function $1/t < 1/\,\mathrm{ord}_t(v) < 1/\log t$ and its derivatives

$$-\frac{1}{t^2} < \frac{d}{dt}\frac{1}{\mathrm{ord}_t(v)} < -\frac{1}{t}, \tag{24.5}$$

and Theorem 24.2, which gives $)A(t) \ll x \log^{-c(q,v)} x$, to estimate the integral:

$$\begin{aligned}
\int_1^\infty \frac{1}{t \,\mathrm{ord}_t(v)} dA(t) &= \frac{A(t)}{t \,\mathrm{ord}_t(v)} - \int_1^\infty \left(\frac{-1}{t^2 \,\mathrm{ord}_t(v)} + \frac{1}{t}\frac{d}{dt}\frac{1}{\mathrm{ord}_t(v)} \right) A(t) dt \\
&\ll O\left(\frac{1}{(\log x)^{c(q,v)+1}} \right) + \int_1^\infty \left(\frac{1}{t^2 \log t} + \frac{1}{t}\frac{1}{\log t} \right) \frac{t}{\log^{c(q,v)} t} dt \\
&= O\left(\frac{1}{(\log x)^{c(q,v)}} \right), \qquad (24.6)
\end{aligned}$$

where $c(q,v) > 1$ is a constant. ■

24.3 An Estimate For The Series $\sum_p \omega(p)$

The new result in Theorem 24.3 is used to sharpen the numerical evaluation of the series

$$\sum_{p \geq 2} \frac{1}{\omega(p)} \leq 0.9091\ldots, \tag{24.7}$$

where $\omega(p) = \mathrm{ord}_{p^2}(2)$. The above estimate was computed in [52]. Similar routines are used here too.

Lemma 24.1. *Let $\omega(p) = \mathrm{ord}_{p^2}(2)$. Then*

$$\sum_{p \geq 2} \frac{1}{\omega(p)} \leq 0.811049529055567378261719\ldots.$$

Proof. Start substituting the data

(i) $\mathrm{ord}_{p^2}(2) = \mathrm{ord}_p(2)$ if $2^{p-1} - 1 \equiv 0 \bmod p^2$, and

(ii) $\operatorname{ord}_{p^2}(2) = p \operatorname{ord}_p(2)$ if $2^{p-1} - 1 \not\equiv 0 \bmod p^2$,

into the series:

$$\begin{aligned}\sum_{p\geq 2} \frac{1}{\omega(p)} &= \sum_{\substack{p\geq 2 \\ 2^{p-1}-1\equiv 0 \bmod p^2}} \frac{1}{\omega(p)} + \sum_{\substack{p\geq 2 \\ 2^{p-1}-1\not\equiv 0 \bmod p^2}} \frac{1}{\omega(p)} \\ &= \sum_{\substack{p\geq 2 \\ 2^{p-1}-1\equiv 0 \bmod p^2}} \frac{1}{\operatorname{ord}_p(2)} + \sum_{\substack{p\geq 2 \\ 2^{p-1}-1\not\equiv 0 \bmod p^2}} \frac{1}{p \operatorname{ord}_p(2)}.\end{aligned} \tag{24.8}$$

Using $\operatorname{ord}_p(2) \geq \log p / \log 2$, the upper bound $W_2(x) \leq 8 \log\log x$, and the numerical data in [52] and [27], set $x = 7 \times 10^{15}$, the first subseries reduces to

$$\begin{aligned}\sum_{\substack{p\geq 2 \\ 2^{p-1}-1\equiv 0 \bmod p^2}} \frac{1}{\operatorname{ord}_p(2)} &= \sum_{\substack{p\leq 10^{15} \\ 2^{p-1}-1\equiv 0 \bmod p^2}} \frac{1}{\operatorname{ord}_p(2)} + \sum_{\substack{p> 10^{15} \\ 2^{p-1}-1\equiv 0 \bmod p^2}} \frac{1}{\operatorname{ord}_p(2)} \\ &\leq \frac{1}{\operatorname{ord}_{1093^2}(2)} + \frac{1}{\operatorname{ord}_{3511^2}(2)} + \sum_{\substack{p> 10^{15} \\ 2^{p-1}-1\equiv 0 \bmod p^2}} \frac{\log 2}{\log p} \\ &\leq \frac{1}{364} + \frac{1}{1755} + \int_{10^{15}}^{\infty} \frac{\log 2}{\log t} dW_2(t) \\ &\leq \frac{1}{364} + \frac{1}{1755} + \frac{8c \log 2 \log\log 10^{15}}{10^{15}} \\ &\leq 0.27665649717990874341880 77,\end{aligned} \tag{24.9}$$

where $0 < c \leq 10$ is a small constant. Fix a number $x = 10^4$, then the second subseries reduces to

$$\begin{aligned}\sum_{\substack{p\geq 2 \\ 2^{p-1}-1\not\equiv 0 \bmod p^2}} \frac{1}{p \operatorname{ord}_p(2)} &= \sum_{\substack{p\leq x \\ 2^{p-1}-1\not\equiv 0 \bmod p^2}} \frac{1}{p \operatorname{ord}_p(2)} + \sum_{\substack{p> x \\ 2^{p-1}-1\not\equiv 0 \bmod p^2}} \frac{1}{p \operatorname{ord}_p(2)} \\ &\leq 0.53439303187565863484291 14\ldots,\end{aligned} \tag{24.10}$$

where the lower tail is computed by a computer algebra system:

$$\sum_{p\leq x} \frac{1}{p \operatorname{ord}_p(2)} = 0.31724579092403272101734 69\ldots, \tag{24.11}$$

and the upper tail is estimated by an integral approximation:

$$\sum_{p>x} \frac{\log 2}{p \log p} \leq \frac{2}{\log x} = 0.21714724095162591382556 45\ldots, \tag{24.12}$$

■

For very large $x \geq 1$ the series is approximately

$$\sum_{p\geq 2} \frac{1}{\omega(p)} \leq .59390228810394146443615 5 + \frac{2}{\log x}. \tag{24.13}$$

Thus, the numerical value can be reduced to $\sum_{p\geq 2} 1/\omega(p) \leq .624$ by increasing $x > 10^{50}$.

24.4 Problems

Exercise 24.1. Given an arbitrary small number $\varepsilon > 0$, use the upper bound $\mathrm{ord}_n(v) < n$ of the order modulo n to show that

$$\sum_{n\geq 2} \frac{1}{n\,\mathrm{ord}_n(v)^{\varepsilon}} \geq \zeta(1+\varepsilon) \prod_{p|v} \left(1 - \frac{1}{p^{1+\varepsilon}}\right).$$

Exercise 24.2. Evaluate the squarefree oprdr series

$$\sum_{n\leq 2} \frac{\mu(n)^2}{n\,\mathrm{ord}_n(v)} \geq \frac{6e^{\gamma}}{\pi^2} \log\log v + O(1).$$

Exercise 24.3. Evaluate the limit

$$\lim_{m\to\infty} \sum_{\substack{n\geq 2 \\ \mathrm{ord}_n(v)=m}} \frac{1}{n} = 0.$$

Exercise 24.4. Evaluate the finite sum

$$\sum_{m\leq x} \sum_{\substack{n\geq 2 \\ \mathrm{ord}_n(v)=m}} \frac{1}{n} = a_v \log x + o(\log x),$$

where a_v is a constant.

Bibliography

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

[2] Bateman, P. T., Horn, R. A. *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp. 16 363-367, 1962.

[3] Michael A. Bennett, Greg Martin, Kevin O'Bryant, Andrew Rechnitzer. *Explicit bounds for primes in arithmetic progressions*. http://arxiv.org/abs/1802.00085.

[4] Julia Brandes. *Twins of s-free numbers*. http://arxiv.org/abs/1307.2066.

[5] Bruce, J. W. A Really Trivial Proof of the Lucas-Lehmer Test. The American Mathematical Monthly. 100 (4): 370-371, 1993.

[6] W.D. Banks, F. Luca, F. Saidak and P. Stanica. *Compositions with the Euler and Carmichael Functions*, Abh. Math. Sem. Univ. Hamburg., 75 (2005), 215-244.

[7] William D. Banks, Tristan Freiberg, Caroline L. Turnage-Butterbaugh. *Consecutive primes in tuples,* http://arxiv.org/abs/1311.7003.

[8] 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.

[9] Balog, Antal; Wooley, Trevor D. *On strings of consecutive integers with no large prime factors.* J. Austral. Math. Soc. Ser. A 64 (1998), no. 2, 266-276.

[10] Cobeli, Cristian. *On a Problem of Mordell with Primitive Roots*, http://arxiv.org/abs/0911.2832.

[11] 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.

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

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

[14] N. A. Carella. *The Error Term of the Summatory Euler Phi Function.* http://arxiv.org/abs/1206.2792.

[15] N. A. Carella. *Primitive Roots In Short Intervals*, http://arxiv.org/abs/1806.01150.

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

[17] Peter J. Cameron and D. A. Preece. *Notes on primitive lambda-roots*, http:www.maths.qmul.ac.ukpjccsgnoteslambda.pdf.

[18] Carmichael, R. D. *Note on a new number theory function*. Bull. Amer. Math. Soc. 16 (1910), no. 5, 232-238.

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

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

[21] N. Costa Pereira. *Estimates for the Chebyshev function $\theta(x)$ and $\psi(x)$,* Math. Comp., 44(169):211-221, 1985.

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

[23] P. Dusart. *Estimates of some functions over primes without R.H.,* http://arxiv.org/abs/1002.0442.

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

[25] 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.

[26] 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.

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

[28] Rainer Dietmann, Christian Elsholtz, Igor E. Shparlinski. *On Gaps Between Primitive Roots in the Hamming Metric*, http://arxiv.org/abs/1207.0842.

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

[30] Erdos, P.; Kac, M. *The Gaussian law of errors in the theory of additive number theoretic functions*. Amer. J. Math. 62, (1940). 738-742.

[31] Euler, Leonhard.*Introduction to analysis of the infinite. Book I.* Translated from the Latin and with an introduction by John D. Blanton. Springer-Verlag, New York, 1988.

[32] Erdos, Paul; Pomerance, Carl; Schmutz, Eric. *Carmichael's lambda function.* Acta Arith. 58 (1991), no. 4, 363-385.

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

[34] Erdos, P.; Turk, J. *Products of integers in short intervals*. Acta Arith. 44 (1984), no. 2, 147-174.

[35] Ford, Kevin. *Zero-free regions for the Riemann zeta function. Number theory for the millennium, II* (Urbana, IL, 2000), 25-56, A K Peters, Natick, MA, 2002.

[36] Friedlander, John; Granville, Andrew. *Limitations to the equi-distribution of primes. IV*. Proc. Roy. Soc. London Ser. A 435 (1991), no. 1893, 197-204.

[37] Friedlander, John; Granville, Andrew. *Limitations to the equi-distribution of primes. I*. Ann. of Math. (2) 129 (1989), no. 2, 363-382.

[38] Friedlander, John B. *Integers free from large and small primes.* Proc. London Math. Soc. (3) 33 (1976), no. 3, 565-576.

[39] Friedlander, J. B.; Lagarias, J. C. *On the distribution in short intervals of integers having no large prime factor*. J. Number Theory 25 (1987), no. 3, 249-273.

[40] Fouvry, E.; Tenenbaum, G. *Entiers sans grand facteur premier en progressions arithmetiques*. Proc. London Math. Soc. (3) 63 (1991), no. 3, 449-494.

[41] S.R. Finch. *Mathematical constants.* Encyclopedia of Mathematics and its Applications 94, (Cambridge University Press, Cambridge, 2003).

[42] Friedlander, John B.; Konyagin, Sergei; Shparlinski, Igor E. *Some doubly exponential sums over $\mathbb{Z}_m$.* Acta Arith. 105, (2002), no. 4, 349-370.

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

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

[45] Martin, Greg. *An asymptotic formula for the number of smooth values of a polynomial.* J. Number Theory 93 (2002), no. 2, 108-182.

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

[47] Granville, Andrew. *Smooth numbers: computational number theory and beyond.* Algorithmic number theory: lattices, number fields, curves and cryptography, 267-323, Math. Sci. Res. Inst. Publ., 44, Cambridge Univ. Press, Cambridge, 2008.

[48] Andrew Granville, Xuancheng Shao. *When does the Bombieri-Vinogradov Theorem hold for a given multiplicative function?* http://arxiv.org/abs/1706.05710.

[49] Andrew Granville, K. Soundararajan. *Sieving and the Erdos-Kac theorem*, http://arxiv.org/abs/math/0606039.

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

[51] Garaev, M. Z. A. A. Karatsuba. *New estimates of double trigonometric sums with exponential functions,* http://arxiv.org/abs/math/0504026.

[52] Granville, Andrew; Soundararajan, K. *A binary additive problem of Erdos and the order of* $2 \bmod p^2$. Ramanujan J. 2 (1998), no. 1-2, 283-298.

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

[54] Hinz, Jurgen G. *Character sums and primitive roots in algebraic number fields*. Monatsh. Math. 95 (1983), no. 4, 275-286.

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

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

[57] Hardy, G. H. Littlewood J.E. *Some problems of Partitio numerorum III: On the expression of a number as a sum of primes.* Acta Math. 44 (1923), No. 1, 1-70.

[58] Harman, Glyn. *Integers without large prime factors in short intervals and arithmetic progressions*. Acta Arith. 91 (1999), no. 3, 279-289.

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

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

[61] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*, 5th ed., Oxford University Press, Oxford, 1979.

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

[63] A.E. Ingham. *On two conjectures in the theory of numbers*. Amer. J. Math., 64 (1942), 313-319.

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

[65] Johnsen, John. *On the distribution of powers in finite fields*. J. Reine Angew. Math. 251 1971 10-19.

[66] 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.

[67] Kurlberg, P. Pomerance, C. *On a problem of Arnold: the average multiplicative order of a given integer.* Algebra and Number Theory, 7 (2013), 981-999.

[68] Landau, Edmund. *Ueber die asymptotischen Werthe einiger zahlentheoretischer Functionen*. Math. Ann. 54 (1901), no. 4, 570-591.

[69] Lichtman, Jared. *Averages of the Mobius function on shifted primes*. http://arxiv.org/abs/2009.08969.

[70] J. P.S. Lay. *Sign changes in Mertens first and second theorems*, http://arxiv.org/abs/1505.03589.

[71] Y. Lamzouri. *A bias in Mertens product formula*, http://arxiv.org/abs/1410.3777v2.

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

[73] Alessandro, Languasco, Alessandro, Zaccagnini. *On the constant in the Mertens product for arithmetic progressions. I.* http://arxiv.org/abs/0706.2807.

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

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

[76] 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.

[77] Muller, Helmut. *On the distribution of the orders of 2(modu) for odd u*. Arch. Math. (Basel) 84 (2005), no. 5, 412-420.

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

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

[80] Greg Martin, Carl Pomerance. *The iterated Carmichael λ-function and the number of cycles of the power generator*. http://arxiv.org/abs/math/0406335.

[81] Moree, Pieter. *Artin's primitive root conjecture -a survey*. http://arxiv.org/abs/math/0412262.

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

[83] 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.

[84] Muller, Thomas W.; Schlage-Puchta, Jan-Christoph. *On the number of primitive λ-roots.* Acta Arith. 115 (2004), no. 3, 217-223.

[85] Murty, M. Ram; Rosen, Michael; Silverman, Joseph H. *Variations on a theme of Romanoff*. Internat. J. Math. 7 (1996), no. 3, 373-391.

[86] Miller, Steven J.; Takloo-Bighash, Ramin. *An invitation to modern number theory*. With a foreword by Peter Sarnak. Princeton University Press, Princeton, NJ, 2006.

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

[88] Ramon M. Nunes. *Square-free numbers in arithmetic progressions,* http://arxiv.org/abs/1402.0684.

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

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

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

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

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

[94] Pintz, Janos. *Landau's problems on primes.* J. Theory. Nombres Bordeaux 21 (2009), no. 2, 357-404.

[95] A. G. Postnikov. *Introduction to analytic number theory*, Translations of Mathematical Monographs, vol. 68, American Mathematical Society, Providence, RI, 1988.

[96] Popa, Dumitru. *A triple Mertens evaluation.* J. Math. Anal. Appl. 444 (2016), no. 1, 464-474.

[97] Redmond, Don. *Number theory. An introduction*. Monographs and Textbooks in Pure and Applied Mathematics, 201. Marcel Dekker, Inc., New York, 1996.

[98] Rose, H. E. *A course in number theory*. Second edition. Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1994.

[99] Igor Rivin. *Some experiments on Bateman-Horn*, http://arxiv.org/abs/1508.07821.

[100] Rekos, Margorzata. *On some complex explicit formulae connected with the Euler's phi function*. I. Funct. Approx. Comment. Math. 29 (2001), 113-124.

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

[102] T. Reuss. *Pairs of k-free Numbers, consecutive square-full Numbers*. http://arxiv.org/abs/1212.3150.

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

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

[105] Schoenfeld, Lowell. *Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II.* Math.Comp. 30 (1976), no. 134, 337-360.

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

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

[108] 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.

[109] Sitaramachandra Rao, R. *On an error term of Landau*. Indian J. Pure Appl. Math. 13 (1982), no. 8, 882-885.

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

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

[112] Gerald Tenenbaum. *Generalized Mertens sums* http://arxiv.org/abs/1910.02781.

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

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

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

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

[117] Mark B. Villarino. *Mertens' Proof of Mertens' Theorem*, http://arxiv.org/abs/math/0504289.

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

[119] von zur Gathen, Joachim; Knopfmacher, Arnold; Luca, Florian; Lucht, Lutz G.; Shparlinski, Igor E. *Average order in cyclic groups*. J. Theor. Nombres Bordeaux 16 (2004), no. 1, 107-123.

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

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

output.tex.