Elementary and Analytic Methods in Number Theory

Daniel Sutantyo

This thesis is presented for the degree of

Master of Science

Centre for Advanced Computing, Algorithms and Cryptography

Department of Computing

Division of Information and Communication Sciences

Macquarie University

August 2007

DECLARATION

This thesis is submitted in fulfilment of the requirements of the degree of Master of Science at Macquarie University and has not been submitted for a higher degree to any other university or institution.

This thesis represents my original work and contributions. I certify that to the best of my knowledge, all sources and assistance received in the preparation of this thesis have been acknowledged.

Daniel Sutantyo

INTRODUCTION

In defiance of Hardy's famous words, number theory has been a continuous source of inspiration for many applications in computer science and cryptography. Unfortunately, algorithms based on number theory are often treated as a kind of black box where the understanding of the underlying mathematics is secondary to the actual application of the algorithm.

The author himself came from a computer science background, and the writing of this thesis was motivated by the desire to learn more about the principles of number theory. It is a compilation of various topics in number theory which were encountered during the author's course of study, particularly in the area of analytic number theory.

The thesis begins with a review of arithmetic functions and modular arithmetics in the first two chapters, which are of course the basic building blocks for any study in number theory. Indeed, these topics are a routine part of any standard literature on number theory, therefore the materials are presented in a rather informal manner at a brisk pace.

Once these pre-requisites have been addressed, we continue with a discussion of several research topics in number theory, as naturally it is the aim of this study to apply these principles and techniques in answering some questions in number theory. We outline the topic of the remaining chapters as follows:

Chapter 3 of the thesis is an investigation of the average divisor function $A(n)$, de-

fined by

$$A(n) = \frac{\sigma(n)}{\tau(n)}$$

where $\sigma(n)$ is the sum of divisors function and $\tau(n)$ is the number of divisors function. Our main motivation was the recent paper by Arnold [Arn05] which conjectured that

$$A(n) \sim \frac{n}{\log n},$$

which unfortunately is incorrect. It is therefore beneficial to discuss the proper method in deriving the correct result, and in this chapter we use an elementary approach to show that

$$A(n) \sim \frac{n}{\sqrt{\log n}}.$$

Chapter 4 is based on a paper authored together with I. Shparlinski [SS07] where we looked at the set of the largest prime divisors of several sequences. Formally, if we let $P(n)$ to be the largest prime divisor of an integer n, then given a sequence

$$\mathcal{A} = \big(a(n)\big)_{n=1}^{\infty},$$

we are interested with the set

$$\mathcal{S}_{\mathcal{A}}(x) = \big\{P\big(a(n)\big) : n \le x\big\}$$

for some real x. In particular, we are interested with the cardinality of this set, and we present a method to derive a lower bound of this set for various sequences, including for polynomial and linear recurrent sequences.

The final topic of the thesis is a derivation of an upper bound for

$$\sum_{n \le x} \chi\big(a + P(n)\big) \tag{1}$$

where χ is a Dirichlet character and $P(n)$ is as defined earlier, with integers a and n. Sums of this type is referred to as character sums, and before we come to the derivation of the bound for this sum, we first outline the two important concepts behind such sum; namely

that of Dirichlet characters in Chapter 5 and of exponential sums in Chapter 6.

The upper bound itself is derived in Chapter 7, where we show that for integers a and $q \geq 1$ with $(a, q) = 1$,

$$\left| \sum_{n \leq x} \chi\big(a + P(n)\big) \right| \ll x \left(\frac{q^{o(1)} \log^5 x}{q^{1/4}} + w^{-2w/3 + o(w)} \right)$$

with $w = (\log x)/(\log q)$. This chapter was based on a joint work with S. Balasuriya and I. Shparlinski [BSSar].

CONTENTS

LIST OF NOTATION

Basic notation

$\mathbb{N}$	The set of positive integers
$\mathbb{Q}$	The set of rational numbers
$\mathbb{R}$	The set of real numbers
$\mathbb{C}$	The set of complex numbers
$\mathbb{Z}$	The set of integers
$\mathbb{Z}/m\mathbb{Z}$	The residue class modulo m
$\ll, \gg$	The Vinogradov symbols
(m, n)	The greatest common divisor of m and n
$(a\|p)$	The Legendre symbol
$\#\mathcal{A}$	The cardinality of set $\mathcal{A}$

Arithmetic functions

$[x]$	The integer part of x
$\{x\}$	The fractional part of x
$\varphi(n)$	Euler function
$\mu(n)$	Möbius function
$\tau(n)$	The number of divisors function
$\sigma(n)$	The sum of divisors function
$\chi(n)$	Dirichlet character
$\pi(x)$	Prime counting function
$\psi(x,y)$	The set of y-smooth integers smaller than x
$P(n)$	The largest prime divisor of n

The letter p is reserved exclusively to denote a prime integer, and we write

$$\sum_{p\leq x} f(p) \qquad \text{and} \qquad \prod_{p\leq x} f(p)$$

respectively to denote sums and products of a function f over all prime values less than or equal to x.

CHAPTER 1

ARITHMETIC FUNCTIONS

In this chapter we review the basic principles of arithmetic functions, followed with discussions of several fundamental arithmetic functions and other related concepts such as Dirichlet convolution and Dirichlet series.

1.1. INTRODUCTION TO ARITHMETIC FUNCTIONS

An *arithmetic function* f is a real or complex-valued function defined on the set of natural numbers, or equivalently, it is a sequence of real or complex numbers. Indeed, in number theory we are often concerned with the study of these sequences, as they inform us on the different properties of the set of integers.

We call an arithmetic function f *additive* if for integers m and n,

$$f(m) + f(n) = f(mn)$$

whenever $(m, n) = 1$, and *multiplicative* if

$$f(m)f(n) = f(mn)$$

whenever $(m, n) = 1$. If the property holds for all m and n regardless of their greatest common divisor, then we call f to be *completely additive* and *completely multiplicative*, respectively.

Additive and multiplicative functions play an important role in number theory because they reflect the multiplicative structure of integers. For example, if $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then

$$f(n) = \sum_{i=1}^{k} f\left(p_i^{\alpha_i}\right), \qquad \text{and} \qquad f(n) = \prod_{i=1}^{k} f\left(p_i^{\alpha_i}\right),$$

for additive and multiplicative functions f, respectively.

In the case of multiplicative functions, this correspondence with the multiplicative structure of integers provide some useful results in studying sums of these functions. In particular, we often encounter sums of a function extended over the divisors of an integer, i.e.

$$\sum_{d|n} f(d), \tag{1.1}$$

and when f is a multiplicative function, we have

$$\sum_{d|n} f(d) = \prod_{i=1}^{k} \Big(1 + f\left(p_i\right) + f\left(p_i^2\right) + \cdots + f\left(p_i^{\alpha_i}\right)\Big). \tag{1.2}$$

It is often the case that decomposing the sum in this manner allows it to be evaluated more easily.

Another useful result related to sums of multiplicative functions is the *Möbius inversion formula*, where for $n \geq 1$ and multiplicative functions f and g,

$$g(n) = \sum_{d|n} f(d) \tag{1.3}$$

if and only if

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right), \tag{1.4}$$

where μ is the Möbius function (see section 1.1.2). The proof can be obtained by substituting one equation into the other.

We are also interested with sums of the form

$$\sum_{n \leq x} f(n)$$

for a given real x. The Möbius inversion formula in this case can be extended to

$$G(x) = \sum_{n \leq x} F\left(\frac{x}{n}\right)$$

if and only if

$$F(x) = \sum_{n \leq x} \mu(n) G\left(\frac{x}{n}\right),$$

where F and G are multiplicative functions defined for all $n \geq 1$.

We continue the discussion by looking at some important arithmetic functions in number theory.

1.1.1 THE FUNCTIONS $[x]$ AND $\{x\}$

For any real number x, we use $[x]$ to denote the *integral part* of x, which is the largest integer n with $n \leq x$, while $\{x\} = x - [x]$ is the *fractional part of* x. In a strict manner, these two functions are not arithmetic functions as x does not have to be a natural number, but it is hard to argue against the ubiquity of these functions in number theory.

For a real x and an integer n, $[x/n]$ gives the number of times n divides into x, or more generally

$$\left[\sqrt[m]{\frac{x}{n}}\right]$$

is the number of integers in the form nk^m for some integer k, which are less than or equal to x.

The integer function in particular is essential in formulas involving counting *lattice points* (points with integer coordinates) under a curve, since for a real-valued function f,

$$\sum_{a<x\leq b} [f(x)]$$

is the number of lattice points under the curve $y = f(x)$. For example, inside the circle $x^2 + y^2 = r^2$ there are

$$1 + 4[r] + 8 + \sum_{0<x\leq \frac{r}{\sqrt{2}}} \left[\sqrt{r^2 - x^2}\right] - 4\left[\frac{r}{\sqrt{2}}\right]^2$$

lattice points.

1.1.2 THE MÖBIUS FUNCTION

The Möbius function is defined by

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n \text{ is square-free,} \\ 0 & \text{otherwise,} \end{cases}$$

where k is the number of prime divisors of n (with $\mu(1) = 1$). It is trivial to show that the Möbius function is multiplicative, and so it follows from (1.2) that

$$\sum_{d|n} \mu(d) = \big(1 + \mu(p_1)\big)\big(1 + \mu(p_2)\big) \cdots \big(1 + \mu(p_k)\big),$$

and since $\mu(p) = -1$, we have the fundamental identity

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{when } n = 1, \\ 0 & \text{otherwise.} \end{cases} \tag{1.5}$$

The above identity is central behind the principle of *inclusion and exclusion*: Let $c_1, c_2, \ldots, c_m$ be a sequence of real or complex numbers corresponding to the positive integers $\delta_1, \delta_2, \ldots, \delta_m$, and C be the sum of c_i when $\delta_i = 1$, that is,

$$C = c_1 \sum_{d|\delta_1} \mu(d) + c_2 \sum_{d|\delta_2} \mu(d) + \cdots + c_m \sum_{d|\delta_m} \mu(d).$$

If we expand the sum and then collect the values of c_i which share the same divisor d, we have

$$C = \sum_{d} \mu(d) C(d)$$

where d runs over all the divisors of $\delta_1, \delta_2, \cdots, \delta_m$, and $C(d)$ is the sum of the values of c_i whose corresponding δ_i is divisible by d.

For example, let

$$g(n) = \sum_{d|n} f(d)$$

and let $\{\delta_1 = 1, \delta_2, \ldots, \delta_k = n\}$ be the divisors of n. By the inclusion- exclusion principle, we can write

$$f(n) = f\left(\frac{n}{\delta_1}\right) \sum_{d|\delta_1} \mu(d) + f\left(\frac{n}{\delta_2}\right) \sum_{d|\delta_2} \mu(d) + \cdots + f\left(\frac{n}{\delta_k}\right) \sum_{d|\delta_k} \mu(d),$$

since only the first term is non-zero. The values of δ_i are divisors of n, therefore for a given

d we have

$$f(n) = \sum_{d|n} \mu(d) C_f(d)$$

where $C_f(d)$ is the sum of $f(n/\delta_i)$ when $d \mid \delta_i$, i.e.

$$C_f(d) = \sum_{e|\frac{n}{d}} f\left(\frac{n}{de}\right) = g\left(\frac{n}{d}\right).$$

Hence,

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right),$$

thus proving one part of the Möbius inversion formula.

1.1.3 THE EULER FUNCTION

The Euler (totient) function of a positive integer n represents the number of integers $\leq n$ which are coprime to n. It is a function of major importance in the study of congruences, as we shall see in the next chapter.

For primes p, it is clear that

$$\varphi(p) = p - 1.$$

For non-primes $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, there are

$$n_1 = n\left(1 - \frac{1}{p_1}\right)$$

numbers smaller than n which are coprime to p_1. Of these, a further

$$n_2 = n_1\left(1 - \frac{1}{p_2}\right)$$

are not divisible by p_2 as well. Continuing this argument, we have

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right).$$

We can use the inclusion-exclusion principle from the previous section to derive a particularly important identity involving Euler function: We have

$$\begin{aligned}\varphi(n) &= \sum_{d|(1,n)} \mu(d) + \sum_{d|(2,n)} \mu(d) + \cdots + \sum_{d|(n,n)} \mu(d) \\ &= \sum_{d|n} \mu(d) \sum_{k=1}^{n/d} 1.\end{aligned}$$

Hence,

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d},$$

and applying Möbius inversion formula gives us

$$n = \sum_{d|n} \varphi(d),$$

which is an important identity in number theory.

1.1.4 LIOUVILLE'S FUNCTION

Liouville's function λ for $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ is defined by

$$\lambda(n) = (-1)^{\alpha_1+\alpha_2+\cdots+\alpha_k},$$

with $\lambda(1) = 1$. It informs us about the parity of the number of prime divisors of n, counting multiplicity, and it is a completely multiplicative function.

If we consider the sum over integer divisors, then from (1.2) we have

$$\sum_{d|n} \lambda(d) = \prod_{i=1}^{k} \left(1 + \lambda\left(p_i\right) + \lambda\left(p_i^2\right) + \cdots + \lambda\left(p_i^{\alpha_i}\right)\right)$$

and unless n is a square, the sum on the right hand side is zero for at least one of the prime divisors, hence

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{if } n \text{ is a square,} \\ 0 & \text{otherwise.} \end{cases}$$

1.1.5 THE VON MANGOLDT FUNCTION

The von Mangoldt function is defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^m \text{ for some integer } n \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

The von Mangoldt function is neither multiplicative nor additive, but it plays a central role in the study of the distribution of prime numbers.

One important identity involving the von Mangoldt function is

$$\log n = \sum_{d|n} \Lambda(d)$$

for $n \geq 1$. To derive this, we see that if $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then for a given d, $\Lambda(d)$ either contributes $\alpha_i \log p_i$ if d is a prime power of p_i, or it disappears when d is a product of two or more primes. Therefore

$$\sum_{d|n} \Lambda(d) = \sum_{i=1}^{k} \alpha_i \log p_i = \log n.$$

1.1.6 THE CHEBYSHEV'S FUNCTIONS

The functions defined by

$$\psi(x) = \sum_{n \leq x} \Lambda(n) \text{ and } \vartheta(n) = \sum_{p \leq x} \log p$$

are referred to as the Chebyshev's ψ-function and ϑ-function, respectively.

We only briefly mention Chebyshev and von Mangoldt functions here, but they are nevertheless very important in the derivation of the analytic proof for the prime number theorem.

1.1.7 THE PRIME NUMBER THEOREM

The prime-counting function $\pi(x)$ counts the number of prime numbers less than or equal to x, and the *prime number theorem* states that

$$\pi(x) \sim \frac{x}{\log x}.$$

The prime number theorem is perhaps the most celebrated result in number theory, and it is crucial for many parts of this thesis, as well as for number theory in general.

We refer the reader to Chapter 13 of [Apo00] for an analytic proof of the prime number theorem.

1.2. THE ORDER OF ARITHMETIC FUNCTIONS

In studying arithmetic functions, we are interested with the *order* or the rate of growth of the functions in question.

One method in measuring the rate of growth is to consider the *maximal order* or the upper bound of the function. For this purpose, we repeat the use of the *big O* notation, where for two arithmetic functions f and g, we write

$$f(n) = O\big(g(n)\big)$$

if there is a constant k such that $|f(n)| \leq kg(n)$ for all sufficiently large n. We also use Vinogradov symbol, $f(n) \ll g(n)$ and $g(n) \gg f(n)$ to express the same relation. Conversely, the *little o* notation

$$f(n) = o\big(g(n)\big)$$

is used to signify that f is asymptotically negligible when compared to g.

The other method is to look at the *average order* of a function, that is, we describe the behaviour of the function being investigated in terms of another function which closely

approximates it. We write

$$\sum_{n\leq x} f(n) \sim \sum_{n\leq x} g(n).$$

if g is the average order of f, or equivalently we can consider the arithmetic mean of f,

$$\frac{1}{n}\sum_{n\leq x} f(n).$$

The average order is useful when the behaviour of the arithmetic function is erratic, since the fluctuation in the values taken is smoothed out as n grows asymptotically, and so it tells us about the typical behaviour of the function.

1.3. SUMMATION TECHNIQUES

Summation formulas allow us to describe the asymptotic behaviour of a function from our knowledge about the behaviour of another arithmetic function. The most commonly used method is *partial summation*, which in a way is a discrete version of integration by parts: If a and f are arithmetic functions, with

$$A(x) = \sum_{n=1}^{x} a(n),$$

then we can write

$$\sum_{n=m}^{x} a(n)f(n) = A(x)f(x) - A(m-1)f(m) + \sum_{n=m}^{x-1} A(n)\left(f(n) - f(n+1)\right).$$

Introducing integrals give us the analytic version:

$$\sum_{n=m}^{x} a(n)f(n) = A(x)f(x) - \int_1^x A(u)f'(u)du.$$

Another important summation technique is Euler's summation formula:

$$\sum_{y<n\leq x} f(n) = \int_y^x f(t)dt + \int_y^x \big(t - \lfloor t\rfloor\big)f'(t)dt + f(x)\big(\lfloor x\rfloor - x\big) - f(y)\big(\lfloor y\rfloor - y\big).$$

where f is a function that is continuously differentiable on $[x, y]$ with $0 < x < y$. For the proofs of these summation formulas, we refer the reader to [MTB06].

1.4. DIRICHLET PRODUCT

As we have seen in the preceding sections, we often see sums which are extended over the divisors of an integer. These sums can be generalised to the form

$$\sum_{d|n} f(d) g\left(\frac{n}{d}\right), \tag{1.6}$$

where f and g are arithmetic functions. This type of sum is known as the *Dirichlet product* (or *Dirichlet convolution*) of f and g, and we write

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right),$$

to signify this relationship. If both f and g are multiplicative, then so is $f * g$.

Along with the addition operator, the set of all arithmetic functions forms a commutative ring. The identity with respect to addition is the function $f(n) = 0$, for all positive n, and so the additive inverse of a given function can be deduced trivially.

The identity with respect to the product operation is the function

$$I(n) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases} \tag{1.7}$$

The function I is identical to the identity (1.5) in subsection 1.1.2, and we can write

$$I(n) = \mu * e = \sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

where $e(n) = 1$ for all n.

To show that I is indeed the identity under product operation, we have

$$(f * I)(n) = \sum_{d|n} f(d) I\left(\frac{n}{d}\right) = \sum_{d|n} f(d) \left[\frac{d}{n}\right] = f(n)$$

since $[d/n] = 0$ when $d < n$. If for a given multiplicative function f we have $f(1) \neq 0$, then there exists a unique multiplicative inverse f^{-1}, such that

$$f * f^{-1} = I$$

with $f^{-1} = 1/f(1)$, and by induction we have,

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d),$$

for $n > 1$. Therefore every multiplicative function is a multiplicative unit in this ring, and in fact if f is completely multiplicative, then

$$f^{-1}(n) = \mu(n) f(n).$$

The introduction of an algebraic structure into the set of arithmetic functions allow us to use techniques from algebra in our work. For example, we could write the Möbius inversion formula (1.3) as:

$$f = g * e$$

and using the fact that $\mu * e = I$,

$$f * \mu = g * e * \mu = g * I = g$$

therefore $g = f * \mu$. The converse can be deduced in the same manner.

1.5. FORMAL DIRICHLET SERIES

The concept of *Dirichlet series* is an important tool in the study of arithmetic functions, and we conclude this chapter with a brief discussion on this topic.

The formal Dirichlet series of an arithmetic function f is the series

$$D(f,s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

where s is a complex number. The addition and product operator from the previous section allow us to define the sum and product of two formal Dirichlet series as

$$D(f,s) + D(g,s) = \sum_{n=1}^{\infty} \frac{f(n)+g(n)}{n^s}$$

and

$$D(f,s)D(g,s) = \sum_{n=1}^{\infty} \frac{h(n)}{n^s}$$

where $h = f * g$ is the Dirichlet product of f and g. The set of all formal Dirichlet series along with the addition and product operation also form a commutative ring, where the product identity given by the series

$$D(I,s) = \sum_{n=1}^{\infty} \frac{I(n)}{n^s}$$

with $I(n)$ as defined by (1.7).

One important identity involving zeta function is the Euler's product: We have

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} \left(1 + f(p) + f(p^2) + \cdots\right),$$

and so with $f(n) = 1/n^s$,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right),$$

which is just a geometric sum, hence

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}.$$

If f is a multiplicative function, then we can generalise the form above to

$$D(f,s) = \prod_p \left(\sum_{m=0}^{\infty} \frac{f(p^m)}{p^{ms}}\right).$$

The two most important series are of course the Dirichlet L-series,

$$D(\chi,s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

where $\chi(n)$ is a Dirichlet character, and the zeta function

$$\zeta(s) = D(1,s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

This thesis will not delve too deeply into the topics of Dirichlet series, but the discussion here should provide the necessary background for later chapters.

CHAPTER 2

THEORY OF CONGRUENCES

In this chapter, we discuss the topic of modular mathematics, starting with linear and polynomial congruences and followed by the topics of quadratic residues and primitive roots.

We assume that the reader is well-acquainted with divisibility theory and some basic results involving prime numbers. We continue the style of presentation adopted in the previous chapter.

2.1. BASIC DEFINITIONS

For integers a, b, and m, we say that a is congruent to b modulo m and we write

$$a \equiv b \pmod{m}$$

to signify that (equivalently):

- $a = b + mt$ for some integer t
- $m \mid (a - b)$

with $0 \leq b < m$, and we call b the *residue* of a modulo m. We can then group integers which are congruent to one another to form a set of *residue classes*, essentially partitioning the set of integers according to their remainders upon division by the modulus m.

The infinitude of integers is therefore reduced to a finite number of residue classes, and this provides us with a powerful tool in the studying integers. It is precisely for this reason that the theory of congruences is considered as one of the most elegant invention in number theory.

To state this formally, we write $\hat{a}$ to represent the residue class containing integers which are congruent to a modulo m, that is,

$$\hat{a} = \{x : x = a + qm, \;\; q = 0, \pm 1, \pm 2, \ldots\},$$

where $0 \leq a < m$. In practice however, if a result involving congruences applies to a, then it naturally applies to all elements in the residue class $\hat{a}$, so for most of our purposes a and $\hat{a}$ are interchangeable.

If we have a set of residue classes represented by $1, 2, \ldots, m$, then we have a *complete residue system* modulo m, and we write $\mathbb{Z}/m\mathbb{Z}$ to denote this. In contrast, a *reduced residue system* modulo m is the set of residue classes which are relatively prime to m (of which there are $\varphi(m)$ classes), and we write $(\mathbb{Z}/m\mathbb{Z})^*$ to represent this system.

2.2. LINEAR CONGRUENCES

We now consider the simplest case of congruences involving polynomials, that is, linear congruences of the form

$$ax \equiv b \pmod{m} \tag{2.1}$$

where a and b are integers.

Since $ax \equiv b \pmod{m}$ implies that $ax - qm = b$ for some integer q, then a solution to exists if and only if $(a, m) \mid b$. In particular if $(a, m) = 1$, then a solution always exists since we can write (Bézout's identity):

$$ar + qm = 1$$

for integers r and q, and upon multiplication with b and taking modulo m, we have

$$arb \equiv b \pmod{m},$$

giving $x \equiv rb \pmod{m}$ as a solution. This solution is unique since $ax_1 \equiv ax_2 \pmod{m}$ implies that $a(x_1 - x_2) \equiv 0 \pmod{m}$, so for non-zero a, it must be the case that $x_1 \equiv x_2 \pmod{m}$.

One consequence of the uniqueness of the solution when $(a, m) = 1$ is that if x runs over the reduced residue system modulo m, then ax also runs over the same reduced residue system. Therefore if $x_1, x_2, \ldots, x_{\varphi(m)}$ are the values of the reduced residue system modulo m, then

$$x_1 x_2 \cdots x_{\varphi(m)} \equiv a x_1 a x_2 \cdots a x_{\varphi(m)} \equiv a^{\varphi(m)} x_1 x_2 \cdots x_{\varphi(m)} \pmod{m},$$

leading to the celebrated Fermat-Euler's theorem:

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

or the more specific Fermat's little theorem:

$$a^{p-1} \equiv 1 \pmod{p}$$

where p is a prime.

On the other hand if $(a, m) = d > 1$, then there exists d solutions, since if $x \equiv c \pmod{m/d}$ is a unique solution to

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}, \tag{2.2}$$

then this solution also satisfies $ax \equiv b \pmod{m}$, and within the complete residue system modulo m, there are d values congruent to $c \pmod{m/d}$, namely

$$c, c + \frac{m}{d}, c + \frac{2m}{d}, \ldots, c + \frac{(d-1)m}{d}.$$

Therefore, the problem is reduced down to the case where $(a, m) = 1$.

By the *Chinese remainder theorem* we can also write the congruence

$$ax \equiv b \pmod{m}, \tag{2.3}$$

with $(a, m) = 1$ and m composite, as a series of n linear congruences

$$\begin{aligned} ax &\equiv b \pmod{m_1} \\ ax &\equiv b \pmod{m_2} \\ &\vdots \\ ax &\equiv b \pmod{m_n} \end{aligned} \tag{2.4}$$

where $m = m_1 m_2 \cdots m_n$ and $(m_i, m_j) = 1$ for any $i, j < n$. Suppose these series of congru-

ences can be solved and we have the series of solutions

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_n \pmod{m_n}, \end{aligned} \tag{2.5}$$

then these congruences have exactly one solution modulo m, namely

$$x = c_1 M_1 M_1' + c_2 M_2 M_2' + \cdots + c_n M_n M_n',$$

where $M_i = m/m_i$, and M_i' is chosen such that $M_i M_i' \equiv 1 \pmod{m_i}$.

2.3. General Polynomial Congruences

In the previous section we have given an overview of linear congruences, while the special case of quadratic polynomials will be discussed in the next section. For now, we generalise to polynomial congruences of an arbitrary degree $n \geq 1$, that is we look at congruences of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{m}$$

where the coefficients are integers in $\mathbb{Z}/m\mathbb{Z}$.

The study of polynomial congruences with higher order degrees is the driving force behind algebraic number theory, and although we do not intend to examine the topic too deeply, we need to mention some important results which are required in later parts.

We start by noting the distinction between polynomial congruences and the more general congruences: Two polynomials f and g are congruent to each other modulo m, and we write

$$f(x) \cong g(x) \pmod{m},$$

if and only if all the coefficients are congruent modulo m. The difference is slight, and

many properties of ordinary congruences are still preserved, but we note that if $f(x) \cong g(x) \pmod{m}$ then $f(x) \equiv g(x) \pmod{m}$ for all x, while the converse is not necessarily true.

Furthermore, a function is said to be *periodic* with period k modulo m if

$$f(x+k) = f(k) \pmod{m}$$

with the smallest positive period being referred to as the *fundamental period*.

2.3.1 LAGRANGE'S THEOREM

The study of polynomial congruences is in most cases analogous to the study of polynomial equations in general algebra, with some results such as the remainder theorem still applying in polynomial congruences. Unfortunately we do not have the equivalent to the fundamental theorem of algebra, which states that a polynomial of degree $n \geq 1$ has n complex roots.

However, we do have a theorem by Lagrange which is an analog of the fundamental theorem of algebra, even though it only applies for prime moduli. *Lagrange's theorem* states that a polynomial of degree $n \geq 1$ with integer coefficients has at most n solutions (counting multiplicities). We give a quick illustration of the proof as follows:

Let $k_1, k_2, \ldots, k_r$ be distinct solutions for $f(x) \equiv 0 \pmod{p}$, where f is a polynomial of degree n, and assume for now that f does not have any multiple roots. We can write

$$f(x) \cong (x - k_1)g(x) \pmod{p}$$

where g is a polynomial of degree $n-1$. Since $f(k_2)$ is also a root of f,

$$f(k_2) \equiv (k_2 - k_1)g(k_2) \equiv 0 \pmod{p},$$

and therefore $g(k_2) \equiv 0$, implying that k_2 is a root of $g(x)$. If we continue this inductive

process, then we have

$$f(x) \cong (x-k_1)(x-k_2)\cdots(x-k_r)g_r(x) \pmod{p}$$

where g_r is a polynomial of degree $n-r$, and $g_r(k_i) \not\equiv 0$ for $1 \leq i \leq r$. Therefore the number of solutions, namely r, can at most be equal to n. The proof only requires small adjustments if f has multiple roots.

2.3.2 HENSEL LIFTING

Even though Lagrange's theorem tells us about the number of solutions for a polynomial with prime modulo, we have not discussed the actual method for finding the roots of this polynomial, nor do we intend to, as this topic is beyond the scope of the thesis.

However, we note that in order to solve a polynomial with composite modulo, we can extend Chinese remainder theorem as follows: The congruence

$$f(x) \equiv 0 \pmod{m}$$

have a solution if and only if there is a solution for each of the congruences

$$\begin{aligned} f(x) &\equiv 0 \pmod{p_1^{\alpha_1}} \\ f(x) &\equiv 0 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ f(x) &\equiv 0 \pmod{p_r^{\alpha_r}}, \end{aligned}$$

with $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$.

Therefore, the problem is essentially reduced to finding solutions to polynomial congruences with a prime power modulus:

$$f(x) \equiv 0 \pmod{p^{\alpha}}. \tag{2.6}$$

If a solution satisfies the congruence (2.6) then clearly it must also satisfies the congruence

$$f(x) \equiv 0 \pmod{p^\beta} \tag{2.7}$$

for all $\beta < \alpha$. In particular, it must satisfy the congruence modulo $p^{\alpha-1}$, therefore if a is a solution to (2.6), then

$$a = qp^{\alpha-1} + r$$

for some integers q and r with $0 \leq r < p^{\alpha-1}$, and since $a \equiv r \pmod{p^{\alpha-1}}$, r is a solution modulo $p^{\alpha-1}$.

Conversely, if we know one such r, then we can work backwards to find a, with a method known as *Hensel lifting*: From Taylor's theorem we have

$$f(x+h) = f(x) + f'(x)h + \frac{1}{2!}f''(x)h^2 + \cdots .$$

Applying this to our congruence, we have

$$f(a) = f(qp^{\alpha-1} + r) \equiv f(r) + f'(r)qp^{\alpha-1} \pmod{p^\alpha}.$$

Since r is a solution modulo $p^{\alpha-1}$, $f(r) = kp^{\alpha-1}$ for some integer k, and we write

$$f(a) \equiv \left(k + qf'(r)\right) p^{\alpha-1} \pmod{p^\alpha}.$$

Therefore, whether or not a is a solution depends on q satisfying the linear congruence

$$k + qf'(r) \equiv 0 \pmod{p}.$$

If $f'(r) \not\equiv 0 \pmod{p}$, then there is a unique solution for q. On the other hand, if $f'(r) \equiv 0 \pmod{p}$, then either $p \nmid k$, in which case there is no solution, or $p \mid k$, in which case there are p solutions for q. It follows that polynomial congruences with composite moduli may have a lot of solutions, and Lagrange's theorem certainly no longer applies in this case.

2.4. QUADRATIC RESIDUES

We now consider the special case of quadratic polynomial congruences

$$x^2 \equiv a \pmod{p}$$

where p is an odd prime and $a \not\equiv 0 \pmod{p}$. If the above congruence has a solution, then a is a *quadratic residue* modulo p, otherwise it is a *quadratic non-residue* modulo p.

If a is a quadratic residue modulo p, then there are two solutions to the above congruence since $(p-k)^2 \equiv k^2 \pmod{p}$, therefore a given residue system modulo p has a total of $(p-1)/2$ quadratic residues belonging to the classes

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

Indeed if $k^2 \equiv l^2 \pmod{p}$ with $0 < k < l \leq (p-1)/2$, then we have

$$(k-l)(k+l) \equiv 0 \pmod{p},$$

and since $1 < k+l < p$, it must be the case that $k = l$. In the same manner, we can write

$$\left(a^{(p-1)/2} - 1\right)\left(a^{(p-1)/2} + 1\right) \equiv 0 \pmod{p},$$

and so either

$$a^{(p-1)/2} \equiv 1 \pmod{p} \tag{2.8}$$

or

$$a^{(p-1)/2} \equiv -1 \pmod{p}. \tag{2.9}$$

A solution a cannot satisfy both congruences (2.8) and (2.9), because this implies that p divides

$$\left(a^{(p-1)/2} + 1\right) - \left(a^{(p-1)/2} - 1\right) = 2.$$

If a is a quadratic residue, then by Fermat's little theorem, a also satisfies the congruence

(2.8), and since there are $(p-1)/2$ quadratic residues, due to Lagrange's theorem, the quadratic residues exhaust all the solutions to the congruence (2.8). Therefore it must be the case that all the non-residues satisfy the congruence (2.9).

One helpful notation involving quadratic residues is the *Legendre symbol*, defined by

$$(a|p) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ 0 & \text{if } p \mid n, \\ -1 & \text{if } a \text{ is not a quadratic residue mod } p. \end{cases}$$

Following from congruences (2.8) and (2.9) and the relation we showed above, we have

$$(a|p) \equiv a^{(p-1)/2} \pmod{p},$$

an identity referred to as the *Euler's criterion*.

Euler's criterion provides a method for computing $(a|p)$ if p is fixed. Conversely given a, we can find p such that a is a quadratic residue using the *quadratic reciprocity law*:

$$(p|q)(q|p) = (-1)^{(p-1)(q-1)/4}$$

where p and q are distinct odd primes.

We can generalise the Legendre symbol to the Jacobi symbol:

$$(a|P) = \prod_{i=1}^{n} (a|p_i)^{\alpha_i}$$

where $P = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ and $(a|p_i)$ is the Legendre symbol. The quadratic reciprocity law can then be extended to the more general case:

$$(P|Q)(Q|P) = (-1)^{(P-1)(Q-1)/4}$$

where P and Q are odd integers with $(P, Q) = 1$. We refer the reader to Chapter V of [Vin54] for the proof of the quadratic reciprocity law.

2.5. PRIMITIVE ROOTS

The Fermat-Euler theorem tells us that

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

However, there may exist an integer $\omega < \varphi(m)$, such that $a^{\omega} \equiv 1 \pmod{m}$. The smallest such integer ω satisfying this property is called the *exponent* of a modulo m. If $\omega = \varphi(m)$ for a given a, then we say that a is a *primitive root* modulo m.

If ω is the exponent of a modulo m, then the positive powers

$$a, a^2, a^3, \ldots, a^{\omega-1}$$

are incongruent modulo m to each other, otherwise if $a^i \equiv a^j \pmod{m}$ with $i < j < \omega$, then $a^{j-i} \equiv 1 \pmod{m}$, thus contradicting the definition of an exponent. Therefore, if a is a primitive root, then the powers of a generate the whole residue system modulo p (except for the zero residue), with the even powers being the quadratic residues.

Furthermore, we have

$$a^i \equiv a^j \pmod{m}$$

if and only if $i \equiv j \pmod{\omega}$ because for integers q and r,

$$1 \equiv a^{j-i} \equiv a^{q\omega+r} \equiv a^r \pmod{m},$$

so it follows that r is equal to zero and that $i \equiv j \pmod{\omega}$. In particular, we have $\omega \mid \varphi(m)$.

2.5.1 EXISTENCE OF PRIMITIVE ROOTS MODULO p

It is not yet clear which moduli have primitive roots, and we now discuss their existence for different moduli. For the rest of the chapter, let p be an odd prime.

If p is an odd prime, then there exist primitive roots modulo p. To show why this is so, we first need the following intermediate results (which applies for any modulo m, not necessarily a prime number): For integers u and v,

(a) If the exponent of a modulo m is uv, then the exponent of a^u modulo m is v.

(b) If the exponent of a modulo m is u and the exponent of b modulo m is v, with $(u, v) = 1$, then the exponent of ab modulo m is uv.

With these two results, we can now prove the existence of primitive roots modulo p as follows: Let the integers

$$\omega_1, \omega_2, \omega_3, \ldots, \omega_{p-1}$$

be the exponents of the elements in the residue system modulo p, and let Ω be the least common multiple of all these exponents.

Given the prime decomposition of $\Omega = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then for each prime in this decomposition, we can find an exponent ω_i, such that $\omega_i = x_{p_s} p_s^{\alpha_s}$ for some constant x_{p_s} and valid values of i and s. Therefore if a_i is the element with the exponent ω_i, we can write

$$a_i^{\omega_i} = a_i^{x_s p_s^{\alpha_s}}.$$

Letting $\widehat{a}_{p_s} = a_i^{x_s}$, by (a) the exponent of $\widehat{a}_{p_s}$ is $p_s^{\alpha_s}$, and in fact we can find one such $\widehat{a}_{p_s}$ for every prime in the decomposition of Ω, and therefore the number

$$\widehat{a} = \widehat{a}_{p_1} \widehat{a}_{p_2} \cdots \widehat{a}_{p_k}$$

has exponent Ω by (b).

Now, the congruence

$$\widehat{a}^{\Omega} \equiv 1 \mod p$$

has $p - 1$ solutions since every element in the residue system is a solution (the exponent of every element is a divisor of Ω), therefore by Lagrange's theorem, $p - 1 \mid \Omega$. On the other

hand, from Fermat's little theorem, we have $\Omega \mid p-1$, and so it follows that $\Omega = p-1$. Therefore, there exists at least one primitive root modulo p.

2.5.2 THE NUMBER OF PRIMITIVE ROOTS MODULO p

From (a) in the preceding section, we see that if the exponent of a is uv, then it is trivial to deduce the exponent of a^u and a^v. We certainly have a much stronger result than this, and in fact if we know the exponent of a, then we can deduce the exponents of all the powers of a.

To see this, suppose that δ is the exponent of a^k for some integer k. By definition δ is the smallest positive integer satisfying

$$a^{k\delta} = 1 \pmod{m}.$$

If ω is the exponent of a, then $\omega \mid k\delta$, and so

$$k\delta \equiv 0 \pmod{\omega}.$$

Letting $d = (\omega, k)$, the above congruence is equivalent to

$$\frac{k\delta}{d} \equiv 0 \left(\mod \frac{\omega}{d}\right).$$

The smallest positive integer satisfying this equation is ω/d, and this is the exponent of a^k. Therefore,

$$\text{exponent of } a^k = \frac{\omega}{d} = \frac{\text{exponent of } a}{(k, \text{exponent of } a)} \tag{2.10}$$

and so given a primitive root a, we can quickly deduce the exponent of each element in the residue class.

Moreover, this result implies that the exponent of any element must be a divisor of $p-1$, and this is the key argument in determining the number of primitive roots for a

prime modulus. Define the set $A(\omega)$ as

$$A(\omega) = \{x : \text{the exponent of } x \text{ is } \omega\},$$

which are disjoint with

$$\sum_{\omega|p-1} \#A(\omega) = p - 1.$$

For a given ω, if a is an element of $A(\omega)$, then a satisfies the congruence

$$a^{\omega} \equiv 1 \pmod{p}, \tag{2.11}$$

and in fact so do a^2, a^3, ..., a^{ω}, which are all distinct. By Lagrange's theorem, these are all the solutions to the congruence (2.11), therefore each number in $A(\omega)$ must be of the form a^k with $k = 1, 2, \ldots, \omega$.

The question now is which powers of a has ω as the exponent, and thus an element of $A(\omega)$? From (2.10), we see that the exponent of a and the exponent of a^k are the same when $(k, \omega) = 1$, or in other words,

$$\#A(\omega) = \varphi(\omega).$$

In particular there are $\varphi(p-1)$ primitive roots modulo p.

2.5.3 Existence of primitive roots modulo p^{α}

The first likely candidate for a primitive root modulo p^{α} for $\alpha \geq 2$ is of course the primitive root modulo p, so let a be the primitive root modulo p and let us investigate this further. Certainly, we have

$$a^{p-1} \not\equiv 1 \pmod{p^2}$$

as a necessary condition for a to be a primitive root modulo p^2.

For some integer T', we have

$$(a+pt)^{p-1} = a^{p-1} + (p-1)a^{p-2}pt + T'p^2,$$

and since $a^{p-1} = 1 + pT$ for some constant T, then

$$\begin{aligned}(a+pt)^{p-1} &= 1 + pT - a^{p-2}pt + T'p^2 \\ &= 1 + p\left(T - a^{p-2}t + T'p\right) \\ &= 1 + pu,\end{aligned}$$

where u runs through the complete residue system modulo p along with t. In particular, we can find a t such that u is not divisible by p, and for this t we can write

$$(a+pt)^{p(p-1)} = (1+pu)^p = 1 + p^2u_2,$$

for some integer u_2. It follows that

$$(a+pt)^{p^2(p-1)} = (1+p^2u_2)^p = 1 + p^3u_3,$$

or more generally, we can find t such that

$$(a+pt)^{p^{r-1}(p-1)} = (1+p^{r-1}u_{r-1})^p = 1 + p^ru_r, \tag{2.12}$$

where the integers $u_2, u_3, \ldots, u_r$ are not divisible by p.

Let ω be the exponent of $(a+pt)$. We know that ω is multiple of $p-1$, and that $\omega \mid \varphi\left(p^\alpha\right) = p^{\alpha-1}(p-1)$, so it must be the case that

$$\omega = p^{r-1}(p-1)$$

where $r = 1, 2, \ldots, \alpha$. We have

$$(a+pt)^{p^{r-1}(p-1)} \equiv 1 \pmod{p^\alpha},$$

and from (2.12),

$$1 + p^r u_r \equiv 1 \pmod{p^\alpha}$$
$$p^r \equiv 0 \pmod{p^\alpha}$$

therefore $r = \alpha$, which means $\omega = \varphi(p^\alpha)$. Hence $(a + pt)$ is a primitive root modulo p^α.

2.5.4 Existence of primitive roots for other moduli

Primitive roots only exist for the moduli

$$1, 2, 4, p^\alpha, \text{and } 2p^\alpha,$$

where p is an odd prime with $\alpha \geq 1$. The first three cases are trivial to show, and the previous sections explained the cases of p and p^α. With a simple argument, we can also deduce the existence of primitive roots modulo $2p^\alpha$.

We first note that an odd primitive root modulo p^α always exist, for if a is a primitive root, then so is $a + p^\alpha$, and only one of them can be even. Let ω be the exponent of a modulo $2p^\alpha$, then we have

$$\omega \mid \varphi(2p^\alpha) = \varphi(p^\alpha).$$

If $a^\omega \equiv 1 \pmod{2p^\alpha}$, then $a^\omega \equiv 1 \pmod{p^\alpha}$, and so

$$\varphi(p^\alpha) = \varphi(2p^\alpha) \mid \omega,$$

therefore a is also a primitive root modulo $2p^\alpha$.

If the modulus m is not of the above form, then for any a which are coprime to the modulus m,

$$a^{\varphi(m)/2} \equiv 1 \pmod{<)F4 > m}$$

and so it follows that there are no primitive roots for these moduli. For the proof, we refer the reader to Chapter 10 of [Apo00]

CHAPTER 3

DISTRIBUTION OF THE AVERAGE DIVISORS

In this chapter, we discuss the asymptotic distribution of the *average divisor* function

$$A(n) = \frac{\sigma(n)}{\tau(n)},$$

where for an integer n, $\sigma(n)$ denotes the sum of the divisors of n, and $\tau(n)$ denotes the number of divisors of n.

The question regarding the distribution of $A(n)$ has recently been investigated in [Arn05] where it was related to the study of some dynamical systems, although unfortunately, the paper gave an incorrect conjecture on the behaviour of the average order of $A(n)$.

We therefore present the proper techniques for the derivation of the average order of $A(n)$, and we show that for some real $x \geq 0$,

$$\sum_{n \leq x} A(n) \sim \frac{x^2}{\sqrt{\log x}}.$$

3.1. INTRODUCTION

The average divisor function is composed of two arithmetic functions, namely the *number of divisors* function and the *sum of divisors* function. We begin with an overview of these functions.

For any positive integer $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, the number of divisors function is defined by

$$\tau(n) = \sum_{d|n} 1 = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1),$$

while the sum of divisors function is defined by

$$\sigma(n) = \sum_{d|n} d = \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \right) \left(\frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \right) \cdots \left(\frac{p_k^{\alpha_k+1} - 1}{p_k - 1} \right).$$

From these definitions, we can immediately see that both functions are multiplicative.

It is a well-known result that

$$\tau(n) \ll n^{\varepsilon}$$

for all $\varepsilon > 0$. However, the values taken by $\tau(n)$ as $n \to \infty$ fluctuates considerably between 2 and a very large number, therefore it is more informative to look at the average order for $\tau(n)$, and it can be shown that

$$\frac{1}{x} \sum_{n \leq x} \tau(n) \sim \log x$$

for all $x \geq 1$.

The fluctuation of values taken by $\sigma(n)$ is much less pronounced, as hinted by the fact that $\sigma(p) = p + 1$, and so on average $\sigma(n)$ is close to n in the order of magnitude. The average order was shown to be

$$\frac{1}{x} \sum_{n \leq x} \sigma(n) \sim cx$$

with $c = \pi^2/12$, with the upper bound being

$$\sigma(n) < n(\log n + 1) = O\left(n^{1+\delta}\right)$$

for all $\delta > 0$. For a thorough discussion of these two functions, we refer the reader to [HW80].

From here, it is natural to question the behaviour of the *average divisor*

$$A(n) = \frac{\sigma(n)}{\tau(n)},$$

which is also a multiplicative function itself. The average divisor function was first considered by O. Ore in [Ore48], where it was introduced along with the *geometric mean* and the *harmonic mean* of the divisors of n. The geometric mean of the divisors of n is defined by

$$G(n) = \left(\prod_{d|n} d\right)^{1/\tau(n)},$$

with $G(n) = \sqrt{n}$ if n is not a square (and with some minor adjustments if n is a square). The harmonic mean is defined by

$$H(n) = \frac{n\tau(n)}{\sigma(n)}.$$

In [Ore48], Ore investigated the integrality of the means for different values of n, but here we will only look at the asymptotic behaviour of $A(n)$.

3.2. INITIAL OBSERVATIONS AND PREVIOUS RESULTS

In studying the behaviour of $A(n)$, we consider only its average order, since it is straightforward to show that

$$\sqrt{n} \leq A(n) \leq \frac{n+1}{2},$$

with $A(n) = (n+1)/2$ if and only if n is a prime. Indeed, it is enough to notice that

$$\frac{n+1}{2} > \frac{d + \frac{n}{d}}{2} \geq \sqrt{n}$$

for any divisor $d \mid n$ with $1 < d < n$.

Furthermore, the behaviour of $A(n)$ is not readily apparent by looking at the distribution of $\tau(n)$ and $\sigma(n)$, as demonstrated by the following values:

n	$\sigma(n)$	$\tau(n)$	$A(n)$
600	1860	24	77.5
601	602	2	301
602	1056	8	132
603	884	6	147.33
604	1064	6	177.33
605	798	6	133
606	1224	8	153
607	608	2	304
608	1260	12	105

In [Arn05], by way of numerical experiments, it was conjectured that

$$A(n) \sim \frac{3n}{2\log n}.$$

However, our numerical calculations showed that $A(n)$ grows asymptotically faster than this, and in fact it was shown by Bateman et al in [BEPS81] that

$$A(n) \sim \frac{cn}{\sqrt{\log n}}.$$

The outline of the proof in [BEPS81] is as follows: Let $g(s)$ be the Dirichlet series

$$\sum_{n=1}^{\infty} \frac{c(n)}{n^s},$$

whose Euler product can be written as

$$\prod_p \left(\left(1 - \frac{1}{p^s}\right)^{1/2} \left(1 + \frac{1}{2}\left(1 + \frac{1}{p}\right) p^{-s} + \frac{1}{3}\left(1 + \frac{1}{p} + \frac{1}{p^2}\right) p^{-2s} + \cdots \right) \right).$$

Therefore, we have

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{A(n) n^{-s}}{n} &= \prod_p \left(1 + \frac{1}{2}\left(1 + \frac{1}{p}\right) p^{-s} + \frac{1}{3}\left(1 + \frac{1}{p} + \frac{1}{p^2}\right) p^{-2s} + \cdots \right) \\ &= \zeta(s)^{1/2} g(s). \end{aligned}$$

From here, the authors presented several ways to deduce that

$$\sum_{n \leq x} \frac{A(n)}{n} \sim \frac{g(1)}{\pi^{1/2}} \frac{x}{(\log x)^{1/2}},$$

which can be done using several methods, including contour integration as well as by a Tauberian theorem by Delange. We refer the reader to [BEPS81] for a sketch of these proofs.

Partial summation can then be used to show that on average

$$A(n) \sim \frac{cn}{\sqrt{\log n}},$$

as we have mentioned earlier.

3.3. THE DISTRIBUTION OF $A(n)$

Our approach is somewhat more elementary, with our main tool being the following theorem by Wirsing [Wir67]:

Lemma 3.1. (Wirsing) *If $h(n)$ is a real-valued multiplicative function satisfying the conditions:*

- $h(n) \geq 0$ *for* $n = 1, 2, \ldots,$
- $h(p^v) \leq c_1 c_2^v$, *where* $v = 2, 3, \ldots,$ *for some constants c_1 and c_2 with* $c_2 < 2,$

- $\sum_{p \le x} h(p) = (\vartheta + o(1)) \dfrac{x}{\log x}$ *for some constant* ϑ.

Then as $x \to \infty$,

$$\sum_{n \le x} h(n) \sim \frac{e^{-\gamma\vartheta}}{\Gamma(\vartheta)} \frac{x}{\log x} \prod_{p \le x} \sum_{v=0}^{\infty} \frac{h(p^v)}{p^v}$$

where γ *is the Euler constant, and*

$$\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} dt$$

is the gamma function.

The above lemma provides an asymptotic formula for the sum of multiplicative with the said properties.

The second result we need is Mertens second theorem on prime numbers:

Lemma 3.2. *For* $x \to \infty$ *we have*

$$\sum_{p \le x} \frac{1}{p} = \log\log x + \mu + O\left(\frac{1}{\log x}\right)$$

where $\mu = 0.2614972\ldots$ *is the Mertens constant.*

The steps in our proof is similar to the approach taken by Bateman et al, in that we begin by deducing the average order of $A(n)/n$ using Wirsing's theorem.

Theorem 3.3. *There exists a constant* $\alpha = 0.813515784\ldots$ *such that*

$$\sum_{n \le x} \frac{A(n)}{n} \sim \frac{\alpha x}{\sqrt{\log x}}.$$

Proof. Let $f(n) = A(n)/n$. We begin by showing that $f(n)$ satisfies the conditions required by Lemma 3.1. The first condition is satisfied trivially as $f(n) \ge 0$, and for the second

condition, $f(p^v)$ is bounded above since

$$\begin{aligned} f(p^v) &= \frac{\sigma(p^v)}{p^v\tau(p^v)} = \frac{1+p+p^2+\cdots+p^v}{p^v(v+1)} \\ &= \frac{p^{v+1}-1}{p^v(p-1)(v+1)} \\ &\leq \frac{p^{v+1}-1}{2(p^{v+1}-p^v)} \leq \frac{p}{2(p-1)} \leq 1. \end{aligned}$$

By the prime number theorem, we also have

$$\sum_{p\leq x} f(p) = \sum_{p\leq x} \frac{p+1}{2p} \sim \frac{1}{2}\sum_{p\leq x} 1 \sim \frac{1}{2}\frac{x}{\log x},$$

hence all the conditions of Lemma 3.1 are satisfied with $\vartheta = 1/2$.

Applying Wirsing's theorem gives us

$$\sum_{n\leq x} f(n) \sim \frac{e^{\gamma/2}}{\sqrt{\pi}}\frac{x}{\log x}\prod_{p\leq x}\sum_{v=0}^{\infty}\frac{f(p^v)}{p^v}. \tag{3.1}$$

The sum over v on the right hand side can be simplified to

$$\begin{aligned} \sum_{v=0}^{\infty}\frac{f(p^v)}{p^v} &= \sum_{v=0}^{\infty}\frac{p^{v+1}-1}{p^{2v}(p-1)(v+1)} \\ &= \frac{1}{p-1}\left(\sum_{v=0}^{\infty}\frac{p^{v+1}}{p^{2v}(v+1)} - \sum_{v=0}^{\infty}\frac{1}{p^{2v}(v+1)}\right). \end{aligned}$$

For the terms inside the brackets, observe that

$$\sum_{v=0}^{\infty}\frac{p^{v+1}}{p^{2v}(v+1)} = p^2\sum_{v=1}^{\infty}\frac{1}{vp^v} = -p^2\log\left(1-\frac{1}{p}\right),$$

and similarly,

$$\sum_{v=0}^{\infty}\frac{1}{p^{2v}(v+1)} = p^2\sum_{v=1}^{\infty}\frac{1}{vp^{2v}} = -p^2\log\left(1-\frac{1}{p^2}\right).$$

Hence we have

$$\begin{aligned}\sum_{v=0}^{\infty}\frac{f(p^v)}{p^v} &= \frac{p^2}{p-1}\left(\log\left(1-\frac{1}{p^2}\right)-\log\left(1-\frac{1}{p}\right)\right)\\ &= \frac{p^2}{p-1}\log\left(1+\frac{1}{p}\right).\end{aligned}$$

We now need to take the product of the above sum over prime values. To simplify our notation, we write

$$\prod_{p\le x}\sum_{v=0}^{\infty}\frac{f(p^v)}{p^v} = \exp(\eta(x))$$

where

$$\eta(x) = \sum_{p\le x}\log\left(\frac{p^2}{p-1}\log\left(1+\frac{1}{p}\right)\right).$$

To establish an upper bound for the term inside the bracket, we write

$$\begin{aligned}\frac{p^2}{p-1}\log\left(1+\frac{1}{p}\right) &= \frac{p^2}{p-1}\left(\frac{1}{p}-\frac{1}{2p^2}+O\left(p^{-3}\right)\right)\\ &= 1+\frac{1}{2p}+O\left(p^{-2}\right),\end{aligned}$$

and upon taking logarithm, we have

$$\log\left(\frac{p^2}{p-1}\log\left(1+\frac{1}{p}\right)\right)-\frac{1}{2p} = O\left(p^{-2}\right). \tag{3.2}$$

Using Mertens second theorem to estimate the sum of $1/2p$ over primes gives us

$$\begin{aligned}\eta(x) &= \sum_{p\le x}\frac{1}{2p}+\sum_{p\le x}\left(\log\left(\frac{p^2}{p-1}\log\left(1+\frac{1}{p}\right)\right)-\frac{1}{2p}\right)\\ &= \frac{1}{2}\log\log x+\mu+\lambda+o(1)\end{aligned}$$

where $\mu = 0.2614972\ldots$ is the Mertens constant and

$$\lambda = \sum_{p}\left(\log\left(\frac{p^2}{p-1}\log\left(1+\frac{1}{p}\right)\right)-\frac{1}{2p}\right) = 0.3930856\ldots$$

which converges because of the bound from (3.2).

Therefore, from (3.1),

$$\begin{aligned}\sum_{n\le x} f(n) &\sim \frac{e^{\gamma/2}}{\sqrt{\pi}}\frac{x}{\log x}\prod_{p\le x}\sum_{v=0}^{\infty}\frac{f(p^v)}{p^v}\\ &\sim \frac{\alpha x}{\sqrt{\log x}}\end{aligned}$$

with $\alpha = 0.813515784\ldots$. □

We now apply partial summation to derive the average order of $A(n)$, continuing on from the previous theorem.

Theorem 3.4. *There exists a constant $\beta = 0.40675789\ldots$ such that*

$$\sum_{n\le x} A(n) \sim \frac{\beta x^2}{\sqrt{\log x}}$$

Proof. Let

$$F(t) = \sum_{n\le t}\frac{A(n)}{n}.$$

Using partial summation we write,

$$\sum_{n\le x} A(n) = \sum_{n\le x}\frac{nA(n)}{n} = xF(x) - \int_1^x F(t)dt.$$

Hence, from the result we derived in the preceding theorem, we have

$$\sum_{n\le x} A(n) \sim \frac{\alpha x^2}{\sqrt{\log x}} - \int_2^x \frac{t}{\sqrt{\log t}}dt.$$

Let $y = x/\log x$, and rewrite the integral as

$$\int_2^y \frac{t}{\sqrt{\log t}}dt - \int_y^x \frac{t}{\sqrt{\log t}}dt.$$

Since $\log t \ge \log 2$ for $t \in [2, y]$, and $\log t \sim \log x$ for $t \in [y, x]$, we derive

$$\int_2^y \frac{t}{\sqrt{\log t}}dt = O\left(\frac{x^2}{(\log x)^2}\right)$$

and

$$\int_y^x \frac{t}{\sqrt{\log t}} dt \sim \frac{a}{\sqrt{\log x}} \int_y^x t dt \quad = \frac{x^2 - y^2}{2\sqrt{\log x}}$$
$$\sim \frac{x^2}{2\sqrt{\log x}}.$$

And thus we have

$$\sum_{n \leq x} A(n) \sim \frac{\beta x^2}{\sqrt{\log x}}$$

for a constant $\beta \approx \alpha/2 = 0.40675789\ldots$. □

3.4. THE DISTRIBUTION OF THE k-TH POWER OF $A(n)$

One possible extension of the result we obtained in the previous section would be to obtain an asymptotic formula for the powers of $A(n)$. Here we are interested with $A_\kappa(n)$ defined as

$$A_\kappa(n) = \left(\frac{1}{\tau(n)} \sum_{d|n} d^\kappa \right)^{1/\kappa}.$$

We start with the asymptotic result for $A_\kappa(n)/n$.

Theorem 3.5. *There exists a constant α_κ such that*

$$\sum_{n \leq x} \frac{A_\kappa(n)}{n} \sim \frac{\alpha_\kappa x}{\sqrt{\log x}}.$$

Proof. As before, we first apply Wirsing theorem using $f_\kappa(n)$ where

$$f_\kappa(n) = \frac{A_\kappa(n)}{n}.$$

It is clear that $f_\kappa(n)$ is non negative, hence we start by showing that the other two condi-

tions required by Lemma 3.1 are met. We see that

$$\begin{aligned} f_\kappa(p^\upsilon) = \frac{A_\kappa(p^\upsilon)}{p^\upsilon} &= \frac{1}{p^\upsilon}\left(\frac{1}{\tau(p^\upsilon)}\sum_{d|p^\upsilon} d^\kappa\right) = \frac{1}{p^\upsilon}\left(\frac{p^{\kappa(\upsilon+1)}-1}{(p^\kappa-1)(\upsilon+1)}\right)^{1/\kappa} \\ &\sim \frac{1}{p^\upsilon}\left(\frac{p^{\kappa(\upsilon+1)}}{(p^\kappa-1)(\upsilon+1)}\right)^{1/\kappa} = \frac{p}{(p^\kappa-1)^{1/\kappa}(\upsilon+1)^{1/\kappa}} \\ &\ll \frac{p}{2^{1/\kappa}(p^\kappa-1)^{1/\kappa}} \ll 1 \end{aligned}$$

since $p^\kappa < 2(p^\kappa - 1)$, hence satisfying the boundedness condition. For the final condition, we have

$$\sum_{p\le x} f(p) = \sum_{p\le x}\frac{1}{p}\left(\frac{p^\kappa+1}{2}\right)^{1/\kappa} \sim \frac{1}{2^{1/\kappa}}\sum_{p\le x} 1 \sim \frac{1}{2^{1/\kappa}}\frac{x}{\log x}$$

and hence $f_k(n)$ satisfies all the requirements of Lemma 3.1 with $\vartheta = 1/2^{1/\kappa}$. Applying Lemma 3.1, we have

$$\begin{aligned} \sum_{\upsilon=0}^{\infty}\frac{f_\kappa(p^\upsilon)}{p^\upsilon} &= \sum_{\upsilon=0}^{\infty}\frac{1}{p^{2\upsilon}}\left(\frac{p^{\kappa(\upsilon+1)}-1}{(p^\kappa-1)(\upsilon+1)}\right)^{1/\kappa} \\ &\sim \sum_{\upsilon=0}^{\infty}\frac{1}{p^{2\upsilon}}\left(\frac{p^{\kappa(\upsilon+1)}}{p^\kappa(\upsilon+1)}\right)^{1/\kappa} = \sum_{\upsilon=0}^{\infty}\left(\frac{1}{p^\upsilon(\upsilon+1)^{1/\kappa}}\right) \\ &= 1 + \frac{1}{2^{1/\kappa}p} + O\left(\frac{1}{p^2}\right). \end{aligned}$$

The product of the sum is therefore

$$\prod_{p\le x}\sum_{\upsilon=0}^{\infty}\frac{f_\kappa(p^\upsilon)}{p^\upsilon} \sim \prod_{p\le x}\sum_{\upsilon=0}^{\infty} 1 + \frac{1}{2^{1/\kappa}p} + O\left(\frac{1}{p^2}\right) = \exp\left(\eta_\kappa(x)\right)$$

where

$$\eta_\kappa(x) = \sum_{p\le x}\log\left(1 + \frac{1}{2^{1/\kappa}p} + O\left(\frac{1}{p^2}\right)\right).$$

Asymptotically,

$$\eta_\kappa(x) \sim \sum_{p\le x}\log\left(1+\frac{1}{2^{1/\kappa}p}\right) = \sum_{p\le x}\frac{1}{2^{1/\kappa}p}$$

and with Lemma 3.2 we have

$$\eta_\kappa(x) \sim \frac{1}{2^{1/\kappa}}\log\log x + \mu + O\left(\frac{1}{\log x}\right)$$

where μ is the Mertens constant. Putting this together with what we have earlier, we have our proof:

$$\sum_{n \leq x} f_\kappa(n) = \sum_{n \leq x} \frac{A_\kappa(n)}{n} \sim \frac{\alpha_\kappa x}{\sqrt{\log x}}$$

for some constant α_κ. □

The next theorem follows naturally:

Theorem 3.6. *There exists a constant β_κ such that*

$$\sum_{n \leq x} A_k(n) \sim \frac{\beta_\kappa x^2}{\sqrt{\log x}}$$

Proof. The proof follows the proof for Theorem 3.4 with the only difference here being the constant term. □

CHAPTER 4

THE SET OF THE LARGEST PRIME DIVISORS

Let $P(n)$ be the largest prime divisor of a positive integer n, with $P(1) = 1$. Given an integer-valued sequence $\mathcal{A} = \big(a(n)\big)_{n=1}^{\infty}$, we write the set of the largest prime divisors of this sequence as

$$\mathcal{S}_{\mathcal{A}}(x) = \big\{P\big(a(n)\big) \,:\, n \le x\big\},$$

for a real $x > 0$.

The study of $\mathcal{S}_{\mathcal{A}}$ for various sequences $\mathcal{A}$ is certainly a classic number theoretic pursuit, and various properties of these sets have been previously considered in other studies. In this chapter, we are particularly interested with the cardinality of $\mathcal{S}_{\mathcal{A}}$, and we shall derive the lower bound of this cardinality for several type of sequences. This chapter is based on a paper authored together with I. Shparlinski [SS07].

4.1. SMOOTH NUMBER

The study of largest prime divisors is closely related to the study of *smooth number*, so it is natural to start with an overview of this concept.

We define a positive integer to be y-smooth if all its prime factors are less than or equal to y, and we define the function

$$\psi(x,y) = \#\{n \leq x : P(n) \leq y\},$$

which counts the number of y-smooth numbers $\leq x$. Smooth numbers are useful in the analysis of several algorithms in computational number theory, particularly that of factorisation and primality testing.

Crandall and Pomerance [CP05] noted that smooth numbers are surprisingly numerous. For example if x is sufficiently large; then only "a vanishingly small fraction" of primes $\leq x$ are in the interval $[1, \sqrt{x}]$, but more than thirty percent of the numbers $\leq x$ are $\sqrt{x}$-smooth.

At first glance, we may approximate the size of $\psi(x,y)$ using a simple probability argument to say that

$$\psi(x,y) \sim x \prod_{y<p\leq x} \left(1 - \frac{1}{p}\right),$$

and so we can use Mertens third theorem to approximate $\psi(x,y)$. However, this argument is flawed since the divisibility of integers are not independent events, in that an integer can be divisible by several primes larger than y. Hence it is no surprise that the actual size of $\psi(x,y)$ is of a smaller order of magnitude than suggested by the above estimate.

The first asymptotic estimate for $\psi(x,y)$ was obtained by Dickman in [Dic30]:

$$\psi\left(x,y\right) \sim x\rho(u),$$

where $u = \log x / \log y$, and $\rho(u)$ is defined to be the continuous function satisfying

$$\rho(u) = 1 \qquad \text{for } 0 \leq u \leq 1$$

and

$$\rho'(u) = -\rho(u-1)/u \qquad \text{for } u > 1.$$

There is no known closed form for $\rho(u)$ for $u > 2$, but it can be approximated numerically and has been shown to decrease to zero rapidly. The function can be reasonably approximated as

$$\log \rho(u) = -\big(1 + o(1)\big) u \log u$$

as $u \to \infty$. Indeed, Canfield et al in [CEP83] showed that

$$\psi(x, y) = x u^{-u + o(u)}$$

as $u \to \infty$ with $u < (1 - \varepsilon) \log x / \log \log x$.

A more precise result was given by Hildebrand in [HT93], stating that

$$\psi(x, y) = x\rho(u) \left\{ 1 + O\left(\frac{\log(u+1)}{\log y} \right) \right\}$$

with

$$y \geq 2, \quad 1 \leq u \leq (\log y)^{3/5 - \varepsilon},$$

giving an asymptotic formula for $\psi(x, y)$ when y is large. Several other results for smaller values of y exist as well, and for these results, we refer the reader to a survey on smooth numbers by Hildebrand and Tenenbaum in [HT93].

4.2. OUTLINE OF OUR METHOD

In the derivation of the lower bounds, we start by considering the number of solutions a congruence of the form

$$a(n) \equiv 0 \pmod{p}, \tag{4.1}$$

where p is an element of the set of largest prime divisors $\mathcal{S}_{\mathcal{A}}(x)$ and $a(n)$ denotes the n-th value in the sequence $\mathcal{A}$.

Using a simple Dirichlet's pigeon-hole argument, we can expect to have one prime in $\mathcal{S}_{\mathcal{A}}(x)$ to be the largest prime divisors for several values in the sequence. Consequently the size of $\mathcal{S}_{\mathcal{A}}(x)$ is smaller than the size of the sequence itself, and it follows that if we set p to be the most common largest prime divisor, then the number of n satisfying this congruence must be at least

$$\left\lceil \frac{\text{the size of the sequence}}{\text{the size of the set of the largest prime divisors}} \right\rceil = \left\lceil \frac{x}{\#\mathcal{S}_{\mathcal{A}}(x)} \right\rceil .$$

Therefore if we have an upper bound for the number of $n \leq x$ satisfying the above congruence, then

$$\frac{x}{\#\mathcal{S}_{\mathcal{A}}(x)} \ll \text{upper bound on the number of solutions.}$$

The results on the upper bounds of the number of solutions for different sequences are readily available, so the lower bound for $\#\mathcal{S}_{\mathcal{A}}(x)$ can be derived from this relation provided that we know p. The difficulty lies on finding the value of p, as we certainly do not have sufficient information to know which prime is the most commonly occurring largest prime divisor.

In the proofs which are to follow, we circumvent this difficulty by considering two subsets of $\{n \leq x\}$:

$$\mathcal{T}_1(x,y) = \{n \leq x : P\big(a(n)\big) \leq y\} \text{ and } \mathcal{T}_2(x,y) = \{n \leq x : P\big(a(n)\big) > y\}$$

for an arbitrarily chosen y. These sets correspond with the sets

$$\mathcal{S}_{\mathcal{T}_1} = \{P\big(a(n)\big) : n \in \mathcal{T}_1\} \text{ and } \mathcal{S}_{\mathcal{T}_2} = \{P\big(a(n)\big) : n \in \mathcal{T}_2\}$$

respectively, and the relation

$$\frac{\#\mathcal{T}_i}{\#\mathcal{S}_{\mathcal{T}_i}} \ll \text{upper bound on the number of solutions}$$

for $i = \{1, 2\}$ still applies. We can then derive a more precise lower bound on either $\#\mathcal{S}_{\mathcal{T}_1}$ or $\#\mathcal{S}_{\mathcal{T}_2}$ because we can now put a restriction on the size of p, and since the lower bound on either of these sets is a lower bound on $\#\mathcal{S}_{\mathcal{A}}(x)$ itself, this provides us with the answer we require.

In the course of proving our theorems, some results involving smooth numbers will help us in determining the size of $\mathcal{T}_1$ and $\mathcal{T}_2$, as it is clear that $\mathcal{T}_1$ is the set of y-smooth largest prime divisors.

4.3. POLYNOMIAL SEQUENCES

Our first sequence of interest is that of polynomial sequences. Let $g(n)$ be a non-constant polynomial with integer coefficients defined on $\mathbb{Z}$. We are interested with the set

$$\mathcal{S}_{\mathcal{G}}(x) = \left\{P\big(g(n)\big) : n \leq x\right\},$$

and in what follows we shall derive a lower bound on the cardinality of this set.

To derive our result we make use of a result on the distribution y-smooth prime divisors of $g(n)$, that is the number of integers $n \leq x$ such that the largest prime divisor of $g(n)$ is less than y,

$$\psi_g(x, y) = \#\{n \leq x : P\big(g(n)\big) \leq y\}$$

where $y = x^{1/u}$ for an arbitrarily chosen u.

We have the following bound which is a partial case of a more general result obtained in [Tim77], which in turns improves the result from [Hmy66]:

Lemma 4.1. *Let $g(n)$ be a polynomial with integer coefficients of degree $k \geq 2$ with t irreducible*

divisors over $\mathbb{Z}$. Then for any fixed $\varepsilon > 0$ and all sufficiently large x, we have:

$$\psi_g(x,y) \leq \frac{(t+\varepsilon)^{[v]}\, x}{k(k-1)^{[v]-1} v^{[v]}}$$

for $y = x^{1/v}$ and $1 \leq v \leq \sqrt{\log x/(2+\varepsilon)}$.

Theorem 4.2. *Let $g(n)$ be a polynomial with integer coefficients of degree $k \geq 2$ which does not split completely over $\mathbb{Z}$, then for the sequence $\mathcal{G} = (g(n))_{n=1}^{\infty}$ we have*

$$\#\mathcal{S}_{\mathcal{G}}(x) \gg \frac{x}{4k^2} - 1.$$

Proof. For this proof, consider the congruence

$$g(n) \equiv 0 \pmod{p}.$$

If we choose the prime p such that it is the most common largest prime divisor in $\mathcal{S}_{\mathcal{G}}(x)$, then this congruence has at least $[x]/\#\mathcal{S}_{\mathcal{G}}(x)$ solutions. On the other hand, by Lagrange theorem, a non-zero polynomial modulo p of degree k has at most k solutions in every interval of length p. Therefore the number of solutions to this congruence is bounded above by $k([x/p]+1)$, and thus

$$\frac{[x]}{\#\mathcal{S}_{\mathcal{G}}(x)} \leq k\left(\left[\frac{x}{p}\right]+1\right).$$

We now partition the set of integers $n \leq x$ into the set $\mathcal{N}_1$ consisting of $n \leq x$ such that $P\big(g(n)\big) \leq x$, and the set $\mathcal{N}_2$ consisting of $n \leq x$ such that $P\big(g(n)\big) > x$.

Since $g(n)$ does not split over $\mathbb{Z}$, the number of its irreducible divisors, t, satisfies $t \leq k-1$. So it follows from Lemma 4.1, with $v = 1$ and $\varepsilon = 1/2$, that the size of $\mathcal{N}_1$ is

$$\#\mathcal{N}_1 \leq \left(\frac{k-1/2}{k}\right) x.$$

The size of $\mathcal{N}_2$ is therefore

$$\#\mathcal{N}_2 \geq x - \#\mathcal{N}_1 - 1 = \frac{x}{2k} - 1.$$

Considering only the values of n in $\mathcal{N}_2$, we know that p must be greater than x to be a prime divisor of $g(n)$ for $n \in \mathcal{N}_2$. Letting $\mathcal{Q} = \{P(g(n)) : n \in \mathcal{N}_2\}$, then for some $p \in \mathcal{Q}$ with $p \geq x$, the congruence

$$g(n) \equiv 0 \pmod{p}, \qquad \text{for } n \in \mathcal{N}_2,$$

has at least $\#\mathcal{N}_2/\#\mathcal{Q}$ solutions. On the other hand, as we noted above, there are at most $k([x/p]+1)$ solutions to this congruence, therefore

$$\frac{\#\mathcal{N}_2}{\#\mathcal{Q}} \leq k\left(\left[\frac{x}{p}\right]+1\right) \leq k\left(\frac{x}{x}+1\right) = 2k. \tag{4.2}$$

Since $\mathcal{Q} \subset \mathcal{S}_{\mathcal{G}}(x)$, a lower bound on $\#\mathcal{Q}$ is also a lower bound for $\#\mathcal{S}_{\mathcal{G}}(x)$, hence from (4.2) we have

$$\#\mathcal{S}_{\mathcal{G}}(x) \geq \#\mathcal{Q} \geq \frac{\#\mathcal{N}_2}{2k} \gg \frac{x}{4k^2} - 1,$$

which gives us the required result. □

4.4. LINEAR RECURRENT SEQUENCES

Our second sequence of interest is that of linear recurrent sequences. Let $\mathcal{U} = \{u(n)\}_{n=1}^{\infty}$ be a linear recurrence sequence of integers satisfying a homogeneous linear recurrence relation

$$c_k u(n+k) + c_{k-1}u(n+k-1) + \cdots + c_0 u(n) = 0$$

with integer coefficients $c_k, c_{k-1}, \ldots, c_0$, and a characteristic polynomial

$$c_k x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c_0.$$

The linear recurrence sequence is non-degenerate if $\alpha_i^s \neq \alpha_j^s$, for $1 \leq i < j \leq m, s = 1, 2, \ldots$, where $\alpha_i, \ldots, \alpha_m$ are pairwise distinct roots of the characteristic polynomial.

The following result from [Shp85] gives an upper bound on the congruence

$$u(n) \equiv 0 \pmod{p}.$$

Lemma 4.3. *For an integer q and a real x let $R_{\mathcal{U}}(x, q)$ be the number of $n \leq x$ such that $u(n) \equiv 0 \pmod{q}$. Then if the linear recurrence sequence $\mathcal{U} = \{u(n)\}_{n=1}^{\infty}$ is non-degenerate, then we have*

$$R_{\mathcal{U}}(x, q) \ll \frac{x}{\log q} + 1$$

We also need the following result from [Shp90]:

Lemma 4.4. *Let $\mathcal{L}$ be an arbitrary set of r primes, and let $A_{\mathcal{U}}(\mathcal{L}, x)$ be the number of $n \leq x$ such that $u(n)$ is composed only of prime $\mathcal{L}$. Then if the linear recurrence sequence $\mathcal{U} = \{u(n)\}_{n=1}^{\infty}$ is non-degenerate, then for a real $x \geq 0$ we have*

$$A_{\mathcal{U}}(\mathcal{L}, x) \ll r(\log x)^2$$

We now derive the lower bound for

$$\#\mathcal{S}_{\mathcal{U}}(x) = \#\left\{P\big(u(n)\big) : n \leq x\right\}$$

as follows:

Theorem 4.5. *For a non-degenerate linear recurrence sequence $\mathcal{U} = \{u(n)\}_{n=1}^{\infty}$ we have*

$$\#\mathcal{S}_{\mathcal{U}}(x) \gg \log x$$

Proof. From the congruence

$$u(n) \equiv 0 \pmod{p},$$

there is a prime p such that the congruence has at least $x/\#\mathcal{S}_{\mathcal{U}}(x)$ solutions, and combining

this with Lemma 4.3, we have

$$\frac{x}{\#\mathcal{S}_{\mathcal{U}}(x)} \ll \frac{x}{\log p} + 1.$$

Similar to the previous theorem, we partition the set of integers $n \leq x$ into the set $\mathcal{M}_1$ consisting of $n \leq x$ such that $P\big(u(n)\big) \leq y$, and the set $\mathcal{M}_2$ consisting of $n \leq x$ such that $P\big(u(n)\big) > y$, where y is a value to be determined shortly.

We now consider the solutions to the above congruence for $n \in \mathcal{M}_2$. Letting $\mathcal{R} = \big\{P\big(u(n)\big) : n \in \mathcal{M}_2\big\}$, we have

$$\frac{\#\mathcal{M}_2}{\#\mathcal{R}} \ll \frac{x}{\log p} + 1. \tag{4.3}$$

To deduce the size of $\mathcal{M}_2$, we set $y = x/(\log x)^2$, so by the prime number theorem there are approximately $x/(\log x)^3$ primes smaller than y. The set $\mathcal{M}_1$ are composed of only primes smaller than y, so if we let $\mathcal{L}$ be the first $r = x/(\log x)^3$ primes, then from Lemma 4.4 we have

$$\#\mathcal{M}_1 \ll \frac{x}{\log x}.$$

Therefore

$$\#\mathcal{M}_2 \geq x - \#\mathcal{M}_1 \geq x - \frac{x}{\log x} = \big(1 + o(1)\big)x.$$

Continuing from (4.3), since the primes in $\mathcal{R}$ is greater than or equal to y,

$$\frac{\#\mathcal{M}_2}{\#\mathcal{R}} \ll \frac{x}{\log p} + 1 \ll \frac{x}{\log y} \ll \frac{x}{\log x},$$

and therefore as required we have

$$\#\mathcal{S}_{\mathcal{U}}(x) \geq \#\mathcal{R} \gg \log x.$$

□

4.5. OTHER SEQUENCES

We discuss several other sequences, starting with the sequence

$$\mathcal{F} = \{n! + 1\}_{n=1}^{x}.$$

We have the following result which is a partial case of a more general estimate in [LS05]:

Lemma 4.6. *For a prime p and a real x let $T(x, p)$ be the number of $n \le x$ such that $n! + 1 \equiv 0 \pmod{p}$. Then for any prime $p > x \ge 1$ we have*

$$T(x, p) \ll x^{2/3}$$

In the following theorem, we derive the lower bound on the cardinality of

$$\mathcal{S}_{\mathcal{F}}(x) = \{P(n! + 1) : n \le x\}.$$

Theorem 4.7. *For $\mathcal{F} = \{n! + 1\}_{n=1}^{\infty}$ we have*

$$\#\mathcal{S}_{\mathcal{F}}(x) \ge x^{1/3}.$$

Proof. Clearly we have at least one prime p such that the congruence

$$n! + 1 \equiv 0 \pmod{p}, \qquad 1 \le n \le x,$$

has at least $\lceil x/\#\mathcal{S}_{\mathcal{F}}(x) \rceil$ solutions. We consider two different cases: one when $p > x$, and the other when $p \le x$. For $p > x$ we can apply Lemma 4.6 directly to obtain

$$\frac{x}{\#\mathcal{S}_{\mathcal{F}}(x)} \ll x^{2/3}.$$

If $p \le x$, we see that for p is a prime divisor of $(n! + 1)$ only when $p > n$. Hence the number of $n \le x$ satisfying the congruence is the same as the number of $n \le p$ satisfying

it, and we use Lemma 4.6 with $x = p$ to obtain

$$\frac{x}{\#\mathcal{S}_{\mathcal{F}}(x)} \ll p^{2/3}.$$

Therefore we have

$$\left\lceil \frac{x}{\#\mathcal{S}_{\mathcal{F}}(x)} \right\rceil \ll \min\left\{x^{2/3}, p^{2/3}\right\} \ll x^{2/3}$$

and the result now follows. □

The second sequence we consider is the sequence $\mathcal{V} = \{v(n)\}_{n=1}^{x}$ where

$$v(n) = \prod_{i=1}^{n} p_i + 1$$

with p_n denoting the n^{th} prime. Let $W(x, p)$ be the number of $n \leq x$ such that

$$v(n) \equiv 0 \pmod{p}.$$

We take a special case for the following bound from [LLS05]:

Lemma 4.8. *For any prime p and real x with $p > x \geq 3$, we have:*

$$W(x, p) \ll \frac{x \log\log x}{\log x}$$

The lower bound on $\mathcal{S}_{\mathcal{V}}(x)$ can the be derived as follows:

Theorem 4.9. *Let $\mathcal{V} = \big(v(n)\big)_{n=1}^{\infty}$. We have*

$$\#\mathcal{S}_{\mathcal{V}}(x) \geq \frac{\log x}{\log\log x}.$$

Proof. As before, we note that there is a prime p such that the congruence

$$v(n) \equiv 0 \pmod{p}, \qquad 1 \leq n \leq x,$$

has at least $\lceil x/\#\mathcal{S}_{\mathcal{V}}(x) \rceil$ solutions. Similar to the previous theorem, we can apply Lemma 4.8 to obtain a lower bound when $x < p$.

If $p < x$, we note that for p to be a prime divisor of $v(n)$, p must be greater than the n-th prime, therefore $n \leq p/\log p \leq p$, and we apply Lemma 4.8 with $x = p$. Hence we have

$$\left\lceil \frac{x}{\#\mathcal{S}_{\mathcal{V}}(x)} \right\rceil \ll \min\left\{ \frac{x \log\log x}{\log x}, \frac{p \log\log p}{\log p} \right\}$$

□

The final sequence we will look at is the sequence of products of middle binomial sequence $\mathcal{B} = \{b(n)\}_{n=1}^{\infty}$, where

$$b(n) = \prod_{i=1}^{n} \binom{2i}{i}.$$

Theorem 4.10. *For the sequence $\mathcal{B} = \{b(n)\}_{n=1}^{\infty}$ as defined earlier, we have*

$$\#\mathcal{S}_{\mathcal{B}}(x) \gg \frac{2x}{\log 2x}$$

Proof. We see that since

$$b(n) = \binom{2}{1}\binom{4}{2}\cdots\binom{2n}{n}$$

the largest prime divisor of $b(n)$ is the prime immediately smaller than $2n$. As n increases by 2 up to x, $\mathcal{S}_{\mathcal{B}}(x)$ will contain all primes smaller than $2x$, hence the result follows trivially from the prime number theorem. □

CHAPTER 5

DIRICHLET CHARACTERS

Dirichlet was the first person to prove that the arithmetic progression

$$a, a+q, a+2q, \ldots$$

contains infinitely many primes when $(a, q) = 1$. In the course of proving this theorem, Dirichlet introduced a set of functions known as Dirichlet characters, which has since became an important tool in number theory.

We shall introduce the notion of Dirichlet characters and discuss some of its properties in this chapter.

5.1. INTRODUCTION

One of the many proofs for the infinitude of primes was an analytic argument by Euler, which began with the identity

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 - \frac{1}{p}\right)^{-1}$$

for a real $s > 1$, which upon taking the logarithm becomes

$$\log \zeta(s) = \sum_{p} \sum_{m=1}^{\infty} \frac{1}{m p^{ms}}.$$

The inner sum for $m \geq 2$ is bounded above since,

$$\sum_{m=2}^{\infty} \frac{1}{m p^{ms}} \leq \sum_{m=2}^{\infty} \frac{1}{p^m},$$

and since this sum is simply a geometric progression, we have

$$\sum_{p} \sum_{m=2}^{\infty} \frac{1}{p^m} = \sum_{p} \frac{1/p^2}{1 - 1/p} = \sum_{p} \frac{1}{p(p-1)} < \sum_{n=2}^{\infty} \frac{1}{n^2} < 1.$$

Therefore, since $\log \zeta(s)$ is unbounded as $s \to 1^+$, we conclude that $\sum_p 1/p^s$ must be unbounded as well, which proves that there are infinitely many primes.

Dirichlet wanted to show that $\sum_p 1/p^s$ also diverges when the primes in the summation is restricted to only those in the form $p \equiv a \pmod{q}$, thus showing that there are infinitely many primes in the arithmetic progression

$$a, a + q, a + 2q, \ldots$$

with $(a, q) = 1$. Therefore he needed a method to collect numbers which are congruent to a modulo q, and for this purpose he introduced the arithmetic function known as *Dirichlet characters*, defined by

$$\chi(n) = \omega^{v(n)}, \tag{5.1}$$

where ω is a real or complex $(q-1)$-th root of unity satisfying

$$\omega^{q-1} = 1,$$

and $v(n)$ chosen such that for a primitive root g modulo q,

$$g^{v(n)} \equiv n \pmod{q}.$$

Dirichlet first proved his theorem for the simpler case when q is prime, as this guarantee the existence of a primitive root modulo q. The construction of these characters is then straightforward; for a primitive root g, setting

$$\chi(g) = \omega \tag{5.2}$$

will give us a unique character modulo q, as the powers of g will run through the residue system modulo q, thus along with (5.1), the character is uniquely defined for every n in the residue class. Furthermore, there are $q-1$ choices for the right hand side of (5.2), namely ω, ω^2, $\cdots$, ω^{q-1}, and each choice gives a unique function, therefore giving us a total of $q-1$ characters.

The function χ has three important properties: First, it is periodic modulo q, as

$$\chi(n+q) = \omega^{v(n+q)} = \omega^{v(n)} = \chi(n).$$

Secondly, the function is multiplicative, since

$$v(mn) \equiv v(m) + v(n) \pmod{q-1},$$

and this implies that

$$\chi(mn) = \omega^{v(mn)} = \omega^{v(m)+v(n)} = \chi(m)\chi(n).$$

Most importantly however is the property that a linear combination of this function can be used to select integers which are congruent to a modulus q. To see why this is the case,

consider the sum

$$\sum_{\omega} \omega^k = \begin{cases} q-1 & k \text{ is divisible by } q-1, \\ 0 & \text{otherwise,} \end{cases}$$

taken over all roots of unity ω. If we set $k = v(n) - v(a)$, we have

$$\sum_{\omega} \omega^{v(n)-v(a)} = \begin{cases} q-1 & v(n) \equiv v(a) \pmod{q-1}, \\ 0 & \text{otherwise,} \end{cases}$$

and since $v(n) \equiv v(a) \pmod{q-1}$ implies that $n \equiv a \pmod{q}$, we now have a method to capture the values of n which are congruent to a modulo q.

Dirichlet then used these characters to form the L-function

$$L(s) = \sum_{\substack{n=1 \\ n \not\equiv 0 \pmod{q}}} \frac{\chi(n)}{n^s}.$$

Since χ is multiplicative, we have the analog of the Euler's identity,

$$L(s) = \prod_{p \neq q} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1},$$

and after taking the logarithm, we have

$$\log L(s) = \sum_{p \neq q} \sum_{m=1}^{\infty} \frac{\chi(p^m)}{m p^{ms}}.$$

These steps are analogous to the steps we have shown at the start of this chapter, and therefore the inner sum for $m \geq 2$ is again convergent, and so we can write

$$\log L(s) = \sum_{p} \frac{\chi(p)}{p^s} + O(1).$$

If we multiply this by $\overline{\chi}(a) = 1/\chi(a)$ and summing over all χ, we have

$$\begin{aligned}\sum_{\chi} \overline{\chi}(a) \log L(s) &= \sum_{\chi} \sum_{p} \frac{\overline{\chi}(a)\chi(p)}{p^s} + O(q) \\ &= (q-1) \sum_{p \equiv a \pmod{q}} \frac{1}{p^s} + O(q).\end{aligned}$$

Therefore the primes congruent to a modulo q are isolated in the right hand side, and what is left to do now is to show that the left hand side goes to infinity as $s \to 1^+$.

The rest of the proof is not within the scope of this thesis, as we merely intend to give a historical background on Dirichlet characters. For a more complete treatment, we refer the reader to an excellent exposition by Davenport in [Dav00].

5.2. PROPERTIES OF DIRICHLET CHARACTERS

Previously we considered only Dirichlet characters with prime modulus q. We now generalise so that q can be any positive integer.

5.2.1 DEFINITIONS AND BASIC PROPERTIES

If χ is a complex-valued arithmetic function defined on the set of integers, then for a positive integer q, χ is a Dirichlet character if and only if

(a) χ is completely multiplicative,

(b) χ is periodic modulo q,

(c) $\chi(n) = 0$ if and only if $(n, q) > 1$,

with $\chi(1) = 1$ and $\chi(0) = 0$ for all n and q (assuming χ is not identically one). The period q is referred to as the modulus or the conductor of the character.

If $(n, q) = 1$, then consequently there exists some k such that $n^k \equiv 1 \pmod{q}$, hence

$$\chi(n^k) = \big(\chi(n)\big)^k = 1,$$

and therefore $\chi(n)$ is a k-th root of unity. The character which is identically one for all n coprime to q, denoted by

$$\chi_1(n) = \begin{cases} 1 & \text{if } (n, q) = 1, \\ 0 & \text{otherwise,} \end{cases}$$

is called the principal or trivial character modulo q.

Furthermore, the formal definition earlier states that a character χ is periodic modulo q. If q is indeed the smallest period of χ, then χ is a *primitive character*, and it is otherwise called an *imprimitive character*.

5.2.2 Construction of Dirichlet characters

Earlier in the chapter, we touched on the construction of Dirichlet characters for prime modulus using primitive roots, which do not always exist for some non-prime moduli. As the modulus q is now generalised to be any positive integer, we now expand on the idea of Dirichlet characters construction.

For a prime modulus q, we define a Dirichlet character to be

$$\chi_h(n) = e^{2\pi i h v(n)/\varphi(q)} \tag{5.3}$$

if $(n, q) = 1$, where as previously defined $v(n)$ is the *index* of n modulo q of a given primitive root g, that is the number such that

$$g^{v(n)} \equiv 1 \pmod{q},$$

and the choice of $h = 1, 2, \ldots, \varphi(q)$ gives a unique character (hence there are $\varphi(q)$ unique characters modulo a prime q, indexed by h).

The above description is perhaps superfluous in view of the construction we outlined earlier, but we repeat it nonetheless for the similarity in defining characters where the modulus is a prime power: For $q = p^\alpha$, with $\alpha \geq 1$, we have the same definition that

$$\chi_h(n) = e^{2\pi i h v(n)/\varphi(q)},$$

except of course $h = 1, 2, \ldots, \varphi(q^\alpha) - 1$, and everything else is as defined previously.

If q is composite with $q = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where p_i are odd primes, then

$$\chi = \chi_1 \chi_2 \cdots \chi_r$$

is a Dirichlet character modulo q, where χ_i denotes a Dirichlet character modulo p_i (of which there are $\varphi(p_i^{\alpha_i})$). Since

$$\varphi(q) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k}),$$

this method allows us to construct every Dirichlet character modulo q.

In the case of Dirichlet characters with 2^α moduli, we do not have any primitive roots. The existence of a primitive root allows to have a unique $v(n)$ for every n, and as we can see from (5.3), this allows us to build the character in a straightforward manner. However, given a modulo 2^α, with $\alpha \geq 3$, we can show that for every odd integer n there is a unique $v(n)$ such that

$$n \equiv (-1)^{(n-1)/2} 5^{v(n)} \pmod{2^\alpha}.$$

To show this we begin by showing that the exponent of 5 modulo 2^α is $2^{\alpha-2}$. Let f be the exponent of 5 modulo 2^α, then we have (from the final section of Chapter 2):

$$f \mid \varphi(2^\alpha)/2 = 2^{\alpha-2}$$

and so $f \leq 2^{\alpha-2}$, and in fact this tells us that the exponent of f is some power of 2, say 2^β.

On the other hand, we have

$$2^\alpha \mid (5^f - 1) = (1 + 2^2)^{2^\beta} - 1 = 2^{\beta+2}t$$

for some odd number t. Hence $\beta \geq \alpha - 2$, and so $f = 2^\beta = 2^{\alpha-2}$.

Therefore the numbers

$$5, 5^2, \ldots, 5^{2^{\alpha-2}}$$

are incongruent modulo 2^α, each being $\equiv 1 \pmod 4$, and so are the numbers

$$-5, -5^2, \ldots, -5^{2^{\alpha-2}},$$

each being $\equiv 3 \pmod 4$. Hence we have generated $2^{\alpha-1} = \varphi(2^\alpha)$ numbers which are incongruent to each other.

Characters modulo 2^α can then be defined as

$$\chi_{a,c}(n) = (-1)^{a(n-1)/2} e^{2\pi i c v(n)/2^{\alpha-2}}$$

for odd n, where $a = 1, 2$, and $c = 1, 2, \ldots, \varphi(2^\alpha)/2$.

CHAPTER 6

EXPONENTIAL SUMS

One of the most ubiquitous functions in analytic number theory is the exponential function

$$e\big(f(x)\big) = e^{2\pi i f(x)},$$

where f is a real-valued function defined on $x \in \mathcal{X}$ for some arbitrary set $\mathcal{X}$. An exponential sum therefore refers to sums of the form

$$S(f) = \sum_{x\in\mathcal{X}} e\big(f(x)\big) = \sum_{x\in\mathcal{X}} e^{2\pi i f(x)}. \tag{6.1}$$

Exponential sums are essentially Fourier coefficients of the sequence under consideration, so it is not surprising that they carry valuable information. Many problems in number theory can be reduced to the study of such sums.

For a brief illustration on how exponential sums can be applied in number theory, consider the simplest form of exponential sums, namely the linear exponential sums of the form

$$\sum_{x=1}^{m} e^{2\pi i a x/m},$$

where a, n and m are integers. Sums of this form can be evaluated directly, since

$$\sum_{x=1}^{m} e^{2\pi iax/m} = \begin{cases} m, & \text{if } m \mid a, \\ 0, & \text{otherwise.} \end{cases} \tag{6.2}$$

The first case is trivial as each term in the sum evaluates to 1, while the second case is immediate if we consider the sum as a geometric progression and we see that if $m \nmid a$, then

$$\sum_{x=1}^{m} e^{2\pi iax/m} = \frac{e^{2\pi ia} - 1}{e^{2\pi ia/m} - 1} = 0.$$

We can relate linear exponential sums to the problem of finding the number of solutions to the congruence

$$x_1^n + \cdots + x_k^n \equiv c \pmod{p},$$

for some integer c and prime p (this is essentially a much simplified analog of Waring's problem).

Let $T(c)$ be the number of solutions of this congruence for a given c, with the variables x_i running through the set of residue class modulo p. Clearly if the tuple $(x_1, \ldots, x_k)$ is a solution, then

$$x_1^\alpha + \cdots + x_k^\alpha - c \equiv 0 \pmod{p},$$

therefore from (6.2),

$$\begin{aligned} T(a) &= \sum_{x_1,\ldots,x_k=1}^{p} \frac{1}{p} \sum_{n=1}^{p} e^{2\pi in(x_1^\alpha + \cdots + x_k^\alpha - c)/p} \\ &= \frac{1}{p} \sum_{n=1}^{p} e^{-2\pi inc/p} \sum_{x_1,\ldots,x_k=1}^{p} e^{2\pi in(x_1^\alpha + \cdots + x_k^\alpha)/p}. \end{aligned}$$

Since each variable x_i run through the same values modulo p, we can simplify the inner sum to

$$\sum_{x_1,\ldots,x_k=1}^{p} e^{2\pi in(x_1^\alpha + \cdots + x_k^\alpha)/p} = \left(\sum_{x=1}^{p} e^{2\pi inx^\alpha/p} \right)^k,$$

thus expressing the number of solutions in terms of exponential sums.

Unfortunately a closed form expression such as the one illustrated above, is quite rare. Nevertheless, in most applications it is quite enough to know the upper bound rather than the exact value of an exponential sum. The trivial upper bound for any exponential form is of course

$$\left| \sum_{x \in \mathcal{X}} e^{2\pi i f(x)/m} \right| \leq \#\mathcal{X}.$$

If we view the terms inside an exponential sum as points in different directions on the complex plane (with sufficient randomness), then we can expect to have some cancellations inside the sum. A proper estimate therefore should be well below this trivial bound, and the improvement of this upper bound is the major driving force behind the study of exponential sums.

In this chapter we introduce some concepts related to exponential sums and show some examples of common forms of exponential sums. The topic is certainly a vast and formidable one, hence we present only the basic concepts. For a detailed exposition on the theory of exponential sums, we refer the reader to the work of N. M. Korobov [Kor92]

6.1. BASIC PROPERTIES OF EXPONENTIAL SUMS

The set $\mathcal{X}$ on which an exponential sum is defined is often a residue system modulo m, and this gives rise to a class of exponential sums known as *rational exponential sums*, of the form

$$\sum_{x\in\mathcal{X}} e^{2\pi i f(x)/m},$$

where f is an integer valued function and the denominator m is a positive integer (often being a prime). If the function is periodic modulo m with fundamental period k, then the sum

$$S(f) = \sum_{x=1}^{k} e^{2\pi i f(x)/m} \tag{6.3}$$

is called a *complete sum*. More generally, the sum (6.3) is complete if the fractional part of f satisfy $\{f(n+k)\} = \{f(n)\}$.

If the summation in (6.3) extends only to some value less than the period, then this type of sum is called an *incomplete sum*, which is typically harder to estimate than complete sums. For example, in the case of linear exponential sums outlined earlier, for M smaller than the period m, we have

$$\left|\sum_{x=1}^{M} e^{2\pi i a x}\right| = \frac{\left|e^{2\pi i a M}-1\right|}{\left|e^{2\pi i a}-1\right|} \leq \frac{2}{\left|e^{2\pi i a}-1\right|}.$$

For $0 \leq a \leq 1/2$,

$$\left|e^{2\pi i a}-1\right| = 2\sin \pi a \geq 4a,$$

therefore, combining this with the trivial bound, we have

$$\left|\sum_{x=1}^{M} e^{2\pi i a x}\right| \leq \min\left(M, \frac{1}{2a}\right).$$

Complete exponential sums unsurprisingly exhibit properties which are similar to the underlying congruence class: Suppose $\mathcal{X}$ is a residue system modulo m, then for $x \in \mathcal{X}$ and integers a and b, if $(a,m) = 1$, then $ax + b$ also runs through the same residue system,

hence

$$\sum_{x=1}^{m} e^{2\pi i f(x)} = \sum_{x=1}^{m} e^{2\pi i f(ax+b)}.$$

The exponential sums mentioned so far have all been one-dimensional sums, but of course we can generalise this so that an exponential sum is defined on a set of vectors, in which case we have a *multiple exponential sum*. Principal among multiple exponential sum is the *double exponential sum*,

$$S(F) = \sum_{x\in\mathcal{X}} \sum_{y\in\mathcal{Y}} e^{2\pi i F(x,y)},$$

where the polynomial F is defined on $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ for some arbitrary set $\mathcal{X}$ and $\mathcal{Y}$.

One additional property we shall mention is the *multiplication formula* of exponential sums: If $f_1, \ldots, f_k$ are periodic functions with periods $m_1, \ldots, m_k$ which are coprime to each other, and

$$\{f(x)\} = \{f_1(x) + \cdots + f_k(x)\} \tag{6.4}$$

then

$$\sum_{x=1}^{m_1\cdots m_k} e^{2\pi i f(x)} = \prod_{i=1}^{k} \sum_{x_i=1}^{m_i} e^{2\pi i f_i(x_i)}.$$

To see this, note that if $x_1, \ldots, x_k$ respectively runs through the residue classes modulo $m_1, \ldots, m_k$, then

$$x_1 m_2 \cdots m_k + m_1 x_2 \cdots m_k + \cdots + m_1 \cdots m_{k-1} x_k$$

runs through the residue class modulo $m_1 \cdots m_k$. Therefore

$$\sum_{x=1}^{m_1\cdots m_k} e^{2\pi i f(x)} = \sum_{x_1=1}^{m_1} \cdots \sum_{x_k=1}^{m_k} e^{2\pi i f(x_1 m_2\cdots m_k + \cdots + m_1\cdots m_{k-1}x_k)}.$$

From (6.4) we have

$$\sum_{x=1}^{m_1\cdots m_k} e^{2\pi i f(x)} = \sum_{x_1=1}^{m_1} \cdots \sum_{x_k=1}^{m_k} e^{2\pi i (f_1(x_1 m_2\cdots m_k) + \cdots + f_k(m_1\cdots m_{k-1}x_k))}$$

and since for a valid i, m_i is coprime to $(m_1 \cdots m_k)/m_i$, then

$$\{(x_i m_1 \cdots m_k)/m_i\} = \{x_i\}$$

and the multiplication formula follows. The multiplication formula is important as it reduces an exponential sum with an arbitrary denominator into exponential sums with prime denominators.

6.2. GAUSSIAN SUMS

A *Gaussian sum* is a complete rational exponential sum of the second degree,

$$G(a,q) = \sum_{n=1}^{q} e^{2\pi i a n^2/q}$$

where a and q are integers with $(a,q) = 1$. As in the case of linear exponential sums, Gaussian sums can also be explicitly evaluated as:

$$|G(a,q)| = \begin{cases} \sqrt{q} & \text{if } q \equiv 1 \pmod 2, \\ \sqrt{2q} & \text{if } q \equiv 0 \pmod 4, \\ 0 & \text{if } q \equiv 2 \pmod 4. \end{cases}$$

The proof for these statements involves an important method in working with exponential sums, and we briefly illustrate it as follows:

For a complex z, we have $|z|^2 = z\overline{z}$, therefore

$$|G(a,q)|^2 = G(a,q)\overline{G}(a,q) = \sum_{x=1}^{q} e^{2\pi i a x^2/q} \sum_{y=1}^{q} e^{-2\pi i a y^2/q}.$$

Since $x+y$ runs through the same residue system as x, if we replace x with $x+y$ in the summation, we have

$$\begin{aligned} \sum_{x=1}^{q} e^{2\pi i a x^2/q} \sum_{y=1}^{q} e^{2\pi i a y^2/q} &= \sum_{x=1}^{q} \sum_{y=1}^{q} e^{2\pi i a (x^2+2xy)/q} \\ &= \sum_{x=1}^{q} e^{2\pi i a x^2/q} \sum_{y=1}^{q} e^{2\pi i a (2xy)/q}. \end{aligned}$$

The inner sum is therefore reduced to a linear sum, and we note that if q is odd, then since

$(a,q)=1$, the terms disappear except when $x=q$, in which case

$$|G(a,q)|^2 = qe^{2\pi iaq} = q.$$

If q is even, then the inner sum disappear unless $x=q$ or $x=q/2$, hence

$$|G(a,q)|^2 = q\left(e^{2\pi iaq/4}+1\right),$$

and the result follows.

The important observation to be made is that in the above method we reduced the problem to one involving linear exponential sums. Therefore given an exponential sum with arbitrary degree n (a generalisation of a Gaussian sum), we can apply the above process iteratively until we arrive at a linear sum. This method was introduced by H. Weyl in [Wey16].

6.3. EXTEND AND CONQUER

For this section, consider the double sum

$$W_c = \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} e^{2\pi icxy/p}$$

where $\mathcal{X}$ and $\mathcal{Y}$ are arbitrary subsets of a residue system modulo a prime p.

In the estimation of the sum W_c, we can extend the summation over x to include more values with the hope that the resulting sum is more convenient to evaluate. he key ingredient here is Cauchy's inequality:

$$(x_1+x_2+\cdots+x_r)^2 \le r\left(x_1^2+x_2^2+\cdots+x_r^2\right).$$

By Cauchy's inequality, we see that

$$|W_c|^2 \leq \#\mathcal{X} \sum_{x\in\mathcal{X}} \left| \sum_{y\in\mathcal{Y}} e^{2\pi icxy/p} \right|^2.$$

We can *extend* the summation to include all x in the residue class:

$$|W_c|^2 \leq \#\mathcal{X} \sum_{x=1}^{p} \left| \sum_{y\in\mathcal{Y}} e^{2\pi icxy/p} \right|^2,$$

thereby adding more terms into our sum, but at the benefit of having the summation of x over a fixed set, rather than some arbitrary set $\mathcal{X}$.

The second step we need to take here is to *conquer*:

$$\begin{aligned}\sum_{x=1}^{p} \left| \sum_{y\in\mathcal{Y}} e^{2\pi icxy/p} \right|^2 &= \sum_{x=1}^{p} \left(\sum_{y_1\in\mathcal{Y}} e^{2\pi icxy_1/p} \sum_{y_2\in\mathcal{Y}} e^{-2\pi icxy_2/p} \right) \\ &= \sum_{y_1,y_2\in\mathcal{Y}} \sum_{x=1}^{p} e^{2\pi icx(y_1-y_2)/p},\end{aligned}$$

and again we have a linear sum, and since y_1, $y_2 < p$, the inner sum evaluates to 1 only when $y_1 = y_2$, hence

$$|W_c|^2 \leq \#\mathcal{X}p \sum_{\substack{y_1,y_2\in\mathcal{Y} \\ y_1=y_2}} 1 = \#\mathcal{X}\#\mathcal{Y}p,$$

and so

$$|W_c| \leq \sqrt{\#\mathcal{X}\#\mathcal{Y}}$$

which is better than the trivial bound of $|W_c| \leq \#\mathcal{X}\#\mathcal{Y}$.

6.4. CLONING

The method of extend and conquer outlined above requires a double exponential sum, but we can actually create multiple *clones* of a sum in order to create a double sum for this purpose. We illustrate this process in the following example:

Let g be an element of a residue system modulo p with exponent ω. For integers a and b with $(a, p) = 1$, define the sum

$$S(a,b) = \sum_{x=1}^{\omega} e^{2\pi i a g^x/p} e^{2\pi i b x/\omega}.$$

The function $e^{2\pi i a g^x/p} e^{2\pi i b x/\omega}$ is periodic with period ω, hence for a given y with $1 \leq y \leq \omega$:

$$\begin{aligned} S(a,b) &= \sum_{x=1}^{\omega} e^{2\pi i a g^{x+y}/p} e^{2\pi i b(x+y)/\omega} \\ &= e^{2\pi i b y} \sum_{x=1}^{\omega} e^{2\pi i a g^y g^x/p} e^{2\pi i b x/\omega} \end{aligned}$$

Therefore $|S(a,b)| = |S(ag^y, b)|$, effectively cloning our original sum.

The next step is to extend by summing over all y, creating the double sum

$$\begin{aligned} \sum_{y=1}^{\omega} |S(ag^y, b)|^2 &= \sum_{y=1}^{\omega} \left| \sum_{x=1}^{\omega} e^{2\pi i a g^y g^x/p} e^{2\pi i b x/\omega} \right|^2 \\ &\leq \sum_{c=1}^{p} \left| \sum_{x=1}^{\omega} e^{2\pi i c g^x/p} e^{2\pi i b x/\omega} \right|^2. \end{aligned}$$

Then we conquer:

$$\begin{aligned} \sum_{c=1}^{p} \left| \sum_{x=1} e^{2\pi i c g^x/p} e^{2\pi i b x/\omega} \right|^2 &= \sum_{c=1}^{p} \sum_{x_1=1}^{\omega} e^{2\pi i c g^{x_1}/p} e^{2\pi i b x_1/\omega} \sum_{x_2=1}^{\omega} e^{-2\pi i c g^{x_2}/p} e^{-2\pi i b x_2/\omega} \\ &= \sum_{x_1,x_2=1}^{\omega} e^{2\pi i b(x_1-x_2)/\omega} \sum_{c=1}^{p} e^{c(g^{x_1}-g^{x_2})/p}. \end{aligned}$$

Since

$$g^{x_1} \equiv g^{x_2} \pmod{p}$$

if and only if

$$x_1 \equiv x_2 \pmod{\omega},$$

the terms in the inner sum above vanish unless this congruence is satisfied, hence

$$|S(a,b)|^2 = \frac{1}{\omega}\sum_{y=1}^{\omega}|S(ag^y,b)|^2 \leq p.$$

which leads to the bound

$$|S(a,b)| \leq \sqrt{p}$$

provided that $(a,p) = 1$.

6.5. MORE ON SUMS WITH EXPONENTIAL FUNCTION

A sum with exponential function takes the form

$$S(f) = \sum_{x=1}^{p} e^{2\pi i a q^x/m}$$

where a, $m \geq 2$, and $q \geq 2$ are integers with $(m,q) = 1$.

To illustrate how one can work with this sum, consider the following example: For some prime p and integer m_1, let $m = pm_1$ where $p \mid m_1$, and let ω be the exponent of q modulo m and ω_1 be the exponent of q modulo m_1. If $\omega \neq \omega_1$, then

$$\sum_{x=1}^{\omega} e^{2\pi i a q^x/m} = 0 \tag{6.5}$$

for any integer a such that $p \nmid a$.

To derive this result, we first show that

$$\omega = p\omega_1. \tag{6.6}$$

To do so, we note that since ω is the exponent of q modulo m, we have

$$q^{\omega} \equiv 1 \pmod{m_1}$$

hence $\omega_1 \mid \omega$. On the other hand, $q^{\omega_1} = 1 + k_1 m_1$ for some constant k, hence

$$q^{p\omega_1} = (1 + k_1 m_1)^p \equiv 1 \pmod{m}$$

which implies that $\omega \mid p\omega_1$. Therefore $(\omega/\omega_1) \mid p$, and since p is prime, this implies (6.6).

Now, let T be the number of solutions to the congruence

$$q^x \equiv q^y \pmod{m}$$

where $1 \leq x, y \leq \omega$. Of course every powers of q are distinct, and so trivially there are ω solutions for this equation, namely when $x = y$. On the other hand, we can express the number of solutions in terms of exponential sums:

$$\omega = \sum_{x,y=1}^{\omega} \frac{1}{m} \sum_{a=1}^{m} e^{2\pi i a(q^x - q^y)/m} = \frac{1}{m} \sum_{a=1}^{m} \left| \sum_{x=1}^{\omega} e^{2\pi i a q^x/m} \right|^2.$$

Therefore

$$\begin{aligned} \sum_{\substack{a=1 \\ (a,p)=1}}^{m} \left| \sum_{x=1}^{\omega} e^{2\pi i a q^x/m} \right|^2 &= \sum_{a=1}^{m} \left| \sum_{x=1}^{\omega} e^{2\pi i a q^x/m} \right|^2 - \sum_{\substack{a=1 \\ (a,p)=p}}^{m} \left| \sum_{x=1}^{\omega} e^{2\pi i a q^x/m} \right|^2 \\ &= m\omega - \sum_{a_1=1}^{m_1} \left| \sum_{x=1}^{p\omega_1} e^{2\pi i a_1 q^x/m_1} \right|^2 \\ &= m\omega - p^2 m_1 \omega_1 = 0, \end{aligned}$$

hence proving (6.5).

6.6. OTHER FORMS OF EXPONENTIAL SUMS

The current chapter serves only as a basic introduction to the idea of exponential sums and as such we do not intend to go any deeper into the topic. We note however that there are certainly quite a number of exponential sums forms which have not been mentioned, including:

- Sums the form

$$S(f) = \sum_{x=1}^{q} e^{2\pi i f(x)/q}$$

  where q is composite,

- Sums where the polynomial f has irrational coefficients,

- Sums with recurrence sequences,

and the list certainly goes on from here. Further references on exponential sums can be found in [Vin85], [Vin04], [Shp02], as well as [Kor92] which we mentioned earlier.

CHAPTER 7

MULTIPLICATIVE CHARACTER SUMS OF THE LARGEST PRIME DIVISOR

In this chapter, we present our result on the upper bound for the character sum

$$\sum_{n \leq x} \chi\big(a + P(n)\big)$$

where, as before, $P(n)$ denotes the largest prime divisor of a positive integer n, a is an integer, and χ is a primitive Dirichlet character modulo a positive integer q with $(a, q) = 1$.

This chapter was based on a paper authored together with S. Balasuriya and I. Shparlinski [BSSar].

7.1. CHARACTER SUMS

Character sums refer to sums of Dirichlet characters and it is similar to the idea of exponential sums outlined in the previous chapter. There are of course some distinctions between the two concepts (in particular, the exponential function is additive while Dirichlet characters are multiplicative functions), but in number theory, the applications and principles behind the two concepts are almost identical.

7.2. REQUIRED RESULTS

In Chapter 4 we mentioned how the study of the largest prime divisors is invariably linked to the study of smooth numbers, and indeed, one of the main ingredient in this chapter is the distribution of $\psi(x,y) = \#\{n \leq x : P(n) \leq y\}$.

The result we need is the following lemma, which is a substantially relaxed version of Corollary 1.3 in a paper by Hildebrand and Tenenbaum [HT93]:

Lemma 7.1. *Let $u = \log x/\log y$, where $x \geq y > 1$. If $u \to \infty$ as $x \to \infty$, and $u \leq y^{1/2}$, then*

$$\psi(x,y) = xu^{-u+o(u)}.$$

For the next lemma, letting $y = x^{1/u}$ as before, we define $\mathcal{P}_m = \mathcal{P}[L_m, x/m]$ to be the set of primes p such that $L_m \leq p \leq x/m$, where $L_m = \max\{y, P(m)\}$. We have the following lemma from [BHS05]:

Lemma 7.2. *Let $x \geq y > 0$. For any two functions $h(k)$ and $f(k)$, if $\max\{|h(k)|, |f(k)|\} \leq 1$, then for all positive integers k, we have*

$$\sum_{n\leq x} h\big(P(n)\big)f(n) = \sum_{m\leq x/y}\sum_{p\in\mathcal{P}_m} h(p)f(mp) + O\big(\psi(x,y)\big)$$

The next lemma is a relaxed version of the first theorem in [Rak94]. As before, $\tau(n)$

denotes the number of positive divisors of an integer n.

Lemma 7.3. *For any integers a and $q \geq 1$ with $(a,q) = 1$,*

$$\left|\sum_{p\leq x} \chi(p+a)\right| \ll x\tau(q)\log^5 x\left(\sqrt{\frac{1}{q}+\frac{q}{x}\tau^2(q)}+x^{-1/6}\tau(q)\right)$$

7.3. PROOF OF THE THEOREM

Theorem 7.4. *For any integers a and $q \geq 1$ with $(a,q) = 1$,*

$$\left|\sum_{n\leq x} \chi\big(a+P(n)\big)\right| \ll x\left(\frac{q^{o(1)}\log^5 x}{q^{1/4}}+w^{-2w/3+o(w)}\right)$$

where $w = (\log x)/(\log q)$.

Proof. We note that the above bound is trivial if $q \leq \log^{20} x$, therefore we are only interested with the values of $q > \log^{20} x$. Our main objective here is to find the upper bound for the sum

$$\sum_{n\leq x} \chi\big(P(n)+a\big),$$

and we start by separating this sum into two parts as follows: If we let $h(a) = \chi\big(P(n)+a\big)$ and $f(a) = 1$, for all integer a, then from Lemma 7.2 we can write

$$\sum_{n\leq x} \chi\big(P(n)+a\big) = \sum_{m\leq x/y}\sum_{p\in\mathcal{P}_m} \chi(p+a) + O\big(\psi(x,y)\big), \tag{7.1}$$

where $\mathcal{P}_m$ is as defined in Lemma 7.2.

There are now two parts to consider; namely the double sum and the error term. For the error term, if we choose $y = x^{1/u} = q^{1.5+o(1)}$, then

$$u = \frac{\log x}{\log y} \leq \log x \leq q \leq y^{1/2},$$

and as this satisfies the condition for Lemma 7.1, we can write

$$O\left(xu^{-u+o(u)}\right) = O\left(xw^{-2w/3+o(w)}\right) \tag{7.2}$$

where $w = \log x/\log q$.

For the double sum, by Lemma 7.3,

$$\left|\sum_{p\in\mathcal{P}_m}\chi(p+a)\right| \ll \frac{x\tau(q)\log^5 x}{m}\left(\sqrt{\frac{1}{q}+\frac{mq}{x}\tau^2(q)}+\left(\frac{x}{m}\right)^{-1/6}\tau(q)\right).$$

Since $\tau(q)\le q^{o(1)}$, we have

$$\left|\sum_{p\in\mathcal{P}_m}\chi(p+a)\right| \ll \frac{xq^{o(1)}\log^5 x}{m}\left(q^{-1/2}+x^{-1/2}m^{1/2}q^{1/2}+x^{-1/6}m^{1/6}\right).$$

and summing over m gives

$$\begin{aligned}\sum_{m\le x/y}&\left|\sum_{p\in\mathcal{P}_m}\chi(p+a)\right| \\ &\ll xq^{o(1)}\log^5 x\left(\frac{1}{q^{1/2}}\sum_{m\le x/y}\frac{1}{m}+\frac{q^{1/2}}{x^{1/2}}\sum_{m\le x/y}\frac{1}{m^{1/2}}+\frac{1}{x^{1/6}}\sum_{m\le x/y}\frac{1}{m^{5/6}}\right)\\ &\ll xq^{o(1)}\log^5 x\left(q^{-1/2}\log(x/y)+q^{1/2}y^{-1/2}+y^{-1/6}\right).\end{aligned}$$

Letting $y = q^{1.5+o(1)}$, we have

$$\sum_{m\le x/y}\left|\sum_{p\in\mathcal{P}_m}\chi(p+a)\right| \ll \frac{xq^{o(1)}\log^5 x}{q^{1/4}}. \tag{7.3}$$

Finally, from (7.2) together with (7.3), we have

$$\left|\sum_{n\le x}\chi\left(P(n)+a\right)\right| \ll \frac{xq^{o(1)}\log^5 x}{q^{1/4}} + O\left(xw^{-2w/3+o(w)}\right)$$

which gives the result of the theorem. □

BIBLIOGRAPHY

[Apo00] T. M. Apostol. *Introduction to analytic number theory*. Springer-Verlag, New York, 2000. Undergraduate Texts in Mathematics.

[Arn05] V. Arnold. Number-theoretical turbulence in Fermat-Euler arithmetics and large Young diagrams geometry statistics. *J. Math. Fluid Mech.*, 7(suppl. 1):S4–S50, 2005.

[BEPS81] P. T. Bateman, P. Erdős, C. Pomerance, and E. G. Straus. The arithmetic mean of the divisors of an integer. In *Analytic number theory (Philadelphia, PA, 1980)*, volume 899 of *Lecture Notes in Math.*, pages 197–220, Berlin, 1981. Springer.

[BHS05] W. D. Banks, G. Harman, and I. E. Shparlinski. Distributional properties of the largest prime factor. *Michigan Math. J.*, 53(3):665–681, 2005.

[BSSar] S. Balasuriya, I. E. Shparlinski, and D. Sutantyo. Multiplicative character sums with the euler function. *Studia Sci. Math. Hung.*, (to appear).

[CEP83] E. R. Canfield, P. Erdős, and C. Pomerance. On a problem of Oppenheim concerning "factorisatio numerorum". *J. Number Theory*, 17(1):1–28, 1983.

[CP05] R. Crandall and C. Pomerance. *Prime numbers*. Springer, New York, second edition, 2005. A computational perspective.

[Dav00] H. Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2000. Revised and with a preface by Hugh L. Montgomery.

[Dic30] K. Dickman. On the frequency of numbers containing prime factors of a certain relative magnitude. *Ark. Mat. Astr. Fys.*, 22:1–14, 1930.

[Hmy66] N. A. Hmyrova. On polynomials with small prime divisors. II. *Izv. Akad. Nauk SSSR Ser. Mat.*, 30:1367–1372, 1966.

[HT93] A. Hildebrand and G. Tenenbaum. Integers without large prime factors. *J. Théor. Nombres Bordeaux*, 5(2):411–484, 1993.

[HW80] G. H. Hardy and E. Wright. *An Introduction to the Theory of Numbers*. Oxford Science Publications, 1980.

[Kor92] N. M. Korobov. *Exponential Sums and their Applications*. Springer, 1st edition, 1992.

[LLS05] E. Levieil, F. Luca, and I. E. Shparlinski. Prime divisors of some shifted products. *Int. J. Math. Math. Sci.*, 19:3057–3073, 2005.

[LS05] F. Luca and I. E. Shparlinski. Prime divisors of shifted factorials. *Bull. London Math. Soc.*, 37(6):809–817, 2005.

[MTB06] S. J. Miller and R. Takloo-Bighash. *An invitation to modern number theory*. Princeton University Press, Princeton, NJ, 2006. With a foreword by Peter Sarnak.

[Ore48] O. Ore. On the averages of the divisors of a number. *Amer. Math. Monthly*, 55:615–619, 1948.

[Rak94] Z. Kh. Rakhmonov. On the distribution of the values of Dirichlet characters and their applications. *Trudy Mat. Inst. Steklov.*, 207:286–296, 1994.

[Shp85] I. E. Shparlinski. The number of prime divisors of recurrence sequences. *Mat. Zametki*, 38(1):29–34, 168, 1985.

[Shp90] I. E. Shparlinski. Some arithmetic properties of recurrence sequences. *Mat. Zametki*, 47(6):124–131, 1990.

[Shp02] I. E. Shparlinski. Exponential sums in coding theory, cryptology and algorithms. In *Coding theory and cryptology (Singapore, 2001)*, volume 1 of *Lect. Notes Ser. Inst.*

Math. Sci. Natl. Univ. Singap., pages 323–383. World Sci. Publ., River Edge, NJ, 2002.

[SS07] I. E. Shparlinski and D. Sutantyo. On the set of the largest prime divisors. *Publ. Math. Debrecen*, 71/1-2:95–100, 2007.

[Tim77] N. M. Timofeev. Polynomials with small prime divisors. *Taškent. Gos. Univ. Naučn. Trudy*, 548 Voprosy Mat.:87–91, 145, 1977.

[Vin54] I. M. Vinogradov. *Elements of number theory*. Dover Publications Inc., New York, 1954. Translated by S. Kravetz.

[Vin85] I. M. Vinogradov. *Selected works*. Springer-Verlag, Berlin, 1985. With a biography by K. K. Mardzhanishvili, Translated from the Russian by Naidu Psv [P. S. V. Naidu], Translation edited by Yu. A. Bakhturin.

[Vin04] I. M. Vinogradov. *The method of trigonometrical sums in the theory of numbers*. Dover Publications Inc., Mineola, NY, 2004. Translated from the Russian, revised and annotated by K. F. Roth and Anne Davenport, Reprint of the 1954 translation.

[Wey16] H. Weyl. Über die Gleichverteilung von Zahlen mod. Eins. *Math. Ann.*, 77(3):313–352, 1916.

[Wir67] E. Wirsing. Das asymptotische Verhalten von Summen über multiplikative Funktionen. II. *Acta Math. Acad. Sci. Hungar.*, 18:411–467, 1967.

INDEX