Mertens' Theorem for Arithmetical Dynamical Systems

Sawian Jaidee

A thesis submitted to the School of Mathematics of the University of East Anglia in partial fulfilment of the requirements for the degree of Doctor of Philosophy

January 2010

Acknowledgements

First of all, I am heartily thankful to my supervisors, Prof. Shaun Steven and Prof. Thomas Ward, who enabled me to improve my mathematical understanding in my research. I'm also very grateful to be their student because they are very nice and they always gave me some kindly comments and suggestions. Without their supervision and support I could not have completed my thesis so in my life, I won't forget them. I offer my regards and blessing to them for helping me during four years.

Next, I would like to acknowlege the financial support of the office of the Higher Education Commission Thailand (the second program Strategic Scholarships) for doing research in the UK during four years. If I did not get this funding, I would not come to study in the UK, so it is my pleasure to thank the Higher Education Commission Thailand for giving me an opportunity to get very worthwhile and fantastic experiences in the UK.

Lastly, I would like to thank everyone who helped me during the completion of the research, espectially, to my colleagues in school of Mathematics in UEA, UK (Stuart, Anthony, Omar, Matthew Bolton, Ouamporn, Apisit and so on).

Contents

1 Preliminaries **1**

1.1 Introduction 1

1.2 Prime Numbers 3

1.3 Some Basic Definitions and Notation 8

1.3.1 Notation 8

1.3.2 Möbius Inversion Formula 10

1.3.3 Bernoulli Numbers and the Bernoulli Functions 13

1.3.4 Primitive Roots Modulo n 14

1.3.5 Resultants of Polynomials 15

1.3.6 Roots of Unity 16

1.4 The Harmonic Series 17

2 The Arithmetic of Dynamical Systems **22**

2.1 Dynamical Systems 22

2.2 Periodic Points and Orbits 23

2.3 Topological Entropy 26

3 S-integer Dynamical Systems **33**

3.1 Toral Endomorphisms 33

3.2 Non-Archimedean Valuations 37
3.3 Completion and Places of $\mathbb{A}$-fields 43
3.4 S-integer Dynamical Systems 48
3.5 Periodic Points and Topological Entropy of S-integer maps 51
3.6 Growth Rate of Periodic Points 52

4 Mertens' Theorem in Zero Characteristic **55**
4.1 Prime Orbit Theorem and Mertens' Theorem for Orbits 55
4.2 Mertens' Theorem for Toral Automorphisms 61
4.3 Mertens' Theorem for Slow Growth 72

5 Intermediate Growth Examples **91**
5.1 Density of Prime Numbers 91
5.2 An Arithmetic Argument 93
5.3 Finite Sets of Primes 99
5.4 Infinitely Many Primes 109

Abstract

We find an analogue of Mertens' Theorem of analytic number theory for S-integer dynamical systems, which are constructed from arithmetic data, namely $K = \mathbb{Q}$, $\xi = 2$, and S a subset of rational primes. The dynamical Mertens' Theorem gives asymptotics for weighted averages of numbers of closed orbits. Everest, Miles, Stevens and Ward have already proved such a theorem when S is finite. Here, we will be interested in the cases: i) S is co-finite, and ii) S and S^c are infinite. Moreover, we give a dynamical Mertens' Theorem for some toral automorphisms, improving previously obtained error terms.

Chapter 1

Preliminaries

1.1 Introduction

In this thesis, certain growth problems in dynamical system are studied related to the setting of work of Parry and Pollicott [25] drawing analogies between prime numbers and closed orbits. These problems are modelled on Mertens' Theorem.

In analytic number theory, Mertens' Theorem is a formula for asymptotics of the weighted sum over primes (Section 1.2). In this sense, it is concerned with the distribution of prime numbers.

In a dynamical system, Mertens' Theorem is motivated by Mertens' Theorem of analytic number theory so it is defined to be the sum of some positive function concerning the topological entropy (Section 2.3) and the sum is taken over closed orbits. There are several papers which have pointed to the similarity of Mertens' Theorem in analytic number theory and in dynamics. The following list will show some of these papers:

1. Parry and Pollicott [25], and Sharp [29] proved an analogue of the prime number

theorem (see Section 1.2) for closed orbits of axiom A flows.

2. Parry [26] counted the number of closed orbits of a suspension of a shift of finite type and gave the asymptotic formula by following the Wiener-Ikehara proof of the prime number theorem.

3. Waddington [33] found asymptotics for an unweighted orbit-counting sum for quasihyperbolic toral automorphisms (see Section 3.1).

4. Noorani [24] considered closed orbits of an ergodic toral automorphismand proved an analogue of Mertens' Theorem for closed orbits.

5. Everest, Miles, Stevens and Ward [8] studied the counting of closed orbits for S-integer dynamical system (see Section 3.4) arising in non-hyperbolic dynamics. Also, they have shown the asymptotic formula of a dynamical Mertens' Theorem when S is finite.

In this work, we begin by considering the circle doubling map (see Section 2.2), which is the simplest example of a dynamical system. For this map, we can obtain the dynamical Mertens' Theorem formula directly and we improve the error terms in the formula by applying the Euler-Maclaurin Summation Formula (see Section 1.4). A toral endomorphism (see Section 3.1) is a generalization of the circle doubling map. In Section 4.2, we improve the work of Noorani [24] by refining the error terms in the formula for the hyperbolic and the quasihyperbolic toral automorphism (see Section 3.1) and correcting the constant in the main term. Again, we use the Euler-Maclaurin Summation Formula to refine the error terms. In Section 5.3, we look at how the last paper (in the above list) has been done for S-integer dynamical system, which is another generalization of the circle doubling map. The case of S co-finite will be

studied in Section 4.3 and we will notice that Mertens' Theorem in its usual form is not interesting. However, we change it to the suitable form in (40) (in Section 4.3) so that we can use it to derive an asymptotic expression of this form. Moreover, by extending some results in this paper, we obtain an interesting Mertens' Theorem formula (see Section 5.4) when S and S^c are infinite by giving some explicit examples.

1.2 Prime Numbers

We start by describing some of the background in number theory. For instance, the infinitude of prime numbers and the prime number theorem, which grow out of the fundamental theorem of arithmetic. For every real $x > 0$, let $\pi(x)$ be the number of primes less than or equal to x. Thus π is the function counting the prime numbers. The first natural question about prime numbers is: How many primes are there? The Greek mathematician, Euclid, may have been the first to give a proof that there are infinitely many prime numbers, which is equivalent to the following proposition.

Proposition 1.1. *$\pi(x) \to \infty$ as $x \to \infty$.*

Proof. $\pi(x)$ is clearly monotone increasing. If it is bounded, then, for some n,

$$\{p_1, p_2, \ldots, p_n\}$$

comprises all the primes. Let

$$N = 1 + p_1 p_2 \cdots p_n,$$

which is an integer bigger than 1. By the Fundamental Theorem of Arithmetic, N can be factored into primes. Let p be a prime dividing N. If $p | p_1 p_2 \cdots p_n$, then

$$p | N - p_1 p_2 \cdots p_n = 1,$$

which is impossible. Thus the prime p is another prime, not in $\{p_1, p_2, \ldots, p_n\}$, which is absurd. Hence $\pi(x)$ is an unbounded function. $\square$

We remark that a new prime can be generated from $1 + p_1 p_2 \cdots p_n$ by factorizing, but probably $1 + p_1 p_2 \cdots p_n$ is not the next prime.

The next question arising naturally is: How are the primes distributed among the natural numbers? Equivalently: What does the behaviour of π look like? and Can it be compared with simpler functions? This approach leads to results of an asymptotic nature. Returning to the proof of the previous proposition, this proof indeed says more: if $p_1, p_2, \ldots$ are the primes listed in order of size, then the proof shows that

$$p_{n+1} \leq 1 + p_1 p_2 \cdots p_n.$$

So if $u_1 = 2,\ u_{n+1} = u_1 \cdots u_n + 1$, then

$$\pi(x) \geq \min\{n : u_n \geq x\}, \tag{1}$$

giving a very weak rate of growth.

Attempts to improve (1) have been (and remain) a driving force in number theory. According to [27], in 1798, C.F. Gauss (who was only 15 years old) conjectured that

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

This assertion was proved by Hadamard and de la Vallée Poussin in 1896. (Previously, P.L. Chebyshev had shown a weaker result which says that if $\lim_{x\to\infty} \frac{\pi(x)}{x/\log x}$ exists, it must be 1.) Nowadays, we know this result as the *Prime Number Theorem*, giving a rough description of how the primes are distributed:

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

The proof of the Prime Number Theorem exploited analytical properties of the Riemann zeta function,

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}.$$

In 1874 [22], the Polish-Austrian mathematician Franciszek Mertens studied the sum of the reciprocals of the prime numbers and he published the famous theorem on the sum as follows.

Theorem 1.2 (Mertens (1874))**.** *Let $x \geq 1$ be the any real number. Then*

$$\sum_{p \leq x} \frac{1}{p} = \log\log[x] + \gamma + \sum_{m=2}^{\infty} \mu(m) \frac{\log\{\zeta(m)\}}{m} + \delta, \tag{2}$$

where γ is the Euler constant, μ is the Möbius function, ζ is the Riemann zeta function and

$$|\delta| < \frac{4}{\log([x]+1)} + \frac{2}{[x]\log[x]}.$$

It follows that

$$\sum_{p \leq x} \frac{1}{p} = \log\log x + B + O\left(\frac{1}{\log x}\right),$$

where Mertens' constant $B = \gamma + \sum_p \left\{\log(1 - \frac{1}{p}) + \frac{1}{p}\right\}$ has the approximate value 0.2614972128...[32, page 16]. An equivalent form of Mertens' Theorem given in terms of the product taken over all primes p is

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log(x)}. \tag{3}$$

An elementary proof of this can be found in [15]. Both (2) and (3) are known as *Mertens' Theorem of analytic number theory* or, sometimes, the *classical Mertens' Theorem*. These again say something about the distribution of prime numbers.

Another theme in number theory is the analogy between number fields (like $\mathbb{Q}$) and function fields (like $\mathbb{F}_p(t)$). A particularly clear exposition of this may be found

in [37]. The ring $A = \mathbb{F}_p[t]$, the polynomial ring over $\mathbb{F}_p$, has many properties in common with the ring of integers $\mathbb{Z}$. Here we will be interested in an analogue of the Prime Number Theorem obtained by using the zeta function associated to A, which is an analogue of the classical zeta function.

Definition 1.3. The zeta function of A is defined by the infinite series

$$\zeta_A(s) = \sum_{\substack{P \in A \\ P \text{ monic}}} \frac{1}{|P|^s},$$

where $|P| = p^{\deg(P)}$, and the sum is taken over all monic polynomials in A.

For a positive integer d, define a_d to be the number of monic irreducible polynomials in A of degree d. The statement of the classical Prime Number Theorem says that $\pi(x)$ is asymptotic to $x/\log x$ as $x \to \infty$. The analogue of the Prime Number Theorem here gives the asymptotic expression of $a_n,\ n \geq 1$ which is illustrated below.

Theorem 1.4 (The Prime Number Theorem for polynomials)**.**

$$a_n = \frac{p^n}{n} + O\left(\frac{p^{\frac{n}{2}}}{n}\right).$$

If we set $x = p^n$, then

$$a_n = \frac{x}{\log_p x} + O\left(\frac{\sqrt{x}}{\log_p x}\right).$$

Proof. The unique factorization of elements in A into irreducibles shows that

$$\begin{aligned}
\zeta_A(s) &= \prod_{\substack{P \text{ irreducible} \\ P \text{ monic}}} (1 - |P|^{-s})^{-1} \\
&= \prod_{\substack{P \text{ irreducible} \\ P \text{ monic}}} (1 - p^{-s\deg(P)})^{-1} \\
&= \prod_{d=1}^{\infty} (1 - p^{-ds})^{-a_d}
\end{aligned}$$

(the first two products and the sum below are taken over all monic irreducible polynomials).

Since there are exactly p^d monic polynomials of degree d in A, it follows that

$$\sum_{\substack{\deg(P)\leq d \\ P \text{ monic}}} |P|^{-s} = 1 + \frac{p}{p^s} + \frac{p^2}{p^{2s}} + \cdots + \frac{p^d}{p^{ds}}.$$

Consequently,

$$\zeta_A(s) = \frac{1}{1-pu},$$

where $u = p^{-s}$.

Hence

$$\frac{1}{1-pu} = \prod_{d=1}^{\infty}(1-u^d)^{-a_d}.$$

Taking the logarithmic derivative of both sides and then multiplying the result by u, then we get

$$\frac{pu}{1-pu} = \sum_{d=1}^{\infty} \frac{da_d u^d}{1-u^d}$$

Expanding both sides into power series by using geometric series and then comparing coefficients of u^n, we eventually get the following beautiful formula, which was known to Gauss:

$$\sum_{d|n} da_d = p^n. \tag{4}$$

Applying the Möbius inversion formula to (4) in order to write a_n in general term, which is

$$a_n = \frac{1}{n}\sum_{d|n} \mu(d) p^{\frac{n}{d}}.$$

To see how big the sequence a_n is, we may write as

$$a_n = \frac{p^n}{n} - \frac{p^{\frac{n}{2}}}{n} + \frac{1}{n} \sum_{\substack{d|n, \\ d\neq 1,2}} \mu(d) p^{\frac{n}{d}}. \tag{5}$$

Let $N = \{p_1, p_2, \ldots, p_t\}$ be the set of distinct primes dividing n. Recall that, for $d \mid n$,

$$\mu(d) = \begin{cases} (-1)^{|T|} & \text{if } d = \prod_{i \in T} p_i, \quad \text{for some} \quad T \subseteq \{1, 2, \ldots, t\} \\ 0 & \text{otherwise.} \end{cases}$$

So the total of terms in the sum $\sum_{d|n} \mu(d)$ is 2^t and it is easy to see that $2^t \leq p_1 p_2 \cdots p_t \leq n$. Consequently,

$$\begin{aligned} \left| a_n - \frac{p^n}{n} \right| &\leq \frac{p^{\frac{n}{2}}}{n} + \frac{1}{n} \sum_{\substack{d|n, \\ d \neq 1,2}} |\mu(d)| p^{\frac{n}{d}}. \\ &\leq \frac{p^{\frac{n}{2}}}{n} + p^{\frac{n}{3}}. \end{aligned}$$

Hence

$$a_n = \frac{p^n}{n} + O\left(\frac{p^{\frac{n}{2}}}{n}\right).$$

□

We note that the trick in (5) (where exponential growth allows the $d = n$ term in a sum over of n to dominate) will be repeatedly seen in this thesis.

1.3 Some Basic Definitions and Notation

1.3.1 Notation

The following notation and conventions are used systematically in this thesis.

- $\mathbb{Z}$ means the set of all integers.
- $\mathbb{Q}$ means the set of all rational numbers.
- $\mathbb{Q}^\times$ means the set of all non-zero rational numbers.

- $\mathbb{R}$ means the set of all real numbers.
- $\mathbb{C}$ means the set of all complex numbers.
- $\mathbb{N}$ means the set of all non-negative integers or all natural numbers.
- $\mathbb{N}_0$ means the set of all negative integers or all natural numbers.
- $\mathbb{F}_p$ means a finite field p elements.
- $\mathbb{P}$ means the set of all prime numbers.
- For any set $A,\ B,\ B^A$ means the set of all functions from A to B.
- $a \mid b$ means a divides b.
- $[x]$, $\{x\}$ is the integer and fractional parts of the real number x, respectively. In fact, $x = [x] + \{x\}$.
- The letter p, with or without subscript, denotes a prime number.
- $|\cdot|_p$ is the p-adic valuation.
- $m_p := m_p(2)$ is the multiplicative order of $2 \pmod p$.
- For $T \subseteq \mathbb{P},\ |x|_T = \prod_{p \in T} |x|_p$ for any $x \in \mathbb{R}$.
- For $T \subseteq \mathbb{P}$, $o_T = \text{lcm}\{m_p \ :\ p \in T\}$.
- $|A|$ denotes the cardinality of a set A.
- Given a set U, for $A \subseteq U$, $A^c = U \setminus A$, the complement of A with respect to U.
- φ is Euler's totient function.

- γ is the Euler-Mascheroni constant.
- μ is the Möbius function.
- $\mathrm{Res}(p, q)$ denotes the resultant of polynomials p, q in $k[x]$, for k any field.
- $\mathbb{T}^d = (\mathbb{R}/\mathbb{Z})^d$ means the d-dimensional torus.
- $(x_1, x_2)^t = \binom{x_1}{x_2}$ for $(x_1, x_2) \in \mathbb{T}^2$.

Landau's notation : the big O-notation, the little o-notation and $\sim$ are often used and are defined as follows: Given two functions f and g from $\mathbb{R}$ to $\mathbb{R}$:

- $f = O(g)$ means that there exists $A > 0$ such that $|f(x)| < A|g(x)|$ for all $x > 0$; that is the ratio $\frac{f(x)}{g(x)}$ stays bounded as $x \to \infty$.
- $f = o(g)$ means that $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$; that is $g(x)$ grows much faster than $f(x)$.
- $f \sim g$ means that $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

1.3.2 Möbius Inversion Formula

Definition 1.5. A function $f : \mathbb{N} \to \mathbb{C}$ is said to be an *arithmetic function*.

Definition 1.6. An arithmetic function $f : \mathbb{N} \to \mathbb{C}$ is *multiplicative* if for any relatively prime $m, n \in \mathbb{N}$,

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

Definition 1.7. The *Möbius function* $\mu(n)$ is defined as follows:

1. $\mu(1) = 1$;
2. $\mu(n) = 0$ if n has a squared factor;

3. $\mu(p_1 p_2 \cdots p_k) = (-1)^k$ if all the primes $p_1, p_2, \ldots, p_k$ are different.

For instance, $\mu(2) = -1,\ \mu(4) = 0,\ \mu(6) = 1$. Indeed, $|\mu(n)| \leq 1$ for any natural number n. The Möbius function is multiplicative. The sum over all positive divisors of n of the Möbius function is zero except when $n = 1$.

Theorem 1.8.

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

or

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) = \begin{cases} 1 & if\ n = 1, \\ 0 & n > 1. \end{cases} \tag{6}$$

Proof. For each $k \geq 1$, write

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}.$$

Then we have

$$\begin{aligned} \sum_{d|n} \mu(d) &= 1 + \sum_{i=1}^{k} \mu(p_i) + \sum_{i,j=1}^{k} \mu(p_i p_j) + \cdots + \mu(p_1 p_2 ... p_k) \\ &= 1 - k + \binom{k}{2} - \binom{k}{3} + \cdots + (-1)^k \\ &= (1-1)^k = 0, \end{aligned}$$

while, if $n = 1,\ \mu(n) = 1$. □

The formula (6) is rich in application. For instance, it is applied for counting closed orbits in a dynamical system.

Theorem 1.9 (Möbius Inversion Formula)**.** *Let f and g be arithmetic functions. The*

two following properties are equivalent:

$$\begin{aligned} (i)\quad g(n) &= \sum_{d|n} f(d) \qquad (n \geq 1), \\ (ii)\quad f(n) &= \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right) \qquad (n \geq 1). \end{aligned}$$

Proof. ((i)⇒(ii)). In fact

$$\begin{aligned} \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{c|\frac{n}{d}} f(c) && (7) \\ &= \sum_{cd|n} \mu(d) f(c) && (8) \\ &= \sum_{c|n} f(c) \sum_{c|\frac{n}{c}} \mu(d). && (9) \end{aligned}$$

By Theorem 1.8, the inner sum in (9) is 1 if $\frac{n}{c} = 1$ (i.e $n = c$), and 0 otherwise so that the repeated sum in (9) reduces to $f(n)$.

((ii)⇒(i)). We have

$$\begin{aligned} \sum_{d|n} f(d) &= \sum_{d|n} f\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \sum_{c|\frac{n}{d}} \mu\left(\frac{n}{cd}\right) g(c) \\ &= \sum_{cd|n} \mu\left(\frac{n}{cd}\right) g(c) \\ &= \sum_{c|n} g(c) \sum_{d|\frac{n}{c}} \mu\left(\frac{n}{cd}\right) = g(n). \end{aligned}$$

□

1.3.3 Bernoulli Numbers and the Bernoulli Functions

Let $(b_r(x))$ be the sequence of polynomial defined on $[0,1]$ by the conditions

$$\begin{aligned} b_0(x) &= 1, \\ b_r'(x) &= r b_{r-1}(x) \quad (r \geq 1) \\ \int_0^1 b_r(x) &= 0 \quad (r \geq 1). \end{aligned}$$

It is given in terms of the *generating function* as

$$\frac{ye^{xy}}{e^y - 1} = \sum_{r=0}^{\infty} b_r(x) \frac{y^r}{r!},$$

which allow us to calculate the b_r. Thus we have

$$\begin{aligned} b_0(x) &= 1, \\ b_1(x) &= x - \frac{1}{2} \\ b_2(x) &= x^2 - x + \frac{1}{6} \\ b_3(x) &= x^3 + \frac{3}{2}x^2 - \frac{1}{2}x \\ b_4(x) &= x^4 - 2x^3 + x^2 + \frac{1}{30} \\ b_5(x) &= x^5 - \frac{5}{2}x^4 + \frac{5}{4}x^3 - \frac{1}{6}x^2, \end{aligned}$$

and so on. Since $b_k(x)$ is continuous on a compact set, it is bounded: that is, for $x \in [0,1]$,

$$|b_k(x)| \leq C_k, \tag{10}$$

for some constant C_k depending on k.

Definition 1.10. The r^{th} *Bernoulli function*, denoted by $B_r(x)$, is the periodic function of period 1 on $\mathbb{R}$ which coincides with b_r on $[0,1)$ (i.e. $B_r(x) := b_r(\{x\})$ for all $x \in \mathbb{R}$). The r^{th} *Bernoulli number* is denoted by B_r where

$$B_r := B_r(0).$$

We notice that $B_{2r+1} = 0$ for $r > 0$. Some values of B_{2r} for $r \geq 0$ and B_1 are illustrated in the table below:

r	0	1	2	4	6	8	10
B_r	1	$-\frac{1}{2}$	$\frac{1}{6}$	$-\frac{1}{30}$	$\frac{1}{42}$	$-\frac{1}{30}$	$\frac{5}{66}$

1.3.4 Primitive Roots Modulo n

For $n \in \mathbb{N}$, the set

$$Z_n^\times = \{a \in \mathbb{N} \ : \ 1 \leq a \leq n-1 \text{ and } \gcd(a, n) = 1\}$$

forms a group with multiplication modulo n as the operation. It is equivalent to the congruence classes coprime to n and it is sometimes called the *group of units modulo* n or the *group of primitive classes modulo* n.

Lemma 1.11. *[28, page 92]* $Z_n^\times$ *is cyclic if and only if* n *is equal to* $1, 2, 4, p^k$, $2p^k$ *where* p^k *is a power of an odd prime number.*

Definition 1.12. Suppose $Z_n^\times$ is a cyclic group. A *primitive root modulo* n (or *primitive element* of $Z_n^\times$) is a generator of $Z_n^\times$.

Definition 1.13. For $a \in Z_n^\times$, the lowest power of a which is congruent to 1 (mod n) is called the *multiplicative order* of a modulo n, denoted by $m_n(a)$.

Let $\varphi(n)$ be the number of elements in $Z_n^\times$ where $\varphi(n)$ is Euler's totient function. By Euler's theorem, we have $a^{\varphi(n)} \equiv 1 \pmod{n}$ for every element a in $\in Z_n^\times$. This implies that a is a primitive root modulo n if and only if $m_n(a) = \varphi(n)$.

Example 1.14. For $n = 14$, we have

$$Z_{14}^\times = \{1, 3, 5, 9, 11, 13\}.$$

Thus $|Z_n^\times| = \varphi(14) = 6$. The following table will illustrate how to figure out the primitive roots modulo 14.

n	$n,$	$n^2,$	$n^3,$	$n^4,$	$n^5,$	n^6	$,\ldots$	(mod 14)
1	1,							
3	3,	9,	13,	11,	5,	1,		
5	5,	11,	13,	9,	3,	1,		
9	9,	11,	1,					
11	11,	9,	1,					
13	13,	1,						

From the above table, $3, 5$ are primitive roots modulo 14 because they are generators of $Z_{14}^\times$, and $m_{14}(3) = m_{14}(5) = 6$. Also, we get $m_{14}(1) = 1,\ m_{14}(9) = 3,\ m_{14}(11) = 3,\ m_{14}(13) = 2$.

1.3.5 Resultants of Polynomials

Let k be any field. Define $k[x]$ to be the set of all polynomials having coefficients in k. Then $k[x]$ is a commutative ring with identity and it is a unique factorization domain.

Definition 1.15. For $p, q \in k[x]$, we write p, q in terms of linear factors

$$\begin{aligned} p(x) &= a_0(x - r_1)(x - r_2)\cdots(x - r_n) \\ q(x) &= b_0(x - s_1)(x - s_2)\cdots(x - s_m), \end{aligned}$$

for some natural numbers m, n. The *resultant* of p and q, denoted by $\mathrm{Res}(p, q)$ is defined to be

$$\mathrm{Res}(p, q) = a_0^m b_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(r_i - s_j).$$

By the above definition, we immediately obtain the following theorem.

Theorem 1.16. *Given two polynomials p, q in $k[x]$,* $\mathrm{Res}(p, q) = 0$ *if and only if p, q have at least one common root.*

Moreover, according to [1, page 121], Sylvester gave an explicit formula for the resultant of any two polynomials p, q having coefficients in k in terms of a determinant in the coefficients as follow:

Definition 1.17. For $p, q \in k[x]$, we write

$$\begin{aligned} p(x) &= a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \\ q(x) &= b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m, \end{aligned}$$

for some natural numbers m, n. Then $\mathrm{Res}(p, q)$ can be expressed as the $(m+n) \times (m+n)$ determinant:

$$\mathrm{Res}(f, g) = \begin{vmatrix} a_n & a_{n-1} & \cdots & a_1 & a_0 & 0 & 0 & 0 \\ 0 & a_n & \cdots & a_2 & a_1 & a_0 & 0 & 0 \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & \\ 0 & 0 & 0 & a_n & a_{n-1} & \cdots & a_1 & a_0 \\ b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & 0 & 0 \\ 0 & b_m & \cdots & b_2 & b_1 & b_0 & 0 & 0 \\ & & \ddots & \ddots & \ddots & \ddots & \ddots & \\ 0 & 0 & 0 & b_m & b_{m-1} & \cdots & b_1 & b_0 \end{vmatrix}.$$

This formula is known as *Sylvester's Form of the Resultant.*

1.3.6 Roots of Unity

Definition 1.18. Let k be any field. The n^{th} *roots of unity* in k are the elements ω in k such that $\omega^n = 1$. Equivalently, they are all the roots of the polynomial $x^n - 1$.

It is important that we have to be careful about which field k we are considering. Here we are going to exhibit the n^{th} roots of unity in $k = \mathbb{R}$ and $k = \mathbb{C}$.

- If $k = \mathbb{R}$, then the n^{th} roots of unity of this field are 1 and -1, when n is even; just 1 when n is odd.

- If $k = \mathbb{C}$, the Fundamental Theorem of Algebra assures us that the polynomial $x^n - 1$ has exactly n roots (counting multiplicities). Comparing $x^n - 1$ with its formal derivative, nx^{n-1} , we see that they are coprime, and therefore all the roots of $x^n - 1$ are distinct. That is, there exist n distinct complex numbers ω such that $\omega^n = 1$. All the n^{th} roots of unity are:

$$\zeta^k = e^{2\pi ki/n} = \cos(2\pi k/n) + i\sin(2\pi k/n),$$

for $k = 1, 2, ..., n-1$, where

$$\zeta = e^{2\pi i/n} = \cos(2\pi/n) + i\sin(2\pi/n).$$

Definition 1.19. Let k be a field. We call an element ω in k a *root of unity* if there exists a natural number n such that $\omega^n - 1 = 0$. It means that an element ω is a root of unity in k if ω is an n^{th} root of unity in k, for some natural number n.

1.4 The Harmonic Series

The harmonic series is the infinite series

$$\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots$$

which is divergent. The partial sum is given by

$$\sum_{n \leq N} \frac{1}{n} = \log N + \gamma + O(1/N), \tag{11}$$

where

$$\gamma = 1 - \int_1^\infty \frac{\{t\}}{t^2} dt$$

is the *Euler-Mascheroni constant*. The equation (11) may be proved by the Euler Summation Formula (ESF). Since we will later use ESF, we indicate the proof of (11) here. Before giving the proof, let us recall the statement of ESF as follows:

Theorem 1.20. *[2, Theorem 3.1] Let $a < b$ be real numbers, and suppose that f is a complex valued function defined on $[a, b]$ with a continuous derivative on (a, b). Then*

$$\sum_{a<n\leq b} f(n) = \int_a^b f(t)\, dt + \int_a^b \{t\} f'(t)\, dt - f(b)\{b\} + f(a)\{a\}.$$

Lemma 1.21. *There is a constant $\gamma,\ 0 < \gamma < 1$, with the property that*

$$\sum_{n\leq N} \frac{1}{n} = \log N + \gamma + O(1/N).$$

Proof. We will prove this by using Euler's Summation Formula with

$$f(t) = \frac{1}{t} \quad \text{and} \quad a = 1, b = N > 1.$$

Applying ESF,

$$\begin{aligned} \sum_{1<n\leq N} \frac{1}{n} &= \int_1^N \frac{1}{t}\, dt + \int_1^N \frac{\{t\}}{t^2}\, dt \\ &= \log N - \int_1^N \frac{\{t\}}{t^2}\, dt. \end{aligned}$$

Then

$$\sum_{n\leq N} \frac{1}{n} = \log N + 1 - \int_1^N \frac{\{t\}}{t^2}\, dt.$$

$$\int_1^N \frac{\{t\}}{t^2}\, dt = \int_1^\infty \frac{\{t\}}{t^2}\, dt - \int_N^\infty \frac{\{t\}}{t^2}\, dt. \tag{12}$$

The first term on the right hand side in (12) converges since it is bounded above by

$$\int_1^\infty \frac{1}{t^2}\,dt = 1.$$

Since

$$\int_N^\infty \frac{\{t\}}{t^2}\,dt \le \int_N^\infty \frac{1}{t^2}\,dt = \frac{1}{N},$$

it follows that

$$\int_N^\infty \frac{\{t\}}{t^2}\,dt = O(1/N).$$

Now we have

$$\sum_{n\le N} \frac{1}{n} = \log N + 1 - \int_1^\infty \frac{\{t\}}{t^2}\,dt + O(1/N).$$

Hence

$$\sum_{n\le N} \frac{1}{n} = \log N + \gamma + O(1/N),$$

where

$$\gamma = 1 - \int_1^\infty \frac{\{t\}}{t^2}\,dt.$$

Since

$$0 < \int_1^\infty \frac{\{t\}}{t^2}\,dt < \int_1^\infty \frac{1}{t^2}\,dt = 1,$$

it follows that

$$0 < 1 - \int_1^\infty \frac{\{t\}}{t^2}\,dt < 1.$$

□

In addition, Tom M. Apostol [3, page 410] has mentioned that γ has a numerical value correct to 20 decimals; that is $\gamma = 0.57721566490153286060\ldots$ and it is not known whether it is rational or irrational.

In this section, we will refine the remainder term in (11) by using the Euler-Maclaurin Summation Formula (EMSF) shown below.

Theorem 1.22 (Euler-Maclaurin Summation Formula)**.** *[32, Theorem 4] Let k be a nonnegative integer and f be $(k+1)$-times differentiable on $[a,b]$ with $a, b \in \mathbb{Z}$. Then*

$$\begin{aligned}\sum_{a<n\leq b} f(n) &= \int_a^b f(t)dt + \sum_{r=0}^{k} \frac{(-1)^{r+1}}{(r+1)!}(f^r(b) - f^r(a))B_{r+1} \\ &\quad -\frac{(1)^k}{(k+1)!}\int_a^b B_{k+1}(t)f^{(k+1)}(t)dt,\end{aligned}$$

where $B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = 0, B_4 = -\frac{1}{30}, \cdots$ are the Bernoulli numbers.

Proof. The proof of this theorem may be seen in [32, pages 5, 6]. □

Now we will apply the EMSF to the partial sum of the diverging harmonic series generalizing Lemma 1.21.

Lemma 1.23. *For integers $x > 0$,*

$$\sum_{n\leq x} \frac{1}{n} = \log x + \gamma - \sum_{r=0}^{k-1} \left(\frac{B_{r+1}}{r+1}\right) \frac{1}{x^{r+1}} + O(1/x^{k+1})$$

for any $k \in \mathbb{N}_0$.

Proof. Put $f(t) = \frac{1}{t}$, $a = 1$ and $b = x$ in Theorem 1.22. Then

$$\sum_{1<n\leq x} \frac{1}{n} = \log x + \sum_{r=0}^{k} \frac{(-1)^{r+1}}{(r+1)!}\left[\frac{(-1)^r r!}{x^{r+1}} - (-1)^r r!\right] B_{r+1} - \int_1^x \frac{B_{k+1}(t)}{t^{k+2}}dt.$$

Rearranging the middle term of the above equation in the right hand side and adding 1 to both side of this equation, we can reach

$$\sum_{1\le n\le x}\frac{1}{n}=1+\log x+\sum_{r=0}^{k}\frac{B_{r+1}}{r+1}-\sum_{r=0}^{k}\left(\frac{B_{r+1}}{r+1}\right)\frac{1}{x^{r+1}}-\int_1^x\frac{B_{k+1}(t)}{t^{k+2}}dt. \tag{13}$$

For each $k\ge 0$,

$$\begin{aligned}\int_x^\infty\frac{B_{k+1}(t)}{t^{k+2}}dt &= \int_x^\infty\frac{b_{k+1}(\{t\})}{t^{k+2}}dt,\\ &\le \int_x^\infty\frac{C_{k+1}}{t^{k+2}}dt \qquad\qquad \text{by (10)},\\ &= \left(\frac{C_{k+1}}{k+1}\right)\frac{1}{x^{k+1}},\end{aligned}$$

where C_{k+1} is a constant. This yields

$$\int_x^\infty\frac{B_{k+1}(t)}{t^{k+2}}dt=O(1/x^{k+1}). \tag{14}$$

Thus, from (13) and (14), we have

$$\begin{aligned}\sum_{0<n\le x}\frac{1}{n} &= \log x+\left(1+\sum_{r=0}^{k}\frac{B_{r+1}}{r+1}-\int_1^\infty\frac{B_{k+1}(t)}{t^{k+2}}dt\right)-\sum_{r=0}^{k}\left(\frac{B_{r+1}}{r+1}\right)\frac{1}{x^{r+1}}\\ &\qquad +\int_x^\infty\frac{B_{k+1}(t)}{t^{k+2}}dt.\end{aligned}$$

and, since

$$\gamma=\lim_{x\to\infty}\left(\sum_{n\le x}\frac{1}{n}-\log x\right),$$

we must have

$$\begin{aligned}\gamma &= 1+\sum_{r=0}^{k}\frac{B_{r+1}}{r+1}-\int_1^\infty\frac{B_{k+1}(t)}{t^{k+2}}dt.\\ &= 1-\int_1^\infty\frac{\{t\}}{t^2}dt.\end{aligned}$$

□

Chapter 2

The Arithmetic of Dynamical Systems

2.1 Dynamical Systems

A dynamical system is an abstract mathematical model describing the time dependence of a point's position in its space. Such a system is represented by a map whose iterates denote the passage of time. Firstly, I shall give the notion of a discrete dynamical system in general.

Definition 2.1. Let X be a non-empty set and a map $\alpha : X \to X$. The pair (X, α) is said to be a *dynamical system*.

For $t \in \mathbb{N}$, the t^{th} iterate of α is the t-fold composition $\alpha^t = \alpha \circ \alpha \circ \cdots \circ \alpha$. We define α^0 to be the identity map and we have $\alpha^{t+s} = \alpha^t \circ \alpha^s$ for all $t, s \in \mathbb{N}_0$. So

$$\mathcal{A} = \{\alpha^t : X \to X \mid t \in \mathbb{N}_0\}$$

with composition forms a monoid (a semigroup with an identity). If α is invertible

then we can replace $\mathbb{N}^0$ by $\mathbb{Z}$ in this definition, to get a group. We sometimes call (X, α) a *discrete-time dynamical system* because we can think of α in terms of an action of the discrete semigroup $\mathbb{N}_0$ on X; that is, a map $a : X \times \mathbb{N}_0 \to X$ given by $a(x,t) = \alpha^t(x)$ for all, $x \in X, t \in \mathbb{N}_0$, with the properties:

1. $a(x, 0) = x$,

2. $a(a(x,t), s) = a(x, t+s)$ for every $x \in X$ and $t, s \in \mathbb{N}_0$.

If we replaced $\mathbb{N}_0$ by $\mathbb{R}$ or the set of all non-negative real numbers, we would have a *continuous-time dynamical system.*

In practice, the structure of X could be that of a topological space, a measure space, a metric space or a smooth manifold, and α could be a measure-preserving map, a continuous map, an isometry or a differentiable map, respectively.

In the setting of this thesis, X means a compact metric space with a continuous map α, and from now on, all dynamical systems are of this form. Also we are motivated by some specific discrete-time dynamical systems, for example the circle doubling map, which will be explained later.

2.2 Periodic Points and Orbits

Let (X, α) be a dynamical system. For $x \in X$, the *orbit* of x is the set

$$\{x, \alpha(x), \alpha^2(x), \dots\}.$$

If there exists a positive integer k such that $\alpha^k(x) = x$ then this is a finite set

$$\tau := \{x, \alpha(x), \dots, \alpha^k(x) = x\},$$

and is called a *closed orbit* τ *of length* $k = |\tau|$.

Define

$$\begin{aligned}
\mathcal{L}_\alpha(n) &= \{x \in X \mid \#\{\alpha^k(x)\}_{k\in\mathbb{N}} = n\}, \\
\mathcal{F}_\alpha(n) &= \{x \in X \mid \alpha^n(x) = x\}, \text{ and} \\
\mathcal{O}_\alpha(n) &= \{\ \tau \mid \tau \text{ is a closed orbit of } \alpha \text{ of length } |\tau| = n\}.
\end{aligned}$$

which are the set of points of least period n under α, the set of points of period n under α, and the set of orbits of length n under α, respectively. We write

$$\begin{aligned}
L_\alpha(n) &= |\mathcal{L}_\alpha(n)|\,, \text{ the number of points of least period } n, \\
F_\alpha(n) &= |\mathcal{F}_\alpha(n)|\,, \text{ the number of points of period } n \text{ and} \\
O_\alpha(n) &= |\mathcal{O}_\alpha(n)|\,, \text{ the number of orbits of length } n.
\end{aligned}$$

It follows from the above definition that

$$O_\alpha(n) = L_\alpha(n)/n. \tag{15}$$

We notice that

$$\mathcal{F}_\alpha(n) = \bigsqcup_{d|n} \mathcal{L}_\alpha(d).$$

Consequently,

$$F_\alpha(n) = \sum_{d|n} L_\alpha(d), \tag{16}$$

since the $\mathcal{L}_\alpha(n)$ are disjoint for distinct n. By (15) and (16), we have

$$F_\alpha(n) = \sum_{d|n} dO_\alpha(d) \tag{17}$$

and so, by the Möbius inversion formula, we get

$$O_\alpha(n) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) F_\alpha(d). \tag{18}$$

Example 2.2. Let $X = \mathbb{T}$, where $\mathbb{T} = \mathbb{R}/\mathbb{Z}$. Define a continuous map $\alpha : X \to X$ by sending x into $2x \pmod 1$ on $\mathbb{T}$, the *circle doubling map*. Then

$$F_\alpha(1) = 1,\ F_\alpha(2) = 3,\ F_\alpha(3) = 7, \ldots$$

To get the general formula for $F_\alpha(n)$, we consider $2^n x = x \pmod 1$. Thus

$$(2^n - 1)x = 0 \pmod 1.$$

Define a map sending

$$x \mapsto (2^n - 1)x \pmod 1.$$

The kernel of this map is

$$\{0, \tfrac{1}{2^n-1}, \tfrac{2}{2^n-1}, \cdots, \tfrac{2^n-2}{2^n-1}\}$$

which is equal to $\mathcal{F}_\alpha(n)$. Hence $F_\alpha(n) = 2^n - 1$, so F_α is the *Mersenne sequence*.

Remark 2.3. Since

$$\mathbb{T} = \{x + \mathbb{Z} \ :\ x \in [0, 1)\},$$

we can think of $\mathbb{T}$ as $[0, 1)$ with addition $\pmod 1$. Thus the map α is given by

$$\alpha(x) = \begin{cases} 2x & 0 \le x < 1/2, \\ 2x - 1 & 1/2 \le x < 1. \end{cases}$$

Example 2.4. From Example 2.2, we know that $F_\alpha(n) = 2^n - 1$. We apply the formula in (18) so that we derive the number of orbits of length n below.

$$O_\alpha(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) (2^d - 1).$$

Then

$$\begin{aligned}
O_\alpha(1) &= 1, \\
O_\alpha(2) &= \frac{1}{2}\left(\mu(2) + \mu(1)(3)\right) = 1, \\
O_\alpha(3) &= \frac{1}{3}\left(\mu(3) + \mu(1)(7)\right) = 2, \\
O_\alpha(4) &= \frac{1}{4}\left(\mu(4) + \mu(2)(3) + \mu(1)(15)\right) = 3, \\
O_\alpha(5) &= \frac{1}{5}\left(\mu(5) + \mu(1)(31)\right) = 6, \\
O_\alpha(6) &= \frac{1}{6}\left(\mu(6) + \mu(2)(3) + \mu(3)(7) + \mu(1)(63)\right) = 9.
\end{aligned}$$

In general,

$$\begin{aligned}
O_\alpha(n) &= \frac{F_\alpha(n)}{n} + \frac{1}{n}\sum_{d|n, d<n} \mu\left(\frac{n}{d}\right)(2^d - 1) \\
&= \frac{F_\alpha(n)}{n} + O(2^{n/2}),
\end{aligned}$$

since

$$\left| O_\alpha(n) - \frac{F_\alpha(n)}{n} \right| \leq \frac{1}{2} 2^{n/2}.$$

2.3 Topological Entropy

The *topological entropy* of a dynamical system (X, α), denoted by $h(\alpha)$, is a nonnegative real number that measures the complexity of the orbits in the system. There are several different ways to define topological entropy. The original definition was introduced in 1965 by Adler, Konheim and McAndrew, and this definition was modelled after the definition of a measure-theoretic entropy given by Kolmogorov and Sinai. Indeed, there is an analogy between the definition of the measure-theoretic entropy and the topological entropy. A beautiful general relation between measure-theoretic

and topological entropy was established through the work of Goodwyn [11]. Later, Dinaburg [7] and Bowen [4] gave a definition which clarified the meaning of topological entropy: for a system given by an iterated function, the topological entropy represents the exponential growth rate of the number of distinguishable orbits of the iterates. Here, we will introduce the definition of topological entropy by following Dinaburg and Bowen for a continuous function $\alpha : X \to X$, where (X, d) is a compact metric space.

Let (X, d) be a compact metric space and $\alpha : X \to X$ be a continuous map. For each $n \in \mathbb{N}$, define

$$d_n(x, y) = \max\{d(\alpha^i(x), \alpha^i(y)) \ : \ 0 \leq i < n\},$$

for any $x, y \in X$. Then d_n is a metric on X, called a *Bowen-Dinaburg metric.*

Lemma 2.5. *If (X, d) is a compact metric space, then so is (X, d_n) for any positive integer n.*

Proof. Fix $n \in \mathbb{N}$. Assume that (X, d) is a compact metric space. To show that (X, d_n) is a compact metric space, we will prove the following statement: U is an open set in X with respect to the metric d if and only if U is an open set in X with respect to the metric d_n. Let U be an open set in X with respect to d. Then every point in U has a neighbourhood contained in U. Equivalently, for each point u in U, there exists a real number $\gamma > 0$ such that, $B^d_\gamma(u) \subseteq U$. If $d_n(x, u) < \gamma$, then clearly $d(x, u) < \gamma$. Thus $B^{d_n}_\gamma(u) \subset B^d_\gamma(u)$. It follows that given any point u in U, there exists a real number $\gamma > 0$ such that, $B^{d_n}_\gamma(u) \subseteq U$. Hence U is an open set in X with respect to d_n. Conversely, let U be an open set in X with respect the metric d_n. Then given any point u in U, there exists a real number $\gamma > 0$ such that, $B^{d_n}_\gamma(u) \subseteq U$. We can pick $0 < \delta < \gamma$ so that, if $d(x, u) < \delta$, then $d(\alpha^i(x), \alpha^i(u)) < \gamma$ for all $0 \leq i < n$,

as α is continuous. This implies that $B_\delta^d(u) \subseteq B_\gamma^{d_n}(u)$. Hence U is open in X with respect to d. $\square$

Fix $\epsilon > 0$ and $n \geq 1$.

Definition 2.6. We say that $x, y \in X$ are (n, ϵ)-*separated* if $d_n(x, y) \geq \epsilon$. A subset E of X is said to be (n, ϵ)-*separated* if any two different points of E are (n, ϵ)-separated.

Definition 2.7. A subset F of X is said to be (n, ϵ)-*spanning* if, for any $x \in X$, there is some $y \in F$ with $d_n(x, y) < \epsilon$.

Equivalently,

$$X = \bigcup_{y \in F} \bigcap_{i=0}^{n-1} \alpha^{-i} B_\epsilon(\alpha^i y).$$

Then the open cover of X by the set

$$\bigcap_{i=0}^{n-1} \alpha^{-i} B_\epsilon(\alpha^i y)$$

for all $y \in X$ has a finite subcover by compactness. It follows that there is a finite (n, ϵ)-spanning set.

Let $\mathcal{R}(n, \epsilon)$ be the smallest cardinality of any (n, ϵ)-spanning set under α, and let $\mathcal{N}(n, \epsilon)$ be the maximal cardinality of any (n, ϵ)-separated set under α. Note that $\mathcal{R}(n, \epsilon)$ is finite for any $\epsilon > 0$.

Remark 2.8. For $\epsilon > \epsilon^{'}$, we have that $\mathcal{N}(n, \epsilon^{'}) \geq \mathcal{N}(n, \epsilon)$ and $\mathcal{R}(n, \epsilon^{'}) \geq \mathcal{R}(n, \epsilon)$. In particular,

$$\limsup_{n \to \infty} \frac{1}{n} \log \mathcal{N}(n, \epsilon^{'}) \geq \limsup_{n \to \infty} \frac{1}{n} \log \mathcal{N}(n, \epsilon),$$

and

$$\limsup_{n \to \infty} \frac{1}{n} \log \mathcal{R}(n, \epsilon^{'}) \geq \limsup_{n \to \infty} \frac{1}{n} \log \mathcal{R}(n, \epsilon).$$

Lemma 2.9. $\mathcal{R}(n,\epsilon) \leq \mathcal{N}(n,\epsilon) \leq \mathcal{R}(n,\frac{\epsilon}{2})$.

Proof. If E is an (n,ϵ)-separated set of maximal cardinality then E is an (n,ϵ)-spanning set because if not, we could add another point to E and still be (n,ϵ)-separated. Thus the first inequality holds. For the second inequality, let E be (n,ϵ)-separated, and let F be an $(n,\frac{\epsilon}{2})$-spanning set. Define a map $f : E \to F$ by choosing $f(x) \in F$ so that

$$d_n(x, f(x)) \leq \frac{\epsilon}{2}.$$

Since E is (n,ϵ)-separated, f is injective. Hence $|E| \leq |F|$. □

Following Lemma 2.9, we know that $\mathcal{N}(n,\epsilon)$ is finite.

Definition 2.10. The *topological entropy* of the map α is defined by

$$h(\alpha) = \lim_{\epsilon \to 0} \limsup_{n \to \infty} \frac{1}{n} \log \mathcal{N}(n,\epsilon),$$

which is the average exponential growth of the number of distinguishable orbit segments.

Notice that the limit in ϵ exists (and might be ∞) since $\mathcal{N}(n,\epsilon') \geq \mathcal{N}(n,\epsilon)$ if $\epsilon' < \epsilon$.

Example 2.11. Let $X = \mathbb{T}$ and α be the circle doubling map as in Example 2.2. Then $h(\alpha) = \log 2$.

Proof. Let d be the Euclidean metric on $\mathbb{T}$. We notice that if $d(x,y) < \frac{1}{4}$, then

$$d(\alpha(x), \alpha(y)) = 2d(x,y).$$

Given $n \geq 1$, let $x, y \in \mathbb{T}$ be such that $d(x,y) < 2^{-(n+1)}$. Then $d(\alpha^i(x), \alpha^i(y)) < \frac{1}{4}$, for any $i = 1, 2, \ldots, n-1$ and also

$$d(\alpha^i(x), \alpha^i(y)) = 2^i d(x,y).$$

These imply that

$$d_n(x,y) = d(\alpha^{n-1}(x), \alpha^{n-1}(y)) = 2^{n-1}d(x,y).$$

If $d_n(x,y) \geq \epsilon$, for some $\epsilon > 0$, then $d(x,y) \geq \epsilon 2^{-(n-1)}$.

Given $k \geq 1$, choose $\epsilon_k = 2^{-(k+1)}$. Then any (n, ϵ_k)-separated set has cardinality at most 2^{n+k}. The reason is that if there is an (n, ϵ_k)-separated set E, which has cardinality more than 2^{n+k}, then by the pigeonhole principle, it follows that there is an x in E with $d(x,y) < \frac{1}{2^{n+k}}$ for some $y \in E$. Then $d_n(x,y) < \epsilon_k$, which is absurd. Consequently, the set

$$\left\{0, \frac{1}{2^{n+k}}, \frac{2}{2^{n+k}}, \ldots, \frac{2^{n+k}-1}{2^{n+k}}\right\}$$

is a maximal (n, ϵ_k)-separated set. Thus $\mathcal{N}(n, \epsilon_k) = 2^{n+k}$. Hence

$$h(\alpha) = \lim_{k\to\infty} \lim_{n\to\infty} \frac{n+k}{n} \log 2 = \log 2.$$

□

For each natural number $N \geq 2$, let

$$\begin{aligned} \Omega_N &= \{x = (\ldots, x_{-1}, x_0, x_1, \ldots) \mid x_i \in \{0, 1, 2, \ldots, N-1\} \text{ for } i \in \mathbb{Z}\} \\ &= \{0, 1, 2, \ldots, N-1\}^{\mathbb{Z}}, \end{aligned}$$

the space of two-sided sequences of N symbols. Fix integers $n_1 < n_2 < \cdots < n_k$ and $a_i \in \{0, 1, 2, \ldots, N-1\},\ i = 1, 2, \ldots, k$. The subset

$$C^{n_1,n_2,\ldots,n_k}_{a_1,a_2,\ldots,a_k} = \{x \in \Omega_N \mid x_{n_i} = a_i \text{ for } i = 1, 2, \ldots, k\}$$

is called a *cylinder*, and the fixed number k is the rank of the cylinder. Then all cylinders are open sets in the product topology for the discrete topology on the finite

set $\{0, 1, 2, \ldots, N-1\}$. We can define a topology on the space Ω_N by constructing a base from such cylinders. Also, we define a metric on Ω_N by

$$d(x, y) = \sum_{n=-\infty}^{\infty} \frac{|x_n - y_n|}{(10N)^{|n|}} < \infty$$

and obtain the same topology.

For

$$a = (\ldots, a_{-m}, \ldots, a_0, \ldots, a_m, \ldots),$$

the *symmetric cylinder* of rank $2m+1$ is the cylinder

$$C_a^m := C_{a_{-m},\ldots,a_m}^{-m,\ldots,m} = \{x \in \Omega_N \mid x_i = a_i \text{ for } |i| \leq m\},$$

which is an open metric ball of radius $(10N)^{-m}$ around a.

Example 2.12. For $X = \Omega_N$, let α be the shift action on X given by

$$(\alpha(x_n)) = x_{n+1} \text{ for all } n \in \mathbb{Z}.$$

Then $h(\alpha) = \log N$.

Proof. Given $m \geq 1$, let $\epsilon_m = (10N)^{-m}/2$. Now fix $n \geq 1$. For $x = (x_i),\ y = (y_i) \in \Omega_N$, we have

$$d_n(x, y) = \max_{0 \leq j \leq n-1} \left(\sum_{i=-\infty}^{\infty} \frac{|x_{i+j} - y_{i+j}|}{(10N)^{|i|}} \right).$$

If $d_n(x, y) \leq \epsilon_m$, then $x_{i+j} = y_{i+j}$ for all $|i| \leq m$ and $0 \leq j \leq n-1$.

We fix

$$a = (\ldots, a_{-m}, \ldots, a_m, \ldots, a_{m+n-1}, \ldots)$$

in order to define the cylinder

$$C_{a_{-m},\ldots,a_m,\ldots,a_{m+n-1}}^{-m,\ldots,m,\ldots,m+n-1} = \{x \in \Omega_N \mid x_i = a_i \text{ for } -m \leq i \leq m+n-1\},$$

the ball of radius ϵ_m around a with respect to the metric d_n associated with the map α. We claim that any two balls of this radius with respect to the metric d_n are either identical or disjoint. Suppose $a \neq a^{'}$ such that $a = (\dots, a_{-m}, \dots, a_m, \dots, a_{m+n-1}, \dots)$ and $a^{'} = (\dots, a^{'}_{-m}, \dots, a^{'}_{m}, \dots, a^{'}_{m+n-1}, \dots)$ for which

$$C^{-m,\dots,m,\dots,m+n-1}_{a_{-m},\dots,a_m,\dots,a_{m+n-1}} \cap C^{-m,\dots,m,\dots,m+n-1}_{a^{'}_{-m},\dots,a^{'}_m,\dots,a^{'}_{m+n-1}} \neq \emptyset.$$

Then there exists $x^{'}$ such that $d_n(x^{'}, a) < \epsilon_m$ and $d_n(x^{'}, a^{'}) < \epsilon_m$.
Consequently,

$$\begin{aligned} \max_{0\leq j\leq n-1}\left(\sum_{i=-\infty}^{\infty}\frac{|a_{i+j}-a^{'}_{i+j}|}{(10N)^{|i|}}\right) &= d_n(a,a^{'}) \\ &< d_n(a,x^{'})+d_n(x^{'},a^{'}) < (10N)^{-m}. \end{aligned}$$

Thus for each $j = 0, 1, \dots, n-1$, $a_{i+j} = a^{'}_{i+j}$ for $|i| \leq m$. This implies that

$$C^{-m,\dots,m,\dots,m+n-1}_{a} = C^{-m,\dots,m,\dots,m+n-1}_{a^{'}}.$$

If $d_n(x, y) \geq \epsilon_m$, then x and y must not be in the same ball of radius ϵ_m around some a (i.e. if x, y are in the same (n, ϵ_m)-separated set, both of them must stay in different balls of radius ϵ_m around some a). Thus counting the points of a maximal (n, ϵ_m)-separated set is the same as counting the number of balls of radius ϵ_m around points a. Since the covering of Ω_N by such balls is obviously minimal, so a maximal cardinality of (n, ϵ_m)-separated set is equal to the number of choice of $a_{-m}, \dots, a_m, \dots, a_{m+n-1}$. Thus $\mathcal{N}(n, \epsilon_m) = N^{2m+n}$. Hence we obtain

$$h(\alpha) = \lim_{m\to\infty}\lim_{n\to\infty}\frac{2m+n}{n}\log N = \log N.$$

□

Chapter 3

S-integer Dynamical Systems

3.1 Toral Endomorphisms

We will first introduce a definition of a toral endomorphism, which generalizes the circle-doubling map. For $d \geq 1$, let $M_d(\mathbb{Z})$ be the set of all $d \times d$ matrices A having integer entries and $GL_d(\mathbb{Z})$ be the set of all elements A in $M_d(\mathbb{Z})$ such that $\det(A) = \pm 1$.

Definition 3.1. Each matrix A in $M_d(\mathbb{Z})$ such that $\det(A) \neq 0$ defines a linear map on $\mathbb{R}^d$ by $\bar{x} \mapsto A\bar{x}$ for all $\bar{x} \in \mathbb{R}^d$. We define a *toral endomorphism* $\alpha : \mathbb{T}^d \to \mathbb{T}^d$ by

$$\alpha(\bar{x}) = A\bar{x} \pmod 1$$

for all $\bar{x} \in \mathbb{T}^d$ where $\mathbb{T}^d = \mathbb{R}^d/\mathbb{Z}^d$ is the additive d-dimensional torus.

In general, the map α is not invertible. However, if $\det(A) = \pm 1$ then A^{-1} exists and is an integer matrix, hence we have a map α^{-1} given by

$$\alpha^{-1}(\bar{x}) = A^{-1}\bar{x} \pmod 1$$

for all $\bar{x} \in \mathbb{T}^d$. It is easy to see that α^{-1} is the inverse of α.

Definition 3.2. Let $A \in GL_d(\mathbb{Z})$. We say that the map α (in Definition 3.1) is a *toral automorphism.*

Example 3.3. The circle-doubling map is a toral endomorphism because the corresponding matrix to this map is the 1×1 matrix having entry 2 and its determinant obviously is not equal to 0. But it's not a toral automorphism as the determinant is not ± 1.

Example 3.4. Let

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

The associated map $\alpha : \mathbb{T}^2 \to \mathbb{T}^2$ takes the form

$$\alpha(x_1, x_2) = (2x_1 + x_2, x_1 + x_2) \pmod 1.$$

As $\det(A)=1$, so α is a toral automorphism and it is known as *Arnold's cat map.*

Let α_A be the toral endomorphism corresponding to a matrix A and A_α be the matrix corresponding to a toral endomorphism α. Sometimes if we write just α, in this section we mean that α is a toral endomorphism (or a toral automorphism) corresponding to some matrix A. Similarly, A means A_α.

Lemma 3.5. *A toral automorphism $\alpha_A : \mathbb{T}^d \to \mathbb{T}^d$ is ergodic iff no eigenvalue λ_i of A is a root of unity.*

The proof of this lemma can be found in [34, page 29-32].

Definition 3.6. Suppose that $A \in GL_d(\mathbb{Z})$. We say that α_A is a *hyperbolic toral automorphism* if A does not have eigenvalues of modulus 1. Otherwise, α_A is called a *non-hyperbolic toral automorphism* and in particular, α_A is *quasihyperbolic* if it is ergodic and A has some eigenvalues of modulus 1.

Example 3.7. Let α be the same map in Example 3.4. The eigenvalues are $\frac{3\pm\sqrt{5}}{2}$. Thus α is hyperbolic, since A has no eigenvalues of modulus 1.

Example 3.8. Let $\alpha : \mathbb{T}^4 \to \mathbb{T}^4$ be the toral automorphism corresponding to the matrix

$$A = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 8 \\ 0 & 1 & 0 & -6 \\ 0 & 0 & 1 & 8 \end{pmatrix}.$$

Then A has eigenvalues $2+\sqrt{3}\pm\sqrt{6+4\sqrt{3}}$ and $2-\sqrt{3}\pm i\sqrt{4\sqrt{3}-6}$ which are two real eigenvalues and two complex eigenvalues of modulus 1. So α is not hyperbolic, but is ergodic.

Theorem 3.9. *Let α be a hyperbolic or quasihyperbolic toral automorphism of $\mathbb{T}^d$ corresponding to a matrix A having eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_d$. Then the number of points fixed by α^n is given by*

$$F_\alpha(n) = |\det(A^n - I)| = \prod_{i=1}^{d} |\lambda_i^n - 1|.$$

Proof. The sketch of this proof may be found in some part of the proof in Theorem 8.18 [34]. □

Let us consider the special case of a toral automorphism of the 2-dimensional torus $\mathbb{T}^2$.

Proposition 3.10. *Let α be a toral automorphism of $\mathbb{T}^2$ with corresponding matrix A having eigenvalues λ_1, λ_2. Then the number of points fixed by α^n is given by*

$$F_\alpha(n) = |\det(A^n - I)| = \left|\lambda_1^n + \lambda_2^n - 2\right|.$$

Proof. Suppose that $\det(A) = 1$. In fact, $(x_1, x_2) \in \mathbb{T}^2$ is a periodic point with period n for α if and only if

$$(A^n - I)(x_1, x_2)^t = (n_1, n_2)^t \tag{19}$$

for some integers n_1, n_2. We may write

$$A^n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}.$$

and define the map $\beta : \mathbb{R}^2 \to \mathbb{R}^2$ by

$$\beta : (x_1, x_2)^t \mapsto (A^n - I)(x_1, x_2)^t$$

(i.e. $\beta : (x_1, x_2)^t \mapsto ((a_n - 1)x_1 + b_n x_2, c_n x_1 + (d_n - 1)x_2))^t$. This maps $\mathbb{T}^2$ onto the parallelogram

$$\mathcal{R} = \{\gamma u + \delta v \ : \ 0 \leq \gamma, \delta < 1\},$$

where $u = \beta(0, 1)^t$ and $v = \beta(1, 0)^t$. It follows by (19) that a point $(x_1, x_2) \in \mathbb{T}^t$ is periodic iff $(A^n - I)(x_1, x_2)^t$ is an integer point in $\mathcal{R}$. Thus the number of periodic points of period n correspond to the number of integer points in $\mathcal{R}$. Therefore, the number of such points is equal to the area of $\mathcal{R}$. Hence

$$F_\alpha(n) = |\det(A^n - I)|.$$

It remains to calculate the eigenvalue of $A^n - I$. Let μ be an eigenvalue of $A^n - I$ with an eigenvector v. Then

$$(A^n - I)v = \mu v \iff A^n v = (\mu + 1)v$$

so that $\mu + 1$ is an eigenvalue of A^n. The eigenvalues of A^n are given by λ_1^n, λ_2^n since λ_1, λ_2 are eigenvalues of A. Recall that a determinant of a matrix is given by the

product of the eigenvalues.

Consequently,

$$\begin{aligned} |\det(A^n - I)| &= |(\lambda_1^n - 1)(\lambda_2^n - 1)| \\ &= |(\lambda_1\lambda_2)^n + 1 - (\lambda_1^n + \lambda_2^n)| \\ &= |\lambda_1^n + \lambda_2^n - 2|. \end{aligned}$$

as $\lambda_1\lambda_2 = \det(A) = 1$. □

Theorem 3.11. *Let α be a hyperbolic or quasihyperbolic toral automorphism of $\mathbb{T}^d$ corresponding to a matrix A having eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_d$. Then*

$$h(\alpha) = \sum_{|\lambda_i|>1} \log|\lambda_i|.$$

Proof. See [34, Theorem 8.18]. □

3.2 Non-Archimedean Valuations

To understand how to construct S-integer dynamical systems in the later sections, we shall first introduce the notion of a valuation on a field.

Definition 3.12. Let K be a field. A valuation on K is a function $|\cdot| : K \to \mathbb{R}$ satisfying the following properties:

(1) $|x| \geq 0$ for all $x \in K$, with equality if and only if $x = 0$ (positive-definite);

(2) $|xy| = |x| \cdot |y|$ for all $x, y \in K$ (multiplicative);

(3) $|x + y| \leq |x| + |y|$ for all $x, y \in K$ (triangle inequality).

A valuation on K is called *non-archimedean* if also,

(4) $|x + y| \leq \max\{|x|, |y|\}$ for all $x, y \in K$, (ultrametric inequality).

Otherwise, we say that it is an *archimedean* valuation.

Remark 3.13. i) Condition (4) implies condition (3).

ii) Any valuation defines a metric by $d(x, y) = |x - y|$ and a metric is called non-archimedean if

$$d(x, y) \leq \max\{d(x, z), d(z, y)\}.$$

We observe that, for a non-archimedean valuation

$$d(x, y) = |x - y| = |(x - z) + (z - y)| \leq \max\{|x - z|, |z - y|\} = \max\{d(x, z), d(z, y)\}$$

Indeed, the metric d is non-archimedean if and only if the valuation $|\cdot|$ is non-archimedean.

Lemma 3.14. *Let $|\cdot|$ be a non-archimedean valuation on a field K. If $x, y \in K$ such that $|x| \neq |y|$, then*

$$|x + y| = \max\{|x|, |y|\}.$$

Proof. Without loss of generality, we assume that $|y| < |x|$. Then we definitely have

$$|x + y| \leq |x| = \max\{|x|, |y|\}.$$

To prove the other side, we write $x = (x + y) - y$ and we know $|y| = |-y|$. Thus we obtain

$$|x| \leq \max\{|x + y|, |y|\}.$$

This implies that

$$\max\{|x|, |y|\} = |x| \leq |x + y|,$$

since $|y| < |x|$. □

The following corollary will be shown that for a non-archimedean valuation on a field , every triangle is isosceles. This result immediately comes from Lemma 3.14.

Corollary 3.15 (The Isosceles Triangle Principle)**.** *Let $|\cdot|$ be a non-archimedean valuation on a field K and let d be the metric defined as in Remark 3.13(ii). If $x, y, z \in K$ such that $d(x,y) \neq d(z,x)$, then*

$$d(x,y) = \max\{d(x,z), d(z,y)\}.$$

Example 3.16. (1) The most familiar example of a valuation is the usual absolute value on $\mathbb{Q}$. It is an archimedean valuation and is often called the valuation at infinity and denoted $|\cdot|_\infty$.

(2) The *trivial valuation* on any field K, given by $|x| = 1$, for all $x \neq 0$, and $|0| = 0$. It is non-archimedean, but we have to exclude it from most of the theory that we devolop. It is called the *discrete valuation*.

Example 3.17. Now we come to the crucial example. Let $K = \mathbb{Q}$, let p be a prime and for $a \in \mathbb{Z} \setminus \{0\}$, let $\operatorname{ord}_p a$ be the highest power of p which divides a. For example,

$$\operatorname{ord}_3 25 = 0, \;\; \operatorname{ord}_2 50 = 1, \;\; \operatorname{ord}_2 10 = 1, \;\; \operatorname{ord}_7 98 = 2.$$

For any non-zero rational number $x = \frac{a}{b}$, define $\operatorname{ord}_p x = \operatorname{ord}_p a - \operatorname{ord}_p b$. This gives a notion of *signed multiplicity*: we say that 2 divides 8 with multiplicity 3 and divides $\frac{3}{4}$ with multiplicity -2. It is very easy to check that $\operatorname{ord}_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ by sending $a \mapsto \operatorname{ord}_p a$ is well-defined. We also introduce the convention that $\operatorname{ord}_p 0 = \infty$.

Proposition 3.18. *If $x, y \in \mathbb{Q}$, then ord_p has the following properties:*

(1) $\operatorname{ord}_p(xy) = \operatorname{ord}_p(x) + \operatorname{ord}_p(y)$ *;*

(2) $\operatorname{ord}_p(x+y) \geq \min\{\operatorname{ord}_p(x), \operatorname{ord}_p(y)\}$.

Proof. It is easy to check that (1) holds; we will therefore only prove (2). If one of $x, y, x+y$ is 0, the inequality is clear. So let x, y be non-zero rational numbers. Write

$x = p^r \frac{a}{b}$ and $y = p^s \frac{c}{d}$, where $a, b, c, d, r, s \in \mathbb{Z}$ with $p \nmid abcd$. Now if $r = s$, we get

$$x + y = p^r \frac{ad + bc}{bd},$$

since $p \nmid bd$, $\mathrm{ord}_p(x + y) \geq r$. Suppose that $r \neq s$. Without loss of generality, assume $s > r$. Then

$$\begin{aligned} x + y &= p^r \left(\frac{a}{b} + \frac{p^{s-r} c}{d} \right) \\ &= p^r \frac{ad + p^{s-r} bc}{bd}. \end{aligned}$$

Then $\mathrm{ord}_p(x + y) = r = \min \{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}$ as $p \nmid ad + p^{s-r} bc$. □

Define $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ by

$$|x|_p = \begin{cases} p^{-\mathrm{ord}_p x} & \text{if } x \neq 0, \\ 0 & \text{if } x = 0. \end{cases}$$

It is known as the p-adic valuation.

Proposition 3.19. *$|\,.\,|_p$ is a non-archimedean valuation on $\mathbb{Q}$.*

Proof. We can check the properties (1) and (2) directly. It remains to show just only the property (4) as we know that the property (4) implies the property (3). If $x = 0$ or $y = 0$ or $x + y = 0$, then it easy to see that the property (4) is true. Assume therefore that x, y and $x + y$ are all nonzero. By Proposition 3.18, we have

$$\begin{aligned} |x + y|_p &= p^{-\mathrm{ord}_p(x+y)} \\ &\leq p^{-\min\{\mathrm{ord}_p(x), \mathrm{ord}_p(y)\}} \\ &= \max\{p^{-\mathrm{ord}_p(x)}, p^{-\mathrm{ord}_p(y)}\} \\ &= \max\{|x|_p, |y|_p\}. \end{aligned}$$

Hence $|\cdot|_p$ is a non-archimedean valuation on $\mathbb{Q}$. □

Example 3.20. For a prime number p, let $\mathbb{F}_p(t)$ be the field of rational functions over a finite field of characteristic p, that is

$$\mathbb{F}_p(t) = \left\{ \frac{f(t)}{g(t)} : f, g \in \mathbb{F}_p[t] \text{ such that } g(t) \neq 0 \right\},$$

where

$$\mathbb{F}_p[t] = \left\{ \sum_{i=0}^{n} a_i t^i \mid a_i \in \mathbb{F}_p, n \in \mathbb{N}_0 \right\}. \tag{20}$$

For each monic irreducible $v(t) \in \mathbb{F}_p(t)$, we define $|\cdot|_v : \mathbb{F}_p(t) \to \mathbb{R}$ by

$$|f|_v = p^{-\operatorname{ord}_v(f).\deg(v)}$$

for all $f \in \mathbb{F}_p(t)$ and $\operatorname{ord}_v(f)$ is the signed multiplicity with which v divides the rational function f. The field $\mathbb{F}_p(t)$ also has a distinguished valuation called the valuation at infinity defined by

$$\left|\frac{f(t)}{g(t)}\right|_\infty = \left|\frac{f(t)}{g(t)}\right|_{t^{-1}}.$$

This is analogous to the infinite valuation on $\mathbb{Q}$. Also, there is an analogy between valuations $|\,.\,|_v$ on $\mathbb{F}_p(t)$ and valuations $|\cdot|_p$ on $\mathbb{Q}$, so that we may prove that $|\cdot|_v$ is a non-archimedean valuation similarly to the proof in Proposition 3.19.

Lemma 3.21 (Artin-Whaples Product Formula)**.** *For any x in $\mathbb{Q}^\times$, (or in $\mathbb{F}_p(t)$) we have*

$$\prod_{p \leq \infty} |x|_p = 1$$

where $p \leq \infty$ means that we take the product over all of the primes of $\mathbb{Q}$ (or irreducible polynomials in $\mathbb{F}_p[t]$) and then multiply by the valuation at infinity.

Proof. We only need to prove the formula when x is a positive rational number as $\forall p \in \mathbb{P} \cup \{\infty\}, |-1|_p = 1$. So let $x \in \mathbb{Q}^\times$, then it can be written as

$$x = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

where $a_i \in \mathbb{Z},\ p_i \in \mathbb{P},\ i = 1, 2, \ldots, k$ and $p_i \neq p_j$ if $i \neq j$.

Then we have

$$\begin{cases} |x|_q = 1 & \text{if } q \neq p_i \text{ for all } i = 1, 2, \ldots, k \\ |x|_{p_i} = p_i^{-a_i} & \text{for } i = 1, 2, \ldots, k \\ |x|_\infty = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}. & \end{cases}$$

The formula follows at once, and the case $\mathbb{F}_p(t)$ is the same. □

The following lemma, which allows us to compute the p-adic valuation $|a^n - 1|_p$ for any odd prime number and $\gcd(a, p) = 1$, will play a crucial role in Chapters 4 and 5.

For a prime p, let $m_p(a)$ be the multiplicative order of $a \pmod p$.

Lemma 3.22. *Let p be an odd prime and a be an integer such that $\gcd(a, p) = 1$. Then*

$$|a^n - 1|_p = \begin{cases} |n|_p |a^{m_p(a)} - 1|_p & \text{if } m_p(a) \mid n, \\ 1 & \text{if } m_p(a) \nmid n. \end{cases}$$

In other words,

$$\mathrm{ord}_p(a^n - 1) = \begin{cases} \mathrm{ord}_p(n) + \mathrm{ord}_p(a^{m_p(a)} - 1) & \text{if } m_p(a) \mid n, \\ 0 & \text{if } m_p(a) \nmid n. \end{cases}$$

Proof. We consider $\bar{a} \in \mathbb{Z}_p^\times$, a group of $p - 1$ elements with multiplication modulo p. Let $m_p(a)$ be the order of $\bar{a}$ in $\mathbb{Z}_p^\times$. Thus

$$\bar{a}^{m_p(a)} \equiv 1 \mod p.$$

So

$$|a^{m_p(a)} - 1|_p \leq \frac{1}{p} < 1.$$

Moreover,

$$\bar{a}^n \equiv 1 \mod p \Leftrightarrow m_p(a) \mid n \Leftrightarrow |a^n - 1|_p < 1,$$

and

$$|a^n - 1|_p = 1 \Leftrightarrow m_p(a) \nmid n.$$

If $m_p(a)|n$, then write $n = m_p(a)p^e r$ where $e \geq 0$ and $\gcd(p, r) = 1$.

Then, putting $a^{m_p(a)} = 1 + px$, we have

$$\begin{aligned} |a^n - 1|_p &= |(a^{m_p(a)})^{p^e r} - 1|_p \\ &= \left| (p^e r)px + \binom{p^e r}{p^e r - 2}(px)^2 + \cdots + \binom{p^e r}{1}(px)^{p^e r - 1} + (px)^{p^e r} \right|_p . \end{aligned}$$

Since $|\cdot|_p$ is a non-archimedean valuation and for each $i = 0, 1, \ldots, p^e r - 2$, we have

$$|p^e rpx|_p \geq \left| \binom{p^e r}{i}(px)^{p^e r - i} \right|_p ,$$

It follows that

$$\begin{aligned} |a^n - 1|_p &= |p^e rpx|_p \\ &= |p^e r|_p |px|_p = |n|_p |a^{m_p(a)} - 1|_p. \end{aligned}$$

□

We notice that $\mathrm{ord}_p(m_p(a)) = 0$ because $m_p(a) \mid p - 1$.

3.3 Completion and Places of $\mathbb{A}$-fields

Definition 3.23. Let K be a finite algebraic extension of the rational field $\mathbb{Q}$ or of $\mathbb{F}_p(t)$ for some rational prime p. In the sense of Weil [37], any such field K is called an $\mathbb{A}$-*field*. From here on, we use K to denote an $\mathbb{A}$-field.

A valuation $|\cdot|$ on K defines a metric as in Remark 3.13(ii), giving a notion of open and closed sets and Cauchy sequences in K.

Definition 3.24. A sequence (x_n) of elements of K is called a *Cauchy sequence* if, for every $\epsilon > 0$, there exists M such that we have $|x_n - x_m| < \epsilon$ for all $n, m > M$.

We recall that a sequence (x_n) *converges to* $x \in K$ if, for all $\epsilon > 0$, there exists N such that, for all $n > N$, $|x_n - x| < \epsilon$.

Lemma 3.25. *Every Cauchy sequence of real numbers is bounded.*

Proof. Let (x_n) be a Cauchy sequence. Then there exists a natural number N such that for all $n, m \geq N$, we have $|x_n - x_m| < 1$. Taking $m = N$, we obtain that $|x_n| \leq |x_N| + 1$ for all $n \geq N$. Let

$$M = \max\{|x_1|, |x_2|, \ldots, |x_{N-1}|, |x_N| + 1\}.$$

It follows that $|x_n| \leq M$ for all n. Hence (x_n) is bounded. □

Lemma 3.26. *Every convergent sequence is Cauchy.*

The converse is not true in general, but it holds if $K = \mathbb{R}$ with respect to $|\cdot|_\infty$.

Definition 3.27. We say that K is *complete with respect to* $|\cdot|$ if every Cauchy sequence is convergent with respect to $|\cdot|$.

For example, $\mathbb{R}$ with $|\cdot|_\infty$ is complete, but $\mathbb{Q}$ is not complete with respect to any of its nontrivial valuations. The main point here will be to construct, for each prime p or ∞, a complete field containing $\mathbb{Q}$ to which the valuation $|\cdot|_p$ extends. We first need to recall some concepts from basic topology for any metric space.

Definition 3.28. Let K be a field with valuation $|\cdot|$, let $a \in K$ and r be a positive real number. The *open ball of radius r and centre a* is the set

$$B(a,r) = \{x \in K : |x-a| < r\}.$$

The *closed ball of radius r and centre a* is the set

$$\bar{B}(a,r) = \{x \in K : |x-a| \leq r\}.$$

Definition 3.29. A subset S of K is called dense in K if every open ball around an element of K contains an element of S; that is, if for every $x \in K$ and every $\epsilon > 0$, we have $B(x,\epsilon) \cap S \neq \emptyset$. Equivalently, S is dense in K if, for all $x \in K$, there exists a sequence (x_n) in S such that $\lim_{n\to\infty} x_n = x$.

For example, $\mathbb{Q}$ is dense in $\mathbb{R}$ with $|\cdot|_\infty$ as, given any irrational number x, there exists a sequence (x_n) in $\mathbb{Q}$ converging to x.

Definition 3.30. A field $\bar{K}$ with valuation $||\cdot||$ is the *completion* of K with valuation $|\cdot|$ if

(i) there is an inclusion $i : K \to \bar{K}$ respecting the valuations;

(ii) the image $i(K)$ is dense in $\bar{K}$;

(iii) $\bar{K}$ with $||\cdot||$ is complete.

Example 3.31. $\mathbb{R}$ with respect to $|\cdot|_\infty$ is the completion of $\mathbb{Q}$.

Example 3.32. For a prime p, the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ is denoted by $\mathbb{Q}_p$. What is $\mathbb{Q}_p$? And how may we to construct it? The following process will answer these questions.

For each prime p, define

$$\mathcal{C}_p := \mathcal{C}_p(\mathbb{Q}) = \{(x_n) : (x_n) \text{ is a Cauchy sequence in } \mathbb{Q} \text{ with respect to } |\cdot|_p\},$$

with the additive and multiplicative operations as follows:

$$\begin{aligned}(x_n) + (y_n) &= (x_n + y_n),\\ (x_n) \cdot (y_n) &= (x_n y_n).\end{aligned}$$

Then $(\mathcal{C}_p, +, \cdot)$ is a commutative ring with unity. To prove this statement, we only need to check that $(x_n + y_n)$ and $(x_n y_n)$ are Cauchy. It is very easy to prove the sum is Cauchy as

$$(x_n + y_n) - (x_m + y_m) = (x_n - x_m) + (y_n + y_m).$$

For the product, we need to use the fact in Lemma 3.25 and then apply it to the identity

$$x_n y_n - x_m y_m = x_n(y_n - y_m) + y_m(x_n - x_m).$$

We define $\mathcal{M}_p \subset \mathcal{C}_p$ to be the ideal

$$\{(x_n) \in \mathcal{C}_p \ : \ x_n \to 0\} = \{(x_n) \in \mathcal{C}_p \ : \ \lim_{n\to\infty} |x_n|_p = 0\}$$

of sequences that tend to zero with respect to $|\cdot|_p$. By Lemma 3.2.8 in [12], $\mathcal{M}_p$ is a maximal ideal of $\mathcal{C}_p$. Thus $\mathcal{C}_p/\mathcal{M}_p$ is a field which is defined to be the p-adic field $\mathbb{Q}_p$. So all elements of $\mathbb{Q}_p$ are equivalence classes of Cauchy sequences. For $\bar{x} = x + \mathcal{M}_p \in \mathbb{Q}_p$, where $x = (x_n) \in \mathcal{C}_p$, define

$$||\bar{x}||_p = \lim_{n\to\infty} |x_n|_p.$$

By Lemma 3.2.10 in [12], the limit defining $|\cdot|_p$ exists. It is also well defined: assume that $x + \mathcal{M}_p = y + \mathcal{M}_p$, where $x = (x_n),\ y = (y_n) \in \mathcal{C}_p$ and $x \neq y$. Then $x - y \in \mathcal{M}_p$. Thus

$$\lim_{n\to\infty} |x_n - y_n|_p = 0.$$

Consider

$$\begin{aligned}\lim_{n\to\infty}|x_n|_p &= \lim_{n\to\infty}|x_n - y_n + y_n|_p \\ &\leq \lim_{n\to\infty}|x_n - y_n|_p + \lim_{n\to\infty}|y_n|_p \\ &= \lim_{n\to\infty}|y_n|_p.\end{aligned}$$

Similarly, we get

$$\lim_{n\to\infty}|y_n|_p \leq \lim_{n\to\infty}|x_n|_p.$$

So

$$\lim_{n\to\infty}|x_n|_p = \lim_{n\to\infty}|y_n|_p.$$

Thus the valuation $||\cdot||_p$ on $\mathbb{Q}_p$ is well-defined. To prove that $\mathbb{Q}_p, ||\cdot||_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$, we need to check three properties in Definition 3.30. An inclusion of $\mathbb{Q}$ into the field $\mathbb{Q}_p$ is given by sending $q \in \mathbb{Q}$ to the equivalence class of the constant sequence $(q, q, ..., q) + \mathcal{M}_p$. It is clearly well-defined and also is injective. We need to check the remaining two properties: that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, and that $\mathbb{Q}_p$ is complete. The proof of these properties may be found in [12, page 57-59]. Hence we have proved that $\mathbb{Q}_p, ||\cdot||_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

Definition 3.33. . Two valuations $|\cdot|_1$ and $|\cdot|_2$ on a field K are called *equivalent* if the metrics defined by $|\cdot|_1$ and $|\cdot|_2$ as in Remark 3.13(ii) give the same convergent sequences.

Proposition 3.34. *Let $|\cdot|_1$ and $|\cdot|_2$ be valuations on K, with $|\cdot|_1$ non-trivial. The following are equivalent:*

(i) $|\cdot|_1$ and $|\cdot|_2$ are equivalent;

(ii) for any $x \in K$, we have $|x|_1 < 1 \Leftrightarrow |x|_2 < 1$;

(iii) there exists a positive real number α such that, for all $x \in K$,

$$|x|_1 = |x|_2^{\alpha};$$

(iv) if $\bar{K}_i, ||\cdot||_i$ denotes the completion of K with respect to $|\cdot|_i$, then there is an isomorphism $\phi : \bar{K}_1 \to \bar{K}_2$ such that $||\cdot||_1$ and $||\phi(\cdot)||_2$ are equivalent valuations on $\bar{K}_1$.

Proof. The proof may be found in [12, Theorem 3.1.2]. □

Definition 3.35. Let K be an $\mathbb{A}$-field. A *place* of K is an equivalence class of valuations of K (in the sense of Proposition 3.34). Let $P(K)$ denote the set of places of K and $P_\infty(K)$ denote the set of *infinite* places of K.

If characteristic $K = 0$, an infinite place means an equivalence class of an archimedean valuation on K. For example, $K = \mathbb{Q}$, we have $P_\infty(K) = \{|.|_\infty\}$ because there is only an archimedean valuation on $\mathbb{Q}$. If characteristic $K = p > 0$, an infinite place can be chosen arbitrarily as in Example 3.20. $P_\infty(K)$ is always finite (see [37]). We will only need these ideas for $\mathbb{Q}$ and $\mathbb{F}_p(t)$, where we have the following form of Ostrowski's Theorem.

Theorem 3.36 (Ostrowski)**.** *The places of $\mathbb{Q}$ are in one-to-one correspondence with $\mathbb{P} \cup \{\infty\}$. The places of $\mathbb{F}_p(t)$ are in one-to-one correspondence with*

$$\{\textit{irreducible polynomials in } \mathbb{F}_p[t]\} \cup \{\infty\}.$$

Proof. The proof may be found in [12, Theorem 3.1.3]. □

3.4 S-integer Dynamical Systems

Definition 3.37. Let K be an $\mathbb{A}$-field. For any set $S \subseteq P(K) \setminus P_\infty(K)$, define

$$R_S = \{x \in K : |x|_w \leq 1 \text{ for all } \ w \notin S \cup P_\infty(K)\},$$

the ring of S-integers. It is a discrete subgroup in K (in the discrete topology on K). Write $\hat{R_S}$ for the set of all homomorphisms from R_S to S^1 which is a compact abelian group in the topology of uniform convergence on compact sets. That is, characters are close if they are uniformly close on finite sets in R_S.

Example 3.38. 1. $K = \mathbb{Q}$ and $S = \emptyset$, then

$$R_S = \{x \in \mathbb{Q} : |x|_p \leq 1 \text{ for all primes } p\} = \mathbb{Z}.$$

2. $K = \mathbb{Q}$ and $S = \{2\}$, then

$$R_S = \left\{ \frac{a}{2^n} : a, n \in \mathbb{Z} \right\} = \mathbb{Z}\left[\tfrac{1}{2}\right].$$

3. In general, if $K = \mathbb{Q}$ and S is a finite subset of rational primes, say $\{p_1, p_2, \ldots, p_r\}$, then

$$R_S = \left\{ \frac{a}{b} \in \mathbb{Q} : \text{primes dividing } b \text{ lie in } S \right\} = \mathbb{Z}\left[\frac{1}{p_1 p_2 \cdots p_r}\right].$$

4. $K = \mathbb{F}_p(t)$ and $S = \emptyset$, then $R_S = \mathbb{F}_p[t]$.

5. $K = \mathbb{F}_p(t)$ and $S = \{t\}$, then $R_S = \mathbb{F}_p[t^{\pm 1}]$.

Now, the S-integer dynamical systems, which generalize simple maps like the circle doubling map or toral automorphisms, will be introduced by associating via duality a dynamical system to each pair (R_S, ξ) where ξ is an element of $R_S \setminus \{0\}$ (see [5]).

Definition 3.39. Let ξ be a non-zero element of R_S and let $\alpha = \alpha^{(K,S,\xi)}$ be the surjective endomorphism of the compact group $X^{(K,S,\xi)} = \hat{R_S}$, dual to multiplication by ξ on R_S (i.e. the monomorphism $\hat{\alpha} : R_S \to R_S$ defined by $\hat{\alpha}(x) = \xi x$). The pair $(X^{(K,S,\xi)}, \alpha^{(K,S,\xi)})$ forms a dynamical system which is called an *S-integer dynamical system.*

In my work, we will only be concerned with two cases:

(1) If $K = \mathbb{Q}$ then $\xi = \frac{a}{b}$ is a rational, S is a subset of the rational primes $\mathbb{P}$ including all primes dividing b, and the compact group $\hat{R}_S$ is one-dimensional. If ξ is a unit in R_S, then all primes dividing a are also in S and the resulting map is invertible.

(2) If $K = \mathbb{F}_p(t)$ then $\xi = \frac{a(t)}{b(t)}$ is a rational function, S is a subset of the set of irreducibles of $\mathbb{F}_p[t]$ together with the place at ∞, including all irreducibles dividing $b(t)$. In this case the compact group $\hat{R}_S$ is zero-dimensional.

Example 3.40. (i) Let $K = \mathbb{Q}, S = \emptyset$ and $\xi = 2$. By the above definition, $\hat{\alpha} : \mathbb{Z} \to \mathbb{Z}$ is the map $x \mapsto 2x$, and so the continuous group endomorphism $\alpha : \mathbb{T} \to \mathbb{T}$ is the circle doubling map, $x \mapsto 2x \mod 1$. We note that $\hat{\mathbb{Z}} = \mathbb{T}$.

(ii) Let $K = \mathbb{Q}$, $S = \{2\}$, and $\xi = 2$. Then $\hat{R}_S$ is the solenoid $\widehat{\mathbb{Z}[\frac{1}{2}]}$ and α is the automorphism of X dual to the automorphism $x \mapsto 2x$ on R_S. This is the natural invertible extension of the circle doubling map [18, Section2].

(iii) Let $K = \mathbb{Q}$, $S = \{2, 3, 5, 7, 11, \dots\}$ and $\xi = \frac{3}{2}$. Then $R_S = \mathbb{Q}$ and α is the automorphism of the full solenoid $\widehat{\mathbb{Q}}$ dual to multiplication by $\frac{2}{3}$ on $\mathbb{Q}$ [20, Section2].

(iv) If $K = \mathbb{Q}$ and S contains all primes but one prime (say 3) and $\xi = 2$ then

$$R_S = \mathbb{Z}\left[\frac{1}{2}, \frac{1}{5}, \frac{1}{7}, \frac{1}{11}, \dots\right] = \mathbb{Z}_{(3)}$$

Then α is the automorphism of $X = \hat{R}_S$ dual to the automorphism $x \mapsto 2x$ on R_S.

(v) Let $K = \mathbb{F}_p(t)$, $S = \emptyset$ and $\xi = t$. Then $\hat{R}_S = \prod_{i=0}^{\infty} \{0, 1, \dots, p-1\}$ and α is the one-sided shift on p symbols.

(vi). Let $K = \mathbb{F}_p(t)$, $S = \{t\}$ and $\xi = t$. Then $\hat{R}_S = \prod_{i=-\infty}^{\infty} \{0, 1, \dots, p-1\}$ and α is the left shift on the space of two-sided sequences of p symbols.

3.5 Periodic Points and Topological Entropy of S-integer maps

The following lemma is a generalization of Example 2.2 in Section 2.1.

Theorem 3.41. *Let $(X, \alpha) = (X^{(K,S,\xi)}, \alpha^{(K,S,\xi)})$ be an S-integer dynamical system. Then the number of periodic points $n \geq 1$ is finite for all n if α is ergodic, and*

$$F_\alpha(n) = \prod_{w \in S \cup P_\infty(K)} |\xi^n - 1|_w.$$

Proof. The proof may be found in [5, Theorem 5.2]. □

Theorem 3.42. *The topological entropy of S-integer dynamical system $(X^{(K,S,\xi)}, \alpha^{(K,S,\xi)})$ is given by*

$$h(\alpha^{(K,S,\xi)}) = \sum_{w \in S \cup P_\infty(K)} \log^+ |\xi|_w,$$

where $\log^+ |\xi|_w = \max\{\log |\xi|_w, 0\}$.

Again, the proof can be found in [5, Theorem 4.1]. Example 2.11 is generalized by this lemma.

Example 3.43. (i) Let $K = \mathbb{Q},\ S = \emptyset$ and $\xi = 2$. Then α is the circle doubling map. So $F_\alpha(n) = 2^n - 1$ and $h(\alpha) = \log 2$

(ii) Let $K = \mathbb{Q},\ S = \{2\}$, and $\xi = 2$. Thus

$$F_\alpha(n) = (2^n - 1)|2^n - 1|_2 = 2^n - 1,$$

and $h(\alpha) = \log 2$.

(iii) Let $K = \mathbb{Q},\ S = \{2, 3, 5, 7, 11, \dots\}$ and $\xi = \frac{3}{2}$. The map α has only one periodic point for any period by Lemma 3.41 and Lemma 3.21, and $h(\alpha) = \log 3$.

(iv) If $K = \mathbb{Q}$ and S contains all primes but one prime (say 3) and $\xi = 2$. By following Lemma 3.41 and applying Lemma 3.21, we get $F_\alpha(n) = |2^n - 1|_3^{-1}$. Here $h(\alpha) = \log 2$.

(v) Let $K = \mathbb{F}_p(t),\ S = \{t\}$ and $\xi = t$. By Lemma 3.41,

$$\begin{aligned} F_\alpha(n) &= |t^n - 1|_\infty \times |t^n - 1|_t \\ &= \left|t^{-n} - 1\right|_t \times 1 \\ &= \left|\frac{1 - t^n}{t^n}\right|_t \\ &= p^n. \end{aligned}$$

Thus $F_\alpha(n) = p^n$ for all $n \geq 1$.

(vi). Let $K = \mathbb{F}_p(t),\ S = \emptyset$ and $\xi = t$. The same calculation as in (v) shows that $F_n(\alpha) = p^n$ for all $n \geq 1$.

3.6 Growth Rate of Periodic Points

Let (X, α) be a dynamical system, where α is a continuous map from a compact metric space $X = (X, d)$ to itself. We shall introduce upper and lower growth rates of the number of periodic points p^+ and p^- in such a system as follows:

$$p^+(\alpha) = \limsup_{n\to\infty} \frac{1}{n} \log |F_\alpha(n)|,$$

and

$$p^-(\alpha) = \liminf_{n\to\infty} \frac{1}{n} \log |F_\alpha(n)|.$$

Definition 3.44. If

$$\lim_{n\to\infty} \frac{1}{n} \log |F_\alpha(n)|$$

exists (i.e. $p^+(\alpha) = p^-(\alpha)$), then we say that it is the exponential growth rate of the number of periodic points in a dynamical system.

Following [5], we call any S-integer dynamical system *arithmetic* if it is built from a field of characteristic zero, and *geometric* if not. Equivalently, an S-integer dynamical system (X, α) is called arithmetic if X is connected, and geometric if X is totally disconnected.

Theorem 3.45. *Let $(X^{(K,S,\xi)}, \alpha^{(K,S,\xi)})$ be an ergodic arithmetic S-integer dynamical system with S finite. Then the growth rate of the number of periodic points exists and is given by*

$$p^+(\alpha) = p^-(\alpha) = h(\alpha).$$

Proof. See [5, Theorem 6.1]. □

Theorem 3.46. *Let $(X^{(K,S,\xi)}, \alpha^{(K,S,\xi)})$ be an ergodic geometric S-integer dynamical system with S finite. Then*

$$p^+(\alpha) = h(\alpha).$$

Proof. See [5, Theorem 6.2]. □

We will here restrict our interest to the case $K = \mathbb{Q}, \xi = 2$. By following Theorem 3.45, we guarantee that the exponential growth rate of the number of periodic points and the topological entropy in S-integer dynamical systems arising from the case $K = \mathbb{Q},\ \xi = 2$ and $|S| < \infty$ are equal. However, if S is co-finite, they are not the same. The following table taken from [30, page 29] will illustrate the exponential growth rate of the number of periodic points and the topological entropy in the

systems.

ξ	S	Periodic Points : $F_\alpha(n)$	$h(\alpha)$	$\lim_{n\to\infty} \frac{1}{n} \log \lvert F_\alpha(n)\rvert$
2	$\emptyset$	$2^n - 1$	$\log 2$	$\log 2$
2	$\{3\}$	$\lvert 2^n - 1\rvert \lvert 2^n - 1\rvert_3$	$\log 2$	$\log 2$
2	$\{3, 5\}$	$\lvert 2^n - 1\rvert \lvert 2^n - 1\rvert_3 \lvert 2^n - 1\rvert_5$	$\log 2$	$\log 2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
2	$\{2, 5, 7, 11, \dots\}$	$\lvert 2^n - 1\rvert \prod_{p\neq 3} \lvert 2^n - 1\rvert_p$	$\log 2$	0
2	$\{2, 7, 11, \dots\}$	$\lvert 2^n - 1\rvert \prod_{p\neq 3,5} \lvert 2^n - 1\rvert_p$	$\log 2$	0

This table shows that the exponential growth rates of the number of periodic points is understood when S is finite or co-finite. However, it is not clear in general. For a "typical" (that is, random) set of primes S (see [35], [36], and [5]), the assumption of Artin's conjecture implies that

$$p^-(\alpha) = 0, \text{ and } p^+(\alpha) = h(\alpha). \tag{21}$$

More details can be found in [5].

Chapter 4

Mertens' Theorem in Zero Characteristic

4.1 Prime Orbit Theorem and Mertens' Theorem for Orbits

Let (X, α) be a dynamical system where X is a compact metric space and α is a continuous map. A dynamical analogue of the prime number theorem concerns the asymptotic behaviour of expressions like

$$\pi_\alpha(N) = |\{ \tau \text{ is a closed orbit } : |\tau| \leq N \}|, \tag{22}$$

and a dynamical analogue of Mertens' theorem concerns asymptotic estimates for expressions like

$$M_\alpha(N) = \sum_{|\tau| \leq N} \phi(|\tau|), \tag{23}$$

where ϕ is some positive function of $|\tau|$. For example, if $\phi(|\tau|) = 1$ then $M_\alpha(N) = \pi_\alpha(N)$. In the works of Parry [26], Parry and Pollicot [25], Sharp [29] and others, we

may find results about the asymptotic behaviour of (22) and (23) with $\phi(|\tau|) = \frac{1}{e^{h(\alpha)|\tau|}}$ where $h(\alpha)$ denotes the topological entropy of α under the assumption that X has a metric structure with respect to which α is hyperbolic. They show that

$$\pi_\alpha(N) \sim \frac{e^{h(N+1)}}{N(e^h - 1)},$$

the orbit counting function π_α, and

$$M_\alpha(N) \sim \log N + C_1, \tag{24}$$

for some constant C_1.

Everest, Miles, Stevens and Ward [8] considered the same question for the simplest non-hyperbolic algebraic systems. In simple examples they exhibited uncountably many different asymptotic growth rates for the orbit counting function π_α and they also have shown an explicit rational leading coefficient in the dynamical Mertens' theorem (24) as follows.

Theorem 4.1. *Let $\alpha : X \to X$ be an $S-$integer map with X connected and with S finite. Then there are constants $k_S \in \mathbb{Q}$, C_S and $\delta > 0$ with*

$$M_\alpha(N) = k_S \log N + C_S + O(N^{-\delta}).$$

Example 4.2. Let $\xi = 2$, $K = \mathbb{Q}$, and S be a finite subset of primes, so α is map dual to $x \mapsto 2x$ on the ring $R_S = \{\frac{p}{q} \in \mathbb{Q} : \text{primes dividing } q \text{ lie in } S\}$. The constant k_S for various simple sets S is shown below:

S	value of k_S
$\emptyset$	1
$\{3\}$	$\frac{5}{8}$
$\{3,5\}$	$\frac{55}{96}$
$\{3,7\}$	$\frac{269}{576}$
co-finite	0

In the hyperbolic setting, or for systems close to hyperbolic, $F_\alpha(n)$ and $O_\alpha(n)$ typically grow exponentially fast. This means the natural normalization in Mertens' theorem is a rapidly-decaying function of $|\tau|$.

Example 4.3. In the notation of Section 3.4 taking $\xi = 2,\ K = \mathbb{Q},\ S = \emptyset$ gives the map $x \mapsto 2x$ on $\mathbb{T}$ (the circle doubling map). Hence

$$F_\alpha(n) = 2^n - 1,\ h(\alpha) = \log 2$$

and we claim that

$$\sum_{|\tau| \le N} \frac{1}{2^{|\tau|}} = \log N + C_2 + O(1/N), \tag{25}$$

for some constant C_2.

Proof of claim (25). This result may be seen by isolating dominant terms in $M_\alpha(N)$. Note that

$$M_\alpha(N) = \sum_{|\tau| \le N} \frac{1}{2^{|\tau|}} = \sum_{n \le N} \frac{O_\alpha(n)}{2^n},$$

where

$$O_\alpha(n) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right)(2^d - 1),$$

and define

$$F(N) = \sum_{n\leq N} \frac{1}{n}.$$

Now

$$\begin{aligned} M_\alpha(N) - F(N) &= \left(\sum_{n\leq N}\frac{1}{n}\sum_{d|n}\frac{\mu(\frac{n}{d})(2^d-1)}{2^n}\right) - \sum_{n\leq N}\frac{1}{n} \\ &= \sum_{n\leq N}\frac{1}{n}\sum_{d|n}\left(\frac{\mu(\frac{n}{d})(2^d-1)}{2^n} - 1\right) \\ &= \sum_{n\leq N}\frac{1}{n}\left(-\frac{1}{2^n} + \sum_{d|n,d<n}\frac{\mu(\frac{n}{d})(2^d-1)}{2^n}\right) \\ &= -\sum_{n\leq N}\frac{1}{n2^n} + \sum_{n\leq N}\frac{1}{n2^n}\sum_{d|n,d<n}\mu\left(\frac{n}{d}\right)(2^d-1). \end{aligned}$$

We claim that

$$\sum_{n\leq N}\frac{1}{n2^n} = \log 2 + O(2^{-N}), \tag{26}$$

and

$$\sum_{n\leq N}\frac{1}{n2^n}\sum_{d|n,d<n}\mu\left(\frac{n}{d}\right)(2^d-1) = C_3 + O(2^{-N/2}) \tag{27}$$

for some constant C_3.

Firstly, we want to approximate the error terms of (26) and (27).

Consider

$$\begin{aligned} \left|\sum_{n\leq N}\frac{1}{n2^n} - \sum_{n=1}^{\infty}\frac{1}{n2^n}\right| &= \left|\sum_{n=N+1}^{\infty}\frac{1}{n2^n}\right| \\ &\leq \sum_{n=N+1}^{\infty}\frac{1}{2^n} \\ &= 2^{-N}. \end{aligned}$$

So

$$\sum_{n\leq N}\frac{1}{n2^n}-\sum_{n=1}^{\infty}\frac{1}{n2^n}=O(2^{-N}).$$

Note that

$$|\mu(n)|\leq 1 \text{ and } \sum_{d|n,d<n}(2^d-1)\leq n(2^{n/2}-1)\ \forall n\in\mathbb{N}. \tag{28}$$

Hence

$$\begin{aligned}\left|\sum_{n=N+1}^{\infty}\frac{1}{n2^n}\sum_{d|n,d<n}\mu\left(\frac{n}{d}\right)(2^d-1))\right| &\leq \left|\sum_{n=N+1}^{\infty}\frac{1}{n2^n}n(2^{n/2}-1)\right| \\ &\leq \sum_{n=N+1}^{\infty}\frac{1}{(\sqrt{2})^n} \quad \text{(a geometric series)} \\ &= \frac{1}{(\sqrt{2})^{N+1}}\left(\frac{1}{1-\frac{1}{\sqrt{2}}}\right) \\ &= \frac{2^{-N/2}}{\sqrt{2}-1}.\end{aligned}$$

This implies that

$$\left(\sum_{n\leq N}\frac{1}{n2^n}\sum_{d|n,d<n}\mu\left(\frac{n}{d}\right)(2^d-1)\right)-\left(\sum_{n=0}^{\infty}\frac{1}{n2^n}\sum_{d|n,d<n}\mu\left(\frac{n}{d}\right)(2^d-1)\right)=O(2^{-N/2})$$

It remains to show that

$$\sum_{n=1}^{\infty}\frac{1}{n2^n}=\log 2,$$

and

$$\sum_{n=1}^{\infty}\frac{1}{n2^n}\sum_{d|n,d<n}\mu\left(\frac{n}{d}\right)(2^d-1)$$

converges. We notice that

$$\log(1+x)=x-\frac{x^2}{2}+\frac{x^3}{3}-\frac{x^4}{4}+\cdots. \tag{29}$$

Applying $x=-\frac{1}{2}$ in (29), we get

$$-\log 2=-\frac{1}{2}-\frac{1}{2\cdot 2^2}-\frac{1}{3\cdot 2^3}-\frac{1}{3\cdot 2^3}-\cdots.$$

Thus

$$\sum_{n=1}^{\infty} \frac{1}{n2^n} = \log 2.$$

Since

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{1}{n2^n} \sum_{d|n, d<n} \mu\left(\frac{n}{d}\right)(2^d - 1) &\leq \sum_{n=1}^{\infty} \frac{1}{n2^n} n(2^{\frac{n}{2}} - 1) \qquad \text{(by (28))} \\
&= \sum_{n=1}^{\infty} \frac{1}{(\sqrt{2})^n} - \sum_{n=1}^{\infty} \frac{1}{(2)^n} \quad \text{(a geometric series)} \\
&= \frac{1}{\sqrt{2}} \left(\frac{1}{1 - \frac{1}{\sqrt{2}}}\right) - \frac{1}{2} \left(\frac{1}{1 - \frac{1}{2}}\right) \\
&= \sqrt{2},
\end{aligned}$$

it follows that

$$\sum_{n=1}^{\infty} \frac{1}{n2^n} \sum_{d|n, d<n} \mu\left(\frac{n}{d}\right)(2^d - 1)$$

converges to some constant C_3.

Hence the proof of the claims in (26) and (27) is completed. Therefore, by these claims, we get

$$M_\alpha(N) - F(N) = -\log 2 + C_3 + O(2^{-N/2}).$$

By Lemma 1.21, we obtain that

$$M_\alpha(N) = \log N + C_2 + O(1/N),$$

where $C_2 = \gamma - \log 2 + C_3$. □

As we have shown the partial sum of the diverging harmonic series by using the EMSF in Lemma 1.23, an immediate consequence of Lemma 1.23 and Example 4.3 is the following corollary.

Corollary 4.4. *Let α be the circle doubling map. Then, for any $k \geq 0$,*

$$\sum_{|\tau| \leq N} \frac{1}{2^{|\tau|}} = \log N + C_2 - \sum_{r=0}^{k-1} \left(\frac{B_{r+1}}{r+1} \right) \frac{1}{N^{r+1}} + O(1/N^{k+1}),$$

where B_{r+1} are the Bernoulli numbers.

Notice that if $k = 0$, the statements in Corollary 4.4 and Example 4.3 are the same.

Remark 4.5. The result in (25) is the same as (24) because the map α is hyperbolic. The following example is the simplest non-hyperbolic map in such examples and we can prove (24) directly as the above example. If α is the map in Example 4.2 and S is a nonempty finite set (that is, α is non-hyperbolic), the leading coefficient of $M_\alpha(N)$ is rational less than 1 by Theorem 4.1.

Example 4.6. Taking $\xi = 2,\ K = \mathbb{Q},\ S = \{3\}$ gives the endomorphism $\alpha : x \mapsto 2x$ on $\widehat{\mathbb{Z}[\frac{1}{3}]}$. Then by Theorem 3.41 and Theorem 3.42, we have

$$F_\alpha(n) = (2^n - 1)|2^n - 1|_3,\ h(\alpha) = \log 2$$

and [8] shows that (24) changes to become

$$\sum_{|\tau| \leq N} \frac{1}{2^{|\tau|}} = \frac{5}{8} \log N + C_5 + O(1/N),$$

for some constant C_5.

The proof of the above example can be found in [8], or seen later in Example 5.11.

4.2 Mertens' Theorem for Toral Automorphisms

Let $\alpha : \mathbb{T}^d \to \mathbb{T}^d$ be a toral automorphism corresponding to a matrix A in $GL_d(\mathbb{Z})$. Let $\{\lambda_i | 1 \leq i \leq d\}$ be the set of eigenvalues of A which we may arrange as

$$|\lambda_1| \geq \cdots \geq |\lambda_s| > 1 = |\lambda_{s+1}| = \cdots = |\lambda_{s+2t}| > |\lambda_{s+2t+1}| \geq \cdots \geq |\lambda_d|. \tag{30}$$

By Theorem 3.9, we have

$$F_\alpha(n) = \prod_{i=1}^{d} |\lambda_i^n - 1|.$$

and by Theorem 3.11, the topological entropy $h(\alpha)$ is equal to $\log|\Lambda|$, where $\Lambda = \prod_{i=1}^{s} \lambda_i$. The purpose of this section is to give an elementary proof of the dynamical Mertens' Theorem for toral automorphisms. Indeed, Noorani [24] already proved such a theorem for a quasihyperbolic toral automorphism which is expressed as the form

$$M_\alpha(N) = m \log N + C_6 + o(1),$$

where the constant C_6 is related to analytic data coming from the dynamical zeta function and the constant $m = 2^t$, where $2t$ is the number of eigenvalues modulus one of the matrix A.

In our proof, we improve the error terms in the hyperbolic and the quasihyperbolic cases to $O(N^{-k})$ for any $k \geq 0$ and $O(N^{-1})$, respectively. The result for such toral automorphisms can be derived directly without the need for the dynamical zeta function. Moreover, in the quasihyperbolic case, we will illustrate how to compute the coefficient of the main term and indeed, this constant is not necessarily 2^t as mentioned above.

As mentioned above, we will prove a dynamical analogue of Mertens' theorem for toral automorphisms so let us write

$$M_\alpha(N) = \sum_{n=1}^{N} \frac{O_\alpha(n)}{e^{hn}}.$$

Remark 4.7. In the quasihyperbolic case, we notice that the complex eigenvalues appear in conjugate pairs. Thus we may arrange that $\lambda_{i+t} = \bar{\lambda_i}$ for $s+1 \leq i \leq s+t$.

Then

$$\begin{aligned} |\lambda_i^n - 1||\lambda_{i+t}^n - 1| &= |2 - (\lambda_i^n + \lambda_{i+t}^n)| \\ &= 2 - (\lambda_i^n + \lambda_{i+t}^n) \\ &= (\lambda_i^n - 1)(\lambda_{i+t}^n - 1). \end{aligned}$$

So

$$\prod_{i=s+1}^{s+2t} |\lambda_i^n - 1| = \prod_{i=s+1}^{s+2t} (\lambda_i^n - 1).$$

Now, we will first prove the following two lemmas before we are going to prove the main theorem. Let

$$\epsilon = \min\{|\lambda_s|, |\lambda_{s+2t+1}|^{-1}\} > 1.$$

Lemma 4.8. *Let α be an ergodic toral automorphism corresponding to a matrix $A \in GL_d(\mathbb{Z})$ with topological entropy $h = \log|\Lambda|$. There is an $\epsilon > 0$ such that*

$$\left(F_\alpha(n) - |\Lambda|^n \prod_{i=s+1}^{s+2t} (\lambda_i^n - 1) \right) \cdot |\Lambda|^{-n} = O(\epsilon^{-n}), \tag{31}$$

Proof. Firstly, let us divide the sequence $\prod_{i=1}^{d}(\lambda_i^n - 1)$ into three parts:

$$\prod_{i=1}^{d}(\lambda_i^n - 1) = \underbrace{\prod_{i=1}^{s}(\lambda_i^n - 1)}_{U_n} \underbrace{\prod_{i=s+1}^{s+2t} (\lambda_i^n - 1)}_{V_n} \underbrace{\prod_{i=2t+s+1}^{d} (\lambda_i^n - 1)}_{W_n}.$$

Then we will consider each of these terms as follows:

(i) The term U_n is equal to

$$\Lambda^n + \underbrace{\sum_{D \subset \{1,\ldots,s\}} (-1)^{s-|D|} \left(\prod_{i \in D} \lambda_i^n \right)}_{A},$$

where for each $D \subset \{1, \ldots, s\}$,

$$\frac{\prod_{i \in D} \lambda_i^n}{|\Lambda|^n} = O(\epsilon^{-n}). \tag{32}$$

(ii) The term W_n is equal to

$$(-1)^{d-s} + \underbrace{\sum_{\emptyset \neq F \subseteq \{2t+s+1, \ldots, d\}} (-1)^{d-2t-s-|F|} \left(\prod_{i \in F} \lambda_i^n \right)}_{B},$$

where for each $\emptyset \neq F \subseteq \{2t + s + 1, \ldots, d\}$,

$$\prod_{i \in F} \lambda_i^n = O(\epsilon^{-n}). \tag{33}$$

(iii) $|V_n| \leq 2^{2t}$ since $|\lambda_i| = 1$ for all $i = s + 1, \ldots, s + 2t$.

In order to complete the result of this lemma, notice that

$$\begin{aligned} U_n W_n &= (-1)^{d-s} \Lambda^n + \Lambda^n B + (-1)^{d-s} A + AB \\ &= (-1)^{d-s} \Lambda^n + O(\Lambda^n \epsilon^{-n}) \qquad \text{(by (32) and (33)).} \end{aligned}$$

Consequently,

$$\begin{aligned} \left| \frac{\prod_{i=1}^d (\lambda_i^n - 1) - (-1)^{d-s} \Lambda^n \prod_{i=s+1}^{s+2t} (\lambda_i^n - 1)}{|\Lambda|^n} \right| &= \left| \frac{V_n (U_n W_n - (-1)^{d-s} \Lambda^n)}{|\Lambda|^n} \right| \\ &= \left| \frac{V_n O(\Lambda^n \epsilon^{-n})}{|\Lambda|^n} \right| \\ &\leq C_7 \epsilon^{-n}, \end{aligned}$$

for some constant C_7.

Hence by the reverse triangle inequality, we can get the result as required. □

In Lemma 4.8 we also may write the equation (31) as

$$\frac{F_\alpha(n)}{|\Lambda|^n} = V_n + O(\epsilon^{-n}), \tag{34}$$

and particularly, if α is hyperbolic, then we have

$$\frac{F_\alpha(n)}{|\Lambda|^n} = 1 + O(\epsilon^{-n}).$$

Lemma 4.9. *If ω is a complex number of modulus one and is not a root of unity, then*

$$\sum_{n=1}^{N} \frac{\omega^n}{n} = -\log(1-\omega) + O(N^{-1}). \tag{35}$$

Proof. By [14, page 69-70], we know that $\sum_{n=1}^{N} \frac{\omega^n}{n}$ converges and by the Abel continuity theorem [14, Theorem 2.6.4], it converges to $-\log(1-\omega)$. To get the error term $O(N^{-1})$ in (35), we will apply partial summation [23, Theorem 2.1.1] to the sum $\sum_{n=1}^{N} \frac{\omega^n}{n}$ with $a_n = \omega^n$ and $f(t) = \frac{1}{t}$ on $[1, N]$ as follows.

$$\sum_{n=1}^{N} \frac{\omega^n}{n} = \frac{1}{N} \underbrace{\sum_{n=1}^{N} \omega^n}_{O(1)} + \underbrace{\int_1^\infty \left(\sum_{n=1}^{t} \omega^n \right) \frac{1}{t^2} dt}_{<\infty} - \int_N^\infty \underbrace{\left(\sum_{n=1}^{t} \omega^n \right) \frac{1}{t^2}}_{O(t^{-2})} dt.$$

□

To get an alternative formula of V_n, we may put

$$\Omega = \left\{ \prod_{i \in I} \lambda_i^n \mid I \subseteq \{s+1, \ldots, s+2t\} \right\},$$

$$\mathcal{I}(\omega) = \{I \subset \{s+1, \ldots, s+2t\} \mid \prod_{i \in I} \lambda_i^n = \omega\},$$

and

$$K(\omega) = \sum_{I \in \mathcal{I}(\omega)} (-1)^{|I|}.$$

We notice that $\mathcal{I}(\omega) = \emptyset$ unless $\omega \in \Omega$.

Then we get

$$V_n = \sum_{\omega \in \Omega} K(\omega) \omega^n.$$

Lemma 4.10. *Let α be a quasihyperbolic toral automorphism with topological entropy h. Then there is a constant $m \geq 1$ with*

$$F(N) = m \log N + m\gamma - \sum_{\omega \in \Omega \setminus \{1\}} K(\omega) \log(1-\omega) + O(N^{-1}),$$

Proof. Since α is quasihyperbolic, $t > 0$ and the complex eigenvalues appear in conjugate pairs. It follows that

$$V_n = \sum_{\omega \in \Omega} K(\omega)\omega^n$$

Consequently,

$$\begin{aligned} F(N) &= \sum_{n=1}^{N} \frac{1}{n} \sum_{\omega \in \Omega} K(\omega)\omega^n \\ &= \sum_{\omega \in \Omega} K(\omega) \sum_{n=1}^{N} \frac{\omega^n}{n} \\ &= m \sum_{n=1}^{N} \frac{1}{n} + \sum_{\omega \in \Omega \setminus \{1\}} K(\omega) \sum_{n=1}^{N} \frac{\omega^n}{n} \\ &= m \log N + m\gamma - \sum_{\omega \in \Omega \setminus \{1\}} K(\omega) \log(1-\omega) + O(N^{-1}), \end{aligned}$$

since

$$\sum_{n=1}^{N} \frac{1}{n} = \log N + \gamma + O(N^{-1}),$$

by Lemma 1.21 and

$$\sum_{n=1}^{N} \frac{\omega^n}{n} = -\log(1-\omega) + O(N^{-1}) \quad \text{by Lemma 4.9 .}$$

□

Theorem 4.11. *Let α be a quasihyperbolic toral automorphism with topological entropy h. Then there are constants C_8 and $m \geq 1$ with*

$$M_\alpha(N) = m \log N + C_8 + O(N^{-1}).$$

Proof. Recall that

$$\begin{aligned} M_\alpha(N) &= \sum_{n=1}^{N} \frac{O_\alpha(n)}{e^{hn}} \\ &= \sum_{n=1}^{N} \frac{1}{n|\Lambda|^n} \sum_{d|n} \mu\left(\frac{n}{d}\right) F_\alpha(d), \end{aligned}$$

and

$$V_n = \prod_{i=s+1}^{s+2t} (\lambda_i^n - 1).$$

Define

$$F(N) = \sum_{n \le N} \frac{V_n}{n}.$$

Then

$$\begin{aligned} M_\alpha(N) - F(N) &= \sum_{n=1}^{N} \frac{1}{n|\Lambda|^n} \sum_{d|n} \mu\left(\frac{n}{d}\right) F_\alpha(d) - \sum_{n=1}^{N} \frac{1}{n} V_n \\ &= \sum_{n=1}^{N} \frac{1}{n} \left[\sum_{d|n, d<n} |\Lambda|^{-n} \mu\left(\frac{n}{d}\right) F_\alpha(d) + |\Lambda|^{-n} F_\alpha(n) - V_n \right] \\ &= \sum_{n=1}^{N} \frac{1}{n} \left[\sum_{d|n, d<n} |\Lambda|^{-n} \mu\left(\frac{n}{d}\right) F_\alpha(d) + O(\epsilon^{-n}) \right] \quad \text{(by (34))} \\ &= \sum_{n=1}^{N} \frac{1}{n|\Lambda|^n} \sum_{d|n, d<n} \mu\left(\frac{n}{d}\right) F_\alpha(d) + \sum_{n=1}^{N} \frac{1}{n} O(\epsilon^{-n}), \end{aligned}$$

which are the remainder terms of $M_\alpha(N)$. So we claim that there are constants C_9 and C_{10} such that

$$\sum_{n=1}^{N} \frac{1}{n|\Lambda|^n} \sum_{d|n, d<n} \mu\left(\frac{n}{d}\right) F_\alpha(d) = C_9 + O(\Lambda^{-N/2}), \tag{36}$$

and

$$\sum_{n=1}^{N} \frac{1}{n} O(\epsilon^{-n}) = C_{10} + O(\epsilon^{-N}). \tag{37}$$

Then let us consider how these error terms are obtained in the difference between $M_\alpha(N)$ and $F(N)$. We observe that

$$\left| \sum_{n=N}^{\infty} \frac{1}{n|\Lambda|^n} \sum_{d|n, d<n} \mu\left(\frac{n}{d}\right) F_\alpha(d) \right| \;\leq\; C_{11}\Lambda^{-N/2},$$

for some constant C_{11}, and

$$\left| \sum_{n=N}^{\infty} \frac{1}{n} O(\epsilon^{-n}) \right| \;\leq\; C_{12}\epsilon^{-N},$$

for some constant C_{12}.

Also, we notice that

$$\sum_{n=1}^{\infty} \frac{1}{n|\Lambda|^n} \sum_{d|n, d<n} \mu\left(\frac{n}{d}\right) F_\alpha(d)$$

and

$$\sum_{n=1}^{\infty} \frac{1}{n} O(\epsilon^{-n})$$

are convergent, so they converge to constants C_9 and C_{10}, respectively. It follows that there are constants C_9 and C_{10} for which

$$\sum_{n=1}^{N} \frac{1}{n|\Lambda|^n} \sum_{d|n, d<n} \mu\left(\frac{n}{d}\right) F_\alpha(d) - C_9 \;=\; O(\Lambda^{-N/2}),$$

and

$$\sum_{n=1}^{N} \frac{1}{n} O(\epsilon^{-n}) - C_{10} \;=\; O(\epsilon^{-N}).$$

Here we now complete the claims in (36) and (37). Hence

$$M_\alpha(N) = F(N) + C_9 + C_{10} + O(R^{-N}) \tag{38}$$

where $R = \min\{\epsilon, |\Lambda|^{1/2}\}$.

By Lemma 4.10, we finally conclude that

$$M_\alpha(N) = m \log N + C_8 + O(N^{-1}),$$

where $C_8 = C_9 + C_{10} + m\gamma - \sum_{\omega \in \Omega \setminus \{1\}} K(\omega) \log(1-\omega)$. □

Some notations in the above theorem will be needed again in the following corollary.

Corollary 4.12. *Let α be a hyperbolic toral automorphism with topological entropy h. Then for any $k \geq 0$,*

$$M_\alpha(N) = \log N + C_{14} - \sum_{r=0}^{k-1} \left(\frac{B_{r+1}}{r+1} \right) \frac{1}{N^{r+1}} + O(N^{-(k+1)}),$$

where $C_{14} = C_9 + C_{10} + \gamma$ and the B_{r+1} are the Bernoulli numbers.

Proof. Since α is hyperbolic, $V_n = 1$ and hence

$$F(N) = \sum_{n \leq N} \frac{1}{n}.$$

Replacing $F(N)$ in (38) of the above theorem, then we get

$$M_\alpha(N) = \sum_{n \leq N} \frac{1}{n} + C_9 + C_{10} + O(R^{-N}).$$

Then we apply Lemma 1.23 to $F(N)$ and finally, we can complete the proof as required. □

The following lemma is called *the Kronecker-Weyl lemma*, which will play an important part in computing the constant m appearing in Theorem 4.11.

Lemma 4.13. *Let g be an element of a compact abelian group G. Then the sequence (g^n) is uniformly distributed in the smallest closed subgroup of G containing g.*

Proof. The proof may be found in [8, Lemma 4.1]. □

Corollary 4.14. *Let α be the same map as in Theorem 4.11. The coefficient m in the Theorem is given by*

$$m = \int_X \prod_{i=1}^{t} (2 - 2\cos(2\pi x_i))\, dx_1 \cdots dx_t.$$

where $X \subset \mathbb{T}^d$ is the closure of $\{(n\theta_1, \ldots, n\theta_t) \mid n \in \mathbb{Z}\}$, and $e^{\pm 2\pi i\theta_1}, \ldots, e^{\pm 2\pi i\theta_t}$ are the eigenvalues with unit modulus of the matrix defining α.

Proof. Let $e^{\pm 2\pi i\theta_1}, \ldots, e^{\pm 2\pi i\theta_t}$ be the eigenvalues of modulus one of the matrix corresponding to the map α. Then we may write

$$\begin{aligned} V_n &= \prod_{j=1}^{t}(1 - e^{2\pi i\theta_j n})(1 - e^{-2\pi i\theta_j n}) \\ &= \prod_{j=1}^{t}(2 - 2\cos(2\pi\theta_j n)). \end{aligned}$$

Let $X \subseteq \mathbb{T}^t$ be the closure of $\{(n\theta_1, \ldots, n\theta_t) | n \in \mathbb{Z}\}$. Then the Kronecker-Weyl lemma may be applied to the element $(\theta_1, \ldots, \theta_t) \in X$ and we define the continuous function $f : X \to \mathbb{C}$ by

$$(x_1, \ldots, x_t) \mapsto \prod_{i=1}^{t}(2 - 2\cos(2\pi x_i)).$$

Thus

$$\frac{1}{N}\sum_{n=1}^{N}\prod_{j=1}^{t}(2 - 2\cos(2\pi\theta_j n)) \to \int_X \prod_{i=1}^{t}(2 - 2\cos(2\pi x_i))\, dx_1 \cdots dx_t$$

as $N \to \infty$. Then, by partial summation,

$$\begin{aligned} \sum_{n=1}^{N}\frac{1}{n}V_n &= \sum_{n=1}^{N}\left(\frac{1}{n} - \frac{1}{n+1}\right)\sum_{m=1}^{n}V_m + \frac{1}{N+1}\sum_{m=1}^{N}V_m \\ &\sim \left(\int_X \prod_{i=1}^{t}(2 - 2\cos(2\pi x_i))\, dx_1 \cdots dx_t\right)\log N \end{aligned}$$

so that

$$m = \int_X \prod_{i=1}^{t}(2 - 2\cos(2\pi x_i))\, dx_1 \cdots dx_t.$$

□

The value m depends on relations between arguments of eigenvalues of modulus one. Indeed, the quantity of the constant m may not be the same as its generic value 2^t as illustrated in the following examples:

Example 4.15. 1. If $\{\theta_1, \ldots, \theta_t\}$ is an independent set over $\mathbb{Q}$, (the generic case) then $X = \mathbb{T}^t$, so

$$\begin{aligned} m &= \int_0^1 \ldots \int_0^1 \prod_{i=1}^{t} (2 - 2\cos(2\pi x_i))\, dx_1 \cdots dx_t \\ &= \left(\int_0^1 (2 - 2\cos(2\pi x_1))\, dx_1 \right)^t = 2^t, \end{aligned}$$

as in Noorani [24].

2. Let α be the automorphism of $\mathbb{T}^8$ defined by the matrix $A \oplus A$, where

$$A = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 8 \\ 0 & 1 & 0 & -6 \\ 0 & 0 & 1 & 8 \end{pmatrix}. \tag{39}$$

Here X is a diagonally embedded circle, and

$$\begin{aligned} m &= \iint_{\{x_1 = x_2\}} \prod_{j=1}^{2} (2 - 2\cos(2\pi j x_j)) dx_1 \ldots dx_2 \\ &= \int_0^1 (2 - 2\cos(2\pi x))^2 dx = 6 > 2^2. \end{aligned}$$

3. Let A be the matrix as in the above Example and the map $\alpha : \mathbb{T}^{4t} \to \mathbb{T}^{4t}$ be the toral automorphism corresponding to the matrix $A \oplus \cdots \oplus A$ (t terms). The matrix A has one pair of eigenvalues with modulus one, so there are $2t$ eigenvalues with modulus one of the matrix corresponding to α. In this case X is a diagonally embedded circle, and so

$$\begin{aligned} m &= \int \cdots \int_{\{x_1 = \cdots = x_t\}} \prod_{i=1}^{t} (2 - 2\cos(2\pi x_i))\, dx_1 \cdots dx_t \\ &= \int_0^1 (2 - 2\cos(2\pi x_1))^t\, dx_1 = \frac{(2t)!}{(t!)^2} \sim \frac{2^{2t}}{\sqrt{\pi t}}. \end{aligned}$$

by Stirling's formula. This is much larger than 2^t and it follows that $\frac{m}{2^t}$ may be arbitrarily large.

4.3 Mertens' Theorem for Slow Growth

Our aim is to find dynamical analogues of Mertens' theorem for dynamical systems of slow growth, in which quantities like $F_\alpha(n)$ and $O_\alpha(n)$ are polynomially bounded, even though the topological entropy $h(\alpha) = h$ is positive. The following lemma shows that the usual function $\phi(|\tau|) = \frac{1}{e^{h|\tau|}}$ in Mertens' Theorem in (23) is not interesting when we have polynomially bounded growth.

Lemma 4.16. *If $O_\alpha(n) \leq C_{15} n^k$ for some k, C_{15}, and $h > 0$, then*

$$\sum_{|\tau| \leq N} \frac{1}{e^{h|\tau|}}$$

is bounded.

Proof.

$$\sum_{|\tau| \leq N} \frac{1}{e^{h|\tau|}} = \sum_{n \leq N} \frac{O_\alpha(n)}{e^{hn}} \leq C_{15} \sum_{n \leq N} \frac{n^k}{e^{hn}}$$

converges as $N \to \infty$. □

Example 4.17. In the same situation as Example 3.43(iv), that is if we take $\xi = 2$, $K = \mathbb{Q}$, $S = \{p \mid p \neq 3\}, S^c = \mathbb{P} \backslash S = \{3\}$, then $M_\alpha(N)$ is bounded.

Proof. From Example 3.43(iv), we know $F_\alpha(n) = |2^n - 1|_3^{-1}$ and $h(\alpha) = \log 2$. By Lemma 3.22, $F_\alpha(n)$ can be written as

$$F_\alpha(n) = \begin{cases} 1 & \text{if } n \text{ is odd} \\ 3|n|_3^{-1} & \text{if } n \text{ is even.} \end{cases}$$

Notice that for $n \in \mathbb{N}$,

$$F_\alpha(n) \leq 3n,$$

since $1 \leq |n|_3^{-1} \leq n$ for any natural number n. □

From now on, S^c is a finite set of primes and $|S^c| = m$. From the above example, changing S^c to be any finite subset of $\mathbb{P}$ and following the same method as the proof in the above example, we can see that $M_\alpha(N)$ is bounded. More generally, we will find a dynamical analogue of Mertens' Theorem concerning asymptotic estimates for expressions like

$$M_\alpha^\phi(N) = \sum_{|\tau| \leq N} \phi(\tau), \tag{40}$$

where $\phi = \frac{1}{(\log|\tau|)^{|S^c|}}$, a more appropriate rate function for these slowly growing systems. In orther words,

$$M_\alpha(N) := M_\alpha^\phi(N) = \sum_{n=2}^{N} \frac{O_\alpha(n)}{(\log n)^{|S^c|}}.$$

As usual,

$$F_\alpha(n) = \prod_{p \in S^c} |a^n - 1|_p^{-1}, \tag{41}$$

where $a \in \mathbb{Z}, |a| > 1, \gcd(a,p) = 1 \ \forall p \in S^c$. For the rest of this section, (X, α) is a dynamical system with the property (41). Our interest in this section will be specifically in case $a = 2$. These are examples of "co-finite" S-integer systems: in the notation of [8], these have S containing all but finitely many primes instead of only finitely many primes. Notice that the product formula for $\mathbb{Q}$ shows that if S, S^c are disjoint and $S \cup S^c$ consists of all the primes [37], then

$$\prod_{p \in S \cup \{\infty\}} |a^n - 1|_p \cdot \prod_{p \in S^c} |a^n - 1|_p = 1.$$

In this sense the co-finite systems are complementary to the finite ones considered in [8].

Lemma 4.18. *Let T be a finite subset of primes. For a given a positive integer n, if $o_T \mid n$, then we have*

$$|2^n - 1|_T = |n|_T \left| \frac{2^{o_T} - 1}{o_T} \right|_T,$$

where $o_T = \operatorname{lcm}\{m_p \mid p \in T\}$ and m_p is the multiplicative order of $2 \pmod p$.

Proof. Let $T \subset \mathbb{P}$ with $|T| < \infty$ and n be a positive integer. For each $p \in T$, by Lemma 3.22, we know that

$$|2^n - 1|_p = \begin{cases} |n|_p |2^{m_p} - 1|_p & \text{if } m_p \mid n, \\ 1 & \text{if } m_p \nmid n, \end{cases}$$

and also we get

$$|2^{o_T} - 1|_p = |o_T|_p |2^{m_p} - 1|_p, \tag{42}$$

as m_p always divides o_T.

Consequently,

$$|2^n - 1|_T = |n|_T \left| \frac{2^{o_T} - 1}{o_T} \right|_T.$$

□

By applying Lemma 4.18, we may write $F_\alpha(n)$ (in (41)) as in the following lemma.

Lemma 4.19.

$$F_\alpha(n) = |n|_{U(n)}^{-1} \left| \frac{2^{o_{U(n)}} - 1}{o_{U(n)}} \right|_{U(n)}^{-1},$$

where $U(n) = \{p \in S^c \ : \ m_p \mid n\}$ and $o_{U(n)} = \operatorname{lcm}\{m_p \ : \ p \in U(n)\}$.

Definition 4.20. The *dynamical Dirichlet series* associated to the map α is the formal series

$$d_\alpha(z) = \sum_{n=1}^{\infty} \frac{O_\alpha(n)}{n^z}. \tag{43}$$

Alternatively, $d_\alpha(z)$ can be expressed as

$$d_\alpha(z) = \frac{1}{\zeta(z+1)} \sum_{n=1}^{\infty} \frac{F_\alpha(n)/n}{n^z},$$

by using convolution of Dirichlet series (see [31, Section 3.7]). The dynamical Dirichlet series will play an important role in obtaining the formula for $O_\alpha(n)$ by extracting the coefficients from the series expression for d_α.

The following theorem taken from [9, Theorem 3.3] will be specifically illustrated here for a dynamical system (X, α) having the formula of $F_\alpha(n)$ as in (41).

For a set A, define

$$\mathbb{N}_0^A = \{f : A \to \mathbb{N}_0\}.$$

Theorem 4.21. *Let S^c be a finite subset of primes. Then $d_\alpha(z)$ is a finite linear combination of Dirichlet series of the form*

$$\sum_{\boldsymbol{e} \in \mathbb{N}_0^W} \frac{1}{(b\varphi_W(\boldsymbol{e}))^z} \tag{44}$$

where $b \in \mathbb{N},\ W \subseteq S^c$, and $\varphi_W(\boldsymbol{e}) = \prod_{p \in W} p^{e_p}$.

The (proof of the) above theorem allows us to derive the formula for $O_\alpha(n)$. We know that $d_\alpha(z)$ is the sum in (43) and may then use it to compare with the expression of $d_\alpha(z)$ in this theorem so that the sum in (44) contributes 1 orbit of length n when $n = b\prod_{p \in W} p^{e_p},\ e_p \geq 0$. This gives the following corollary.

Corollary 4.22. *If $d_\alpha(z)$ is expressed as in Theorem 4.21, then there is a finite list $W_1, W_2, \ldots, W_r$ of (not necessarily distinct) subsets of S^c and non-zero integer*

constants $R_1, R_2, \ldots, R_r$, $K_1, K_2, \ldots, K_r$ *such that*

$$O_\alpha(n) = \begin{cases} R_i & \text{if } n = K_i \prod_{p \in W_i} p^{e_p},\ e_p \in \mathbb{N}, \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, $W_i = S^c$ *for some* i.

Example 4.23. For $S^c = \{3\}$, we know that

$$F_\alpha(n) = |2^n - 1|_3^{-1}.$$

By Lemma 4.19, we can write

$$F_\alpha(n) = |n|_{U(n)}^{-1} \left| \frac{2^{o_{U(n)}} - 1}{o_{U(n)}} \right|_{U(n)}^{-1},$$

where $U(n) = \{p \in S^c \ : \ m_p \mid n\}$.

Note that $m_3 = 2$. For $n \geq 1$, if $U(n) = \emptyset$ (i.e. n is odd), then $F_\alpha(n) = 1$. On the other hand, if $U(n) \neq \emptyset$ then n can be written as $n = 2 \cdot 3^e k$ with $e \in \mathbb{N}_0$ and $3 \nmid k$. Thus we get

$$F_\alpha(n) = |2 \cdot 3^e \cdot k|_3^{-1} \left| \frac{2^2 - 1}{2} \right|_3^{-1} = 3^{e+1}.$$

Hence

$$F_\alpha(n) = \begin{cases} 3^{e+1} & \text{if } n = 2 \cdot k \cdot 3^e,\ e \geq 0 \text{ and } \ 3 \nmid k, \\ 1 & \text{otherwise.} \end{cases}$$

By [9, Example 4.1], we know that

$$d_\alpha(z) = 1 + \frac{1}{2^z} \left(\frac{1}{1 - 3^{-z}} \right). \tag{45}$$

Rearranging the terms on the right hand side of (45), the formula of $d_\alpha(z)$ becomes

$$d_\alpha(z) = 1 + \sum_{e=0}^{\infty} \frac{1}{(2 \cdot 3^e)^z},$$

and then we compare it with the equation (43).

Hence

$$O_\alpha(n) = \begin{cases} 1 & \text{if } n = 2 \cdot 3^e,\ e \geq 0 \text{ or } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Example 4.24. For $S^c = \{3, 5\}$, we know that

$$F_\alpha(n) = |2^n - 1|_3^{-1} |2^n - 1|_5^{-1}.$$

Note that $m_3 = 2,\ m_5 = 4$, and $o_{S^c} = 4$. For $n \geq 1$, there are three possibilities for $U(n)$.

Case 1. $U(n) = \{3\}$, then we write $n = 2.3^e k$ for all $e \in \mathbb{N}^0$ and $2 \nmid k,\ 3 \nmid k$. Following the same calculation as in Example 4.23, we reach $F_\alpha(n) = 3^{e+1}$.

Case 2. $U(n) = S^c$. Then we write $n = 4.k.3^{e_1}5^{e_2}$ where $e_1, e_2 \in \mathbb{N}_0$ and $3 \nmid k,\ 5 \nmid k$. Then

$$F_\alpha(n) = |4 \cdot k \cdot 3^{e_1}5^{e_2}|_{S^c}^{-1} \left| \frac{2^4 - 1}{4} \right|_{S^c}^{-1} = 3^{e_1+1}5^{e_2+1}.$$

Case 3. $U(n) = \emptyset$. Clearly, $F_\alpha(n) = 1$. Additionally, $U(n) = \emptyset$ means that n must not be written as in the cases 1 and 2. Thus

$$F_\alpha(n) = \begin{cases} 3^{e+1} & \text{if } \ n = 2 \cdot k \cdot 3^e,\ e \geq 0 \text{ and } \ 2 \nmid k, 3 \nmid k, \\ 3^{e_1+1}5^{e_2+1} & \text{if } \ n = 4 \cdot k \cdot 3^{e_1}5^{e_2},\ e_1, e_2 \geq 0 \text{ and } \ 3 \nmid k,\ 5 \nmid k, \\ 1 & \text{otherwise.} \end{cases}$$

By [9, Example 4.2], we know that

$$\begin{aligned} d_\alpha(z) &= 1 - \frac{1}{2^{z+1}} + \frac{3}{2^{z+1}} \left(1 - \frac{1}{3^{z+1}} - \frac{1}{2^{z+1}} + \frac{1}{6^{z+1}}\right) \frac{1}{1 - 3^{-z}} \\ &+ \frac{15}{4^{z+1}} \left(1 - \frac{1}{3^{z+1}} - \frac{1}{5^{z+1}} + \frac{1}{15^{z+1}}\right) \frac{1}{(1 - 3^{-z})(1 - 5^{-z})}. \end{aligned}$$

Rearranging the terms on the right hand side of the above equation, the formula of $d_\alpha(z)$ becomes

$$\begin{aligned} d_\alpha(z) &= 1 - \frac{1}{2^z} + \frac{3}{4^z} + \sum_{e=1}^{\infty} \frac{1}{(2\cdot 3^e)^z} + \sum_{e=1}^{\infty} \frac{2}{(4\cdot 3^e)^z} \\ &\quad + \sum_{e=1}^{\infty} \frac{3}{(4\cdot 5^e)^z} + \sum_{e_1=1}^{\infty} \frac{2}{(4\cdot 3^{e_1})^z} \sum_{e_2=1}^{\infty} \frac{1}{(5^{e_2})^z}, \end{aligned}$$

and then we compare it with the equation (43).

Hence

$$O_\alpha(n) = \begin{cases} 1 & \text{if } \ n = 2\cdot 3^e,\ e_1 \geq 0 \text{ or } n = 1, \\ 3 & \text{if } \ n = 4\cdot 5^{e_2},\ e_2 \geq 0 \\ 2 & \text{if } \ n = 12\cdot 3^{e_1}5^{e_2},\ e_1 \geq 0, e_2 \geq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Remark 4.25. Of course, it is easy to find a formula for $F_\alpha(n)$ given the formula for $O_\alpha(n)$ using (17); that is

$$F_\alpha(n) = \sum_{d|n} dO_\alpha(d).$$

The next lemmas are simple illustrations of the kind of calculation that will come later.

Lemma 4.26. *For $S^c = \{3\}$, we have*

$$\sum_{1<n\leq N} \frac{O_\alpha(n)}{\log n} = \frac{1}{\log 3}\log\log N + C_{16} + O((\log N)^{-1}),$$

for some constant C_{16}.

Proof. By Example 4.23, we have

$$O_\alpha(n) = \begin{cases} 1 & \text{if } n = 2\cdot 3^k,\ k \geq 0 \text{ or } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

From the formula for the number of orbits of length n under α, we obtain

$$\sum_{1<n\leq N}\frac{O_\alpha(n)}{\log n} = \sum_{0\leq k\leq\frac{\log\left(\frac{N}{2}\right)}{\log 3}}\frac{1}{\log 2\cdot 3^k} \tag{46}$$

$$= \frac{1}{\log 2}+\sum_{0<k\leq\frac{\log\left(\frac{N}{2}\right)}{\log 3}}\frac{1}{\log 2.3^k}. \tag{47}$$

Applying Lemma 1.20 to the summation in (47) with $a=0,\ b=\frac{\log\left(\frac{N}{2}\right)}{\log 3}$ and $f(t)=\frac{1}{\log 2+t\log 3}$, we get

$$\sum_{0<k\leq\frac{\log\left(\frac{N}{2}\right)}{\log 3}}\frac{1}{\log 2.3^k} = \int_0^{\frac{\log\left(\frac{N}{2}\right)}{\log 3}}\frac{1}{\log 2+t\log 3}\,dt \tag{48}$$

$$- \int_0^{\frac{\log\left(\frac{N}{2}\right)}{\log 3}}\frac{\{t\}\log 3}{(\log 2+t\log 3)^2}\,dt \tag{49}$$

$$- f\left(\frac{\log\left(\frac{N}{2}\right)}{\log 3}\right)\left\{\frac{\log\left(\frac{N}{2}\right)}{\log 3}\right\}. \tag{50}$$

Firstly, we calculate the main term of this summation (48) so we obtain

$$\int_0^{\frac{\log\left(\frac{N}{2}\right)}{\log 3}}\frac{1}{\log 2+t\log 3}\,dt=\frac{\log\log N}{\log 3}-\frac{\log\log 2}{\log 3}.$$

Secondly, we consider (49),

$$\left|\int_0^{\frac{\log\left(\frac{N}{2}\right)}{\log 3}}\frac{\{t\}\log 3}{(\log 2+t\log 3)^2}\,dt-\int_0^{\infty}\frac{\{t\}\log 3}{(\log 2+t\log 3)^2}\,dt\right|$$

$$\leq\int_{\frac{\log\left(\frac{N}{2}\right)}{\log 3}}^{\infty}\frac{\log 3}{(\log 2+t\log 3)^2}\,dt\leq(\log N)^{-1},$$

and we know that

$$\int_0^{\infty}\frac{\{t\}\log 3}{(\log 2+t\log 3)^2}\,dt=C_{17}$$

for some constant C_{17}.

Thus

$$\int_0^{\frac{\log\left(\frac{N}{2}\right)}{\log 3}} \frac{\{t\}\log 3}{(\log 2 + t\log 3)^2}\,dt = C_{17} + O((\log N)^{-1}).$$

Finally, for (50), it is easy to see that

$$f\left(\frac{\log\left(\frac{N}{2}\right)}{\log 3}\right)\left\{\frac{\log\left(\frac{N}{2}\right)}{\log 3}\right\} = O((\log N)^{-1}).$$

Hence

$$\begin{aligned}\sum_{1<n\le N}\frac{O_\alpha(n)}{\log n} &= \frac{1}{\log 2} + \frac{\log\log N}{\log 3} - \frac{\log\log 2}{\log 3} + C_{17} + O((\log N)^{-1}) \\ &= \frac{\log\log N}{\log 3} + C_{16} + O((\log N)^{-1}),\end{aligned}$$

as required. □

Lemma 4.27. *For $S^c = \{3,5\}$, we have*

$$\sum_{1<n\le N}\frac{O_\alpha(n)}{(\log n)^2} = \frac{2\log\log N}{\log 3\log 5} + C_{18} + O((\log N)^{-1})$$

for some constant C_{18}.

Proof. By Example 4.24, we may write

$$O_\alpha(n) = \begin{cases} 1 & \text{if } n = 1 \text{ or } n = 2, \\ 3 & \text{if } n = 4, \\ 1 & \text{if } n = 2\cdot 3^{e_1},\ e_1 > 0, \\ 2 & \text{if } n = 4\cdot 3^{e_1},\ e_1 > 0 \\ 3 & \text{if } n = 4\cdot 5^{e_2},\ e_2 > 0 \\ 2 & \text{if } n = 4\cdot 3^{e_1}5^{e_2},\ e_1 > 0, e_2 > 0, \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\sum_{1<n\leq N}\frac{O_\alpha(n)}{(\log n)^2} = \frac{1}{(\log 2)^2}+\frac{3}{(\log 4)^2} \tag{51}$$

$$+\sum_{0<e_1\leq\frac{\log\left(\frac{N}{2}\right)}{\log 3}}\frac{1}{\left(\log(2\cdot 3^{e_1})\right)^2} \tag{52}$$

$$+\sum_{0<e_1\leq\frac{\log\left(\frac{N}{4}\right)}{\log 3}}\frac{1}{\left(\log(4\cdot 3^{e_1})\right)^2} \tag{53}$$

$$+\sum_{0<e_2\leq\frac{\log\left(\frac{N}{4}\right)}{\log 5}}\frac{3}{\left(\log(4\cdot 5^{e_2})\right)^2} \tag{54}$$

$$+\sum_{\substack{4\cdot 3^{e_1}5^{e_2}\leq N,\\ e_1,e_2\in\mathbb{N}}}\frac{2}{\left(\log(4\cdot 3^{e_1}5^{e_2})\right)^2} \tag{55}$$

Applying Lemma 1.20 to the summation in (52) with $a=0,\ b=\frac{\log\left(\frac{N}{2}\right)}{\log 3}$ and $f(t)=\frac{1}{(\log 2+t\log 3)^2}$, we get

$$\sum_{0<e_1\leq\frac{\log\left(\frac{N}{2}\right)}{\log 3}}\frac{1}{\left(\log(2\cdot 3^{e_1})\right)^2} = \int_0^{\frac{\log\left(\frac{N}{2}\right)}{\log 3}}\frac{1}{\left(\log 2+t\log 3\right)^2}\,dt \tag{56}$$

$$-\int_0^{\frac{\log\left(\frac{N}{2}\right)}{\log 3}}\frac{2\{t\}\log 3}{\left(\log 2+t\log 3\right)^3}\,dt \tag{57}$$

$$-f\left(\frac{\log\left(\frac{N}{2}\right)}{\log 3}\right)\left\{\frac{\log\left(\frac{N}{2}\right)}{\log 3}\right\}. \tag{58}$$

Firstly, we calculate the main term which is on the right hand side of (56) so we obtain

$$\int_0^{\frac{\log\left(\frac{N}{2}\right)}{\log 3}}\frac{1}{\left(\log 2+t\log 3\right)^2}\,dt=-\frac{1}{\log 3\log N}+\frac{1}{\log 3\log 2}.$$

Secondly, we consider (57),

$$\left| \int_0^{\frac{\log\left(\frac{N}{2}\right)}{\log 3}} \frac{2\{t\}\log 3}{(\log 2 + t\log 3)^3}\, dt - \int_0^{\infty} \frac{2\{t\}\log 3}{(\log 2 + t\log 3)^3}\, dt \right|$$

$$\leq \int_{\frac{\log\left(\frac{N}{2}\right)}{\log 3}}^{\infty} \frac{2\log 3}{(\log 2 + t\log 3)^3}\, dt = (\log N)^{-2},$$

and we know that

$$\int_0^{\infty} \frac{\{t\}\log 3}{(\log 2 + t\log 3)^2}\, dt = C_{19},$$

for some constant C_{19}.

Thus

$$\int_0^{\frac{\log\left(\frac{N}{2}\right)}{\log 3}} \frac{\{t\}\log 3}{(\log 2 + t\log 3)^2}\, dt = C_{19} + O((\log N)^{-2}).$$

Finally, for (58), it is easy to see that

$$f\left(\frac{\log\left(\frac{N}{2}\right)}{\log 3}\right)\left\{\frac{\log\left(\frac{N}{2}\right)}{\log 3}\right\} = O((\log N)^{-2}).$$

Thus

$$\sum_{0<e_1\leq\frac{\log\left(\frac{N}{2}\right)}{\log 3}} \frac{1}{\left(\log(2\cdot 3^{e_1})\right)^2} = -\frac{1}{\log 3 \log N} + C_{20} + O((\log N)^{-2}),$$

for some constant C_{20}.

Similarly, we can get the sum (53) and (54) as follows:

$$\sum_{0<e_2\leq\frac{\log\left(\frac{N}{4}\right)}{\log 5}} \frac{3}{\left(\log(4\cdot 5^{e_2})\right)^2} = -\frac{3}{\log 5 \log N} + C_{21} + O((\log N)^{-2}),$$

and

$$\sum_{0<e_1\leq\frac{\log\left(\frac{N}{4}\right)}{\log 3}} \frac{2}{\left(\log(4\cdot 3^{e_1})\right)^2} = -\frac{2}{\log 3 \log N} + C_{22} + O((\log N)^{-2}),$$

for some constants $C_{21},\ C_{22}$.

Consider (55):

$$\sum_{\substack{4\cdot 3^{e_1}5^{e_2}\leq N,\\ e_1,e_2\in\mathbb{N}}}\frac{2}{\left(\log(4\cdot 3^{e_1}5^{e_2})\right)^2} = 2\sum_{e_1=1}^{\frac{\log\left(\frac{N}{4}\right)}{\log 3}}\sum_{e_2=1}^{\frac{\log\left(\frac{N}{4\cdot 3^{e_1}}\right)}{\log 5}}\frac{1}{\left(\log(4\cdot 3^{e_1})+e_2\log 5\right)^2} \tag{59}$$

$$= 2\sum_{e_1=1}^{\frac{\log\left(\frac{N}{4}\right)}{\log 3}}\left(\int_0^{\frac{\log\left(\frac{N}{4\cdot 3^{e_1}}\right)}{\log 5}}\frac{1}{\left(\log(4\cdot 3^{e_1})+t\log 5\right)^2}\,dt\right) \tag{60}$$

$$-2\sum_{e_1=1}^{\frac{\log\left(\frac{N}{4}\right)}{\log 3}}\left(\int_0^{\frac{\log\left(\frac{N}{4\cdot 3^{e_1}}\right)}{\log 5}}\frac{2\{t\}\log 5}{\left(\log(4\cdot 3^{e_1})+t\log 5\right)^3}\,dt\right) \tag{61}$$

$$-2\sum_{e_1=1}^{\frac{\log\left(\frac{N}{4}\right)}{\log 3}}\left(\frac{1}{(\log N)^2}\left\{\frac{\log\left(\frac{N}{4\cdot 3^{e_1}}\right)}{\log 5}\right\}\right). \tag{62}$$

The terms in (60), (61) and (62) come from applying Theorem 1.20 to the internal sum on the right hand side of (59) with $f(t)=\frac{1}{\left(\log(4\cdot 3^{e_1})+t\log 5\right)^2}$ and $a=0, b=\frac{\log\left(\frac{N}{4\cdot 3^{e_1}}\right)}{\log 5}$. We will first calculate the terms in (60) and then approximate the terms in (61) and (62) as follows:

For the sum in (60),

$$\sum_{e_1=1}^{\frac{\log\left(\frac{N}{4}\right)}{\log 3}}\left(\int_0^{\frac{\log\left(\frac{N}{4\cdot 3^{e_1}}\right)}{\log 5}}\frac{2}{\left(\log(4\cdot 3^{e_1})+t\log 5\right)^2}\,dt\right) = -\frac{2}{\log 5}\sum_{e_1=1}^{\frac{\log\left(\frac{N}{4}\right)}{\log 3}}\frac{1}{\log N} \tag{63}$$

$$+\frac{2}{\log 5}\sum_{e_1=1}^{\frac{\log\left(\frac{N}{4}\right)}{\log 3}}\frac{1}{\log(4\cdot 3^{e_1})} \tag{64}$$

$$= -\frac{2}{\log 3\log 5}+\frac{2\log 4}{\log 3\log 5\log N} \tag{65}$$

$$+\frac{2\log\log N}{\log 3\log 5}+C_{23}+O((\log N)^{-1}), \tag{66}$$

for some constant C_{23}, since the terms in (66) come from applying Theorem 1.20 to the sum in (64) with $f(t) = \frac{1}{\log(4\cdot 3^t)}$ and $a = 0, b = \frac{\log\left(\frac{N}{4}\right)}{\log 3}$.

Next, we consider (61),

$$\sum_{e_1=1}^{\frac{\log\left(\frac{N}{4}\right)}{\log 3}} \left(\int_0^{\frac{\log\left(\frac{N}{4\cdot 3^{e_1}}\right)}{\log 5}} \frac{4\{t\}\log 5}{\left(\log(4\cdot 3^{e_1}) + t\log 5\right)^3}\, dt \right) \leq +2 \sum_{e_1=1}^{\frac{\log\left(\frac{N}{4}\right)}{\log 3}} \frac{1}{\left((\log(4\cdot 3^{e_1})\right)^2} \tag{67}$$

$$-2 \sum_{e_1=1}^{\frac{\log\left(\frac{N}{4}\right)}{\log 3}} \frac{1}{(\log N)^2} \tag{68}$$

$$= -\frac{2}{\log 3 \log N} + C_{24} + O((\log N)^{-2}) \tag{69}$$

$$-\frac{2}{\log 3 \log N} + \frac{2\log 4}{\log 3 (\log N)^2}, \tag{70}$$

where C_{24} is a constant, and the terms in (69) come from applying Theorem 1.20 to the sum in (67) with $f(t) = \frac{1}{(\log(4\cdot 3^t))^2}$ and $a = 0, b = \frac{\log\left(\frac{N}{4}\right)}{\log 3}$.
Thus the sum in (61) is equal to $C_{25} + O((\log N)^{-1})$ for some constant C_{25}.

Lastly, for (62), it is easy to see that

$$2 \sum_{e_1=1}^{\frac{\log\left(\frac{N}{4}\right)}{\log 3}} \left(\frac{1}{(\log N)^2} \left\{ \frac{\log\left(\frac{N}{4\cdot 3^{e_1}}\right)}{\log 5} \right\} \right) = O((\log N)^{-1}).$$

Hence

$$\sum_{1<n\leq N} \frac{O_\alpha(n)}{(\log n)^2} = \frac{2\log\log N}{\log 3 \log 5} + C_{26} + O((\log N)^{-1}),$$

as required. □

Clearly, the constant terms C_{16} and C_{26} are very complicated even in these simple examples.

Before we go on to prove the main theorem below, we will define some notation in order to write things down more conveniently as follows:
For each $W \subseteq S^c$ (say $W = \{p_1, p_2, \ldots, p_k\}$ and $|W| = k$), we may write

$$n = K_W \cdot \prod_{p \in W} p^{e_p},$$

for some constant K_W and $e_p \geq 0$ for all $p \in W$, and we may write

$$\log n = \log K_W + \sum_{p \in W} e_p \log p.$$

For $\mathbf{e} \in \mathbb{N}_0^W$ (or $\mathbf{e} \in \mathbb{N}^W$), that is

$$\mathbf{e} = (e_p)_{p \in W} \quad \text{and} \quad e_p \in \mathbb{N}_0 \text{ (or } e_p \in \mathbb{N}),$$

we also write

$$\begin{aligned} \varphi_W(\mathbf{e}) &= \prod_{p \in W} p^{e_p}, \\ \psi_W(\mathbf{e}) &= \sum_{p \in W} e_p \log p. \end{aligned}$$

Lemma 4.28. *For $m \geq 1$, let W be a finite subset of primes such that $|W| \leq m$. Then*

$$\sum_{\substack{K\varphi_W(\boldsymbol{e}) \leq N, \\ \boldsymbol{e} \in \mathbb{N}^W}} \frac{1}{(\log N)^m} = O(1), \tag{71}$$

for any $K \geq 1$.

Proof. For $m \geq 1$ and $K \geq 1$, let W be a finite subset of primes such that $|W| \leq m$. Fix $N > 1$, we have

$$\sum_{\substack{K\varphi_W(\mathbf{e}) \leq N, \\ \mathbf{e} \in \mathbb{N}^W}} \frac{1}{(\log N)^m} = \big|\{\mathbf{e} \in \mathbb{N}^W \ : \ K\varphi_W(\mathbf{e}) \leq N\}\big| \times \frac{1}{(\log N)^m}.$$

If $W = \emptyset$, then (71) holds. For each $p \in W$, we have

$$p^{e_p} \leq N, \quad e_p > 0,$$

since

$$K\varphi_W(\mathbf{e}) \leq N.$$

Thus

$$e_p \leq \frac{\log N}{\log p}, \quad e_p > 0.$$

It follows that

$$\left|\{\mathbf{e} \in \mathbb{N}^W \ : \ K\varphi_W(\mathbf{e}) \leq N\}\right| \leq \prod_{p \in W} \frac{\log N}{\log p}.$$

Thus

$$\begin{aligned} \sum_{\substack{K\varphi_W(\mathbf{e}) \leq N, \\ \mathbf{e} \in \mathbb{N}^W}} \frac{1}{(\log N)^m} &\leq \left(\prod_{p \in W} \frac{\log N}{\log p} \right) \times \frac{1}{(\log N)^m} \\ &\leq \prod_{p \in W} \frac{1}{\log p} \\ &= O(1). \end{aligned}$$

Hence we finish this lemma. □

Lemma 4.29. *For $m \geq 1$, let W be a set of primes such that $|W| = k$ and $k < m$. Then*

$$\sum_{\boldsymbol{e} \in \mathbb{N}_0^W} \frac{1}{(z + \psi_W(\boldsymbol{e}))^m} = O(1), \tag{72}$$

for any $z \geq 0$.

Proof. We want to show this lemma by double induction on k and m such that $k < m$. If $k = 0$ and $m = 1$, it is easy to see that (72) holds for any $z \geq 0$. Assume that

for any set of primes U of cardinality less than k, the equation in (72) holds for any $z \geq 0$, and also assume that for any set of primes V of cardinality less than $m-1$,

$$\sum_{\mathbf{e} \in \mathbb{N}_0^V} \frac{1}{(z+\psi_V(\mathbf{e}))^{m-1}} = O(1), \tag{73}$$

for any $z \geq 0$.

We claim that for any set W such that $|W| = k < m$, equation (72) is true for any $z \geq 0$. For $z \geq 0$, let $W = \{p_1, p_2, \ldots, p_k\})$ such that $|W| = k < m$ and let $U = W \setminus \{p_k\}$.

We note that

$$\sum_{\mathbf{e} \in \mathbb{N}_0^U} \left(\frac{1}{(z+\psi_U(\mathbf{e}))^m} \right) = O(1),$$

by using the inductive hypothesis on k for $|U| = k-1 < k$, and

$$\frac{1}{(m-1)\log p_k} \sum_{\mathbf{e} \in \mathbb{N}_0^U} \frac{1}{(z+\psi_U(\mathbf{e}))^{m-1}} = O(1),$$

by using the inductive hypothesis on m for $|U| = k-1 < m-1$.

It follows that

$$\begin{aligned}
\sum_{\mathbf{e} \in \mathbb{N}_0^U} \left(\sum_{e_{p_k}=0}^{\infty} \frac{1}{(z+\psi_W(\mathbf{e}))^m} \right) &\leq \sum_{\mathbf{e} \in \mathbb{N}_0^U} \left(\frac{1}{(z+\psi_U(\mathbf{e}))^m} + \int_0^{\infty} \frac{1}{(z+\psi_W(\mathbf{e}))^m} de_{p_k} \right) \\
&= \sum_{\mathbf{e} \in \mathbb{N}_0^U} \left(\frac{1}{(z+\psi_U(\mathbf{e}))^m} \right. \\
&\qquad \left. + \frac{1}{(m-1)\log p_k (z+\psi_U(\mathbf{e}))^{m-1}} \right) \\
&= \sum_{\mathbf{e} \in \mathbb{N}_0^U} \frac{1}{(z+\psi_U(\mathbf{e}))^m} \\
&\qquad + \frac{1}{(m-1)\log p_k} \sum_{\mathbf{e} \in \mathbb{N}_0^U} \frac{1}{(z+\psi_U(\mathbf{e}))^{m-1}} \\
&= O(1).
\end{aligned}$$

□

Lemma 4.30. *For any $z \geq 1$,*

$$\sum_{\substack{z\varphi_{S^c}(\boldsymbol{e})\leq N \\ \boldsymbol{e}\in\mathbb{N}^{S^c}}} \frac{1}{(\log(z\varphi_{S^c}(\boldsymbol{e})))^m} = \frac{\log\log N}{(m-1)!\log p_1\cdots\log p_m} + O(1). \tag{74}$$

Proof. We will prove this lemma by induction on m (recall $S^c = \{p_1, p_1, \ldots, p_m\}$ and $|S^c| = m$). For $z \geq 1$, following Lemma 4.26, it is obviously that (74) is true for the case $m = 1$. Suppose that (74) holds for any finite set of primes having cardinality less than m. Let $U = S^c \setminus \{p_m\}$ and $|U| = m - 1$.

Consider

$$\sum_{\substack{z\varphi_{S^c}(\mathbf{e})\leq N, \\ \mathbf{e}\in\mathbb{N}^{S^c}}} \frac{1}{(\log(z\varphi_{S^c}(\mathbf{e})))^m} = \sum_{\substack{z\varphi_U(\mathbf{e})\leq N \\ \mathbf{e}\in\mathbb{N}^U}} \sum_{e_{p_m}=1}^{D(\mathbf{e}_U)} \frac{1}{(\log(z\varphi_{S^c}(\mathbf{e})))^m} \tag{75}$$

$$= \sum_{\substack{z\varphi_U(\mathbf{e})\leq N \\ \mathbf{e}\in\mathbb{N}^U}} \left(\int_0^{D(\mathbf{e}_U)} \frac{1}{(\log(z\varphi_{S^c}(\mathbf{e})))^m} de_{p_m} \right) \tag{76}$$

$$- m\log p_m \sum_{\substack{z\varphi_U(\mathbf{e})\leq N \\ \mathbf{e}\in\mathbb{N}^U}} \left(\int_0^{D(\mathbf{e}_U)} \frac{\{e_m\}}{(\log(z\varphi_{S^c}(\mathbf{e})))^{m+1}} de_{p_m} \right) \tag{77}$$

$$+ \sum_{\substack{z\varphi_U(\mathbf{e})\leq N \\ \mathbf{e}\in\mathbb{N}^U}} \left\{ \frac{\log\left(\frac{N}{z\varphi_U(\mathbf{e})}\right)}{\log p_m} \right\} \frac{1}{(\log N)^m}, \tag{78}$$

where $D(\mathbf{e}_U) = \frac{\log\left(\frac{N}{z\varphi_U(\mathbf{e})}\right)}{\log p_m}$. The equations in (76), (77) and (78) come from applying Theorem 1.20 to the internal sum on the right hand side of (75) with $f(t) = \frac{1}{(\log(z\varphi_{S^c}(\mathbf{e})))^m}$ and $a = 0, b = D(\mathbf{e}_U)$. We will approximate the terms in (76), (77) and (78). The inductive hypothesis will play a central role for calculating the main term in (76), while Lemma 4.29 and Lemma 4.28 will be used for estimating the error terms (77) and (78) as shown below.

Firstly, for (76), we have

$$\begin{aligned}\sum_{\substack{z\varphi_U(\mathbf{e})\le N,\\ \mathbf{e}\in\mathbb{N}^U}}\left(\int_0^{D(\mathbf{e}_U)}\frac{1}{(\log z+\psi_{S'}(\mathbf{e}))^m}de_m\right)&=\frac{1}{(m-1)\log p_m}\sum_{\substack{z\varphi_U(\mathbf{e})\le N,\\ \mathbf{e}\in\mathbb{N}^U}}\frac{1}{(\log z+\psi_U(\mathbf{e}))^{m-1}}\\&\quad-\frac{1}{(m-1)\log p_m}\sum_{\substack{z\varphi_U(\mathbf{e})\le N,\\ \mathbf{e}\in\mathbb{N}^U}}\frac{1}{(\log N)^{m-1}}\\&=\frac{1}{(m-1)\log p_m}\sum_{\substack{z\varphi_U(\mathbf{e})\le N,\\ \mathbf{e}\in\mathbb{N}^U}}\frac{1}{(\log z+\psi_U(\mathbf{e}))^{m-1}}\\&\quad+O(1)\quad\text{(by Lemma 4.28)}\\&=\frac{1}{(m-1)!\log p_m\cdots\log p_1}\log\log N+O(1),\end{aligned}$$

by the inductive hypothesis.

Secondly, we consider (77),

$$\begin{aligned}&m\log p_m\sum_{\substack{z\varphi_U(\mathbf{e})\le N,\\ \mathbf{e}\in\mathbb{N}^U}}\left(\int_0^{D(\mathbf{e}_U)}\frac{\{e_m\}}{(\log(z\varphi_{S^c}(\mathbf{e})))^{m+1}}de_{p_m}\right)\\&\le m\log p_m\sum_{\substack{z\varphi_U(\mathbf{e})\le N,\\ \mathbf{e}\in\mathbb{N}^U}}\left(\int_0^{D(\mathbf{e}_U)}\frac{1}{(\log(z\varphi_{S^c}(\mathbf{e})))^{m+1}}de_{p_m}\right)\\&=\sum_{\substack{z\varphi_U(\mathbf{e})\le N,\\ \mathbf{e}\in\mathbb{N}^U}}\frac{1}{(\log(z\varphi_{S^c}(\mathbf{e})))^m}-\sum_{\substack{z\varphi_U(\mathbf{e})\le N,\\ \mathbf{e}\in\mathbb{N}^U}}\frac{1}{(\log N)^m}=O(1),\end{aligned}$$

by Lemma 4.29 and Lemma 4.28.

Thus the term in (77) is equal to $O(1)$.

Finally, for (78) we obtain

$$\begin{aligned}\sum_{\substack{z\varphi_U(\mathbf{e})\le N,\\ \mathbf{e}\in\mathbb{N}^U}}\left\{\frac{\log\left(\frac{N}{z\varphi_U(\mathbf{e})}\right)}{\log p_m}\right\}\frac{1}{(\log N)^m}&\le\sum_{\substack{z\varphi_U(\mathbf{e})\le N,\\ \mathbf{e}\in\mathbb{N}^U}}\frac{1}{(\log N)^m}\\&=O(1),\end{aligned}$$

by Lemma 4.28.

Hence this lemma is completed. □

Here we will show the main theorem which is the general case of Lemma 4.26 and Lemma 4.27.

Theorem 4.31. *There exists a constant C_{S^c} depending on the set S^c such that*

$$\sum_{1<n\leq N} \frac{O_\alpha(n)}{(\log n)^{|S^c|}} = C_{S^c} \log\log N + O(1). \tag{79}$$

Proof. For $n > 1$, let W be a subset of S^c and let K_W be a constant depending on W. If $W \subset S^c$ ($W \neq S^c$), applying Lemma 4.29, we get

$$\sum_{\substack{K_W \varphi_W(\mathbf{e})\leq N \\ \mathbf{e}\in\mathbb{N}^W}} \frac{1}{(\log(K_W\varphi_W(\mathbf{e})))^m} = O(1), \tag{80}$$

since $\log K_W \geq 0$.

Since $K_{S^c} \geq 1$, by Lemma 4.30, we get

$$\sum_{\substack{K_{S^c}\varphi_{S^c}(\mathbf{e})\leq N \\ \mathbf{e}\in\mathbb{N}^{S^c}}} \frac{1}{(\log(K_{S^c}\varphi_{S^c}(\mathbf{e})))^m} = \frac{\log\log N}{(m-1)!\log p_1 \cdots \log p_m} + O(1). \tag{81}$$

By Corollary 4.22, $M_\alpha(N)$ may be written as

$$\sum_{1<n\leq N} \frac{O_\alpha(n)}{(\log n)^{|S^c|}} = \sum_{i=1}^{r} \sum_{\substack{n=K_{W_i}\varphi_{W_i}(\mathbf{e})\leq N, \\ \mathbf{e}\in\mathbb{N}^{W_i}}} \frac{R_{W_i}}{(\log n)^m} + \sum_{\substack{n=K_{S^c}\varphi_{S^c}(\mathbf{e})\leq N, \\ \mathbf{e}\in\mathbb{N}^{S^c}}} \frac{R_{S^c}}{(\log n)^m}, \tag{82}$$

where r is a positive integer, and R_{W_i} and R_{S^c} are constants depending on W_i and S^c, respectively.

Applying (80) and (81) to (82), we deduce that

$$\sum_{1<n\leq N} \frac{O_\alpha(n)}{(\log n)^{|S^c|}} = C_{S^c} \log\log N + O(1),$$

for some constant C_{S^c}. □

Chapter 5

Intermediate Growth Examples

In Chapters 3 and 4, we saw some properties of a family of dynamical systems parametrized by sets of primes in two special cases: a finite set of primes, and a co-finite set of primes. In this chapter we find some examples of the (huge) "intermediate" case – where the set of primes is infinite and has an infinite complement. In this setting little is known apart from some crude estimates for a "typical" set of primes (see [35] and [36]). Throughout this chapter, S is a subset of the set of prime numbers $\mathbb{P}$, and $S^c = \mathbb{P} \setminus S$. Also, p always means an element in $\mathbb{P}$.

5.1 Density of Prime Numbers

The notion of density of S will be given in this section. In particular, we will focus on the natural density of S in order to measure the size of S compared with the set of all prime numbers.

Definition 5.1. Define the *natural density* of $S \subseteq \mathbb{P}$ to be

$$\delta(S) = \lim_{x \to \infty} \frac{|\{p \leq x \mid p \in S\}|}{|\{p \leq x \mid p \in \mathbb{P}\}|},$$

if it exists. In other words, the natural density of S is the proportion of primes in S.

Example 5.2. Let S^1, S^2 be the set all the primes congruent to 1 modulo 4 and the set all the primes congruent to 3 modulo 4, respectively. So

$$\begin{aligned} S^1 &= \{5, 13, 17, 29, 37, 41, 53, 61, 73, \dots\} \\ S^2 &= \{3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, \dots\}. \end{aligned}$$

By Dirichlet's Theorem [10, Theorem 10.5], S^1 and S^2 are infinite, and each has density $\frac{1}{2}$.

Let m be an integer which is not a perfect square and not -1. Write $m = ab^2$ with a square-free. Let $S(m)$ be the set of prime numbers p such that m is a primitive root modulo p. In 1927, Emil Artin conjectured the following statements.

1. $S(m)$ has a positive natural density. In particular, $S(m)$ is infinite.

2. Under the conditions that m is not a perfect power and that a is not congruent to 1 modulo 4, this density is independent of m and equals Artin's constant which can be expressed as an infinite product

$$C_{\text{Artin}} = \prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right) = 0.3739558136\dots$$

In 1967, Hooley [19] proved the conjecture assuming certain cases of the Generalised Riemann Hypothesis: if Artin's conjecture is false, then the Generalised Riemann Hypothesis is false. In 1984, R. Gupta and M. Ram Murty [13] showed unconditionally that Artin's conjecture holds for almost all m using sieve methods. In 1985,

Heath-Brown [17] demonstrated that there are at most two primes for which Artin's conjecture fails (i.e $S(m)$ is finite for at most two exceptional prime numbers m). For example, his work implies that at least one of 3, 5, and 7 is a primitive root modulo p for infinitely many p.

For a prime p, let $m_p := m_p(2)$, the multiplicative order of 2 $\pmod p$.

Example 5.3. Let

$$\begin{aligned} S_2 &= \{p : p \text{ is a prime and } m_p \text{ is even}\} \\ &= \{3, 5, 11, 13, 17, 19, 29, 37, 41, 43, 53, 59, 61, 67, 83, 97, 101, 113, \dots\}. \end{aligned}$$

Its density is 17/24 by [21, Theorem A].

Example 5.4. Let

$$\begin{aligned} S(2) &= \{3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, 139, 149, 163, 173, \dots\} \\ &= \{p \mid m_p = p - 1\} \end{aligned}$$

In other words, $S(2)$ is the set of primes p for which 2 is a primitive root modulo p. It has 38 elements smaller than 500 and there are 95 primes smaller than 500. The ratio (which conjecturally tends to C_{Artin}) is $38/95 = 0.41051\dots$. In addition, we notice that every element in $S(2)$ lies in S_2 and S_2 is strictly bigger than $S(2)$ because 17 is in S_2, but not in $S(2)$. Thus the density of $S(2)$ (if it exists) is not more than 17/24.

5.2 An Arithmetic Argument

A totally multiplicative function is a function $f : \mathbb{N} \to \mathbb{C}$ with the property that

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

for all integers m, n. The following lemmas and proposition, taken from [8] in the case $\mathbb{K} = \mathbb{Q}$, will play a crucial role in calculating the constant arising in Mertens' Theorem.

In order to understand how to get the following lemmas, we shall recall a fact from combinatorial mathematics, *the inclusion-exclusion principle*. Its statement is that if $A_1, A_2, \ldots, A_n$ are finite sets, then

$$\begin{aligned} |\cup_{i=1}^{n} A_i| &= \sum_{i=1}^{n} |A_i| - \sum_{\substack{i,j \\ 1 \le i < j \le n}} |A_i \cap A_j| \\ &+ \sum_{\substack{i,j,k \\ 1 \le i < j < k \le n}} |A_i \cap A_j \cap A_k| + \cdots + (-1)^{n-1} |A_1 \cap \cdots \cap A_n|, \end{aligned}$$

where $|A|$ denotes the cardinality of the set A.

Lemma 5.5. *Let $f : \mathbb{N} \to \mathbb{C}$ and let E be a finite set of natural numbers. Then*

$$\sum_{\substack{n \le N, \\ k \nmid n \forall k \in E}} f(n) = \sum_{D \subseteq E} (-1)^{|D|} \sum_{\substack{n \le N, \\ n_D \mid n}} f(n),$$

where $n_D = \operatorname{lcm}\{n : n \in D\}$.

Proof. The proof is completed by applying the inclusion-exclusion principle. □

Lemma 5.6. *Let $f : \mathbb{N} \to \mathbb{C}$ be a totally multiplicative function with*

$$\sum_{n \le N} f(n) = k_f \log N + C_f + O(1/N),$$

for constants C_f and k_f. Let E be a finite set of natural numbers and, for $D \subseteq E$, let $n_D = \operatorname{lcm}\{n : n \in D\}$. Then

$$\sum_{\substack{n \le N, \\ k \nmid n \forall k \in E}} f(n) = k_{f,E} \log N + C_{f,E} + O(1/N),$$

where

$$k_{f,E} = k_f \sum_{D \subseteq E} (-1)^{|D|} f(n_D),$$

and

$$C_{f,E} = \sum_{D \subseteq E} (-1)^{|D|} \left(C_f - k_f \log(n_D)\right) f(n_D).$$

Proof. From Lemma 5.5, we have

$$\sum_{\substack{n \leq N, \\ k \nmid n \forall k \in E}} f(n) = \sum_{D \subseteq E} (-1)^{|D|} \sum_{\substack{n \leq N, \\ n_D \mid n}} f(n).$$

For each $D \subseteq E$, we get

$$\begin{aligned}
\sum_{\substack{n \leq N, \\ n_D \mid n}} f(n) &= f(n_D) \sum_{n \leq N/n_D} f(n) \quad \text{as } f \text{ is a totally multiplicative function,} \\
&= f(n_D) \left[k_f \log(N/n_D) + C_f + O(1/N)\right], \\
&= k_f f(n_D) \log N + C_{f,n_D} + O(1/N),
\end{aligned}$$

where $C_{f,n_D} = \left(C_f - k_f \log(n_D)\right) f(n_D)$.

Hence

$$\begin{aligned}
\sum_{\substack{n \leq N, \\ k \nmid n \forall k \in E}} f(n) &= \sum_{D \subseteq E} (-1)^{|D|} \left[k_f f(n_D) \log N + C_{f,n_D} + O(1/N)\right] \\
&= \left[k_f \sum_{D \subseteq E} (-1)^{|D|} f(n_D)\right] \log N + C_{f,E} + O(1/N),
\end{aligned}$$

where $C_{f,E} = \sum_{D \subseteq E} (-1)^{|D|} \left(C_f - k_f \log(n_D)\right) f(n_D)$.
Note that the error remains $O(1/N)$ since the sum is finite. □

For any finite subset T of rational primes, we write $|x|_T$ for $\prod_{p \in T} |x|_p$ and put

$$f_T(n) = \frac{|n|_T}{n}.$$

Then $f_T(n)$ is a totally multiplicative function.

Proposition 5.7.

$$\sum_{n\le N} f_T(n) = k_T \log N + C_T + O(1/N), \tag{83}$$

where

$$k_T = \prod_{p\in T} \frac{p}{p+1} \quad \textit{and} \quad C_T = k_T \left(\gamma - \sum_{p\in T} \frac{p\log p}{p^2-1}\right).$$

Proof. We will prove this by induction on $m = |T|$. If $m = 0$, then we get the familiar statement

$$\sum_{n\le N} \frac{1}{n} = \log N + \gamma + O(1/N),$$

where γ is the Euler-Mascheroni constant. We first assume that (83) holds for any positive integer less than m. Then we will show that (83) is true for m. Putting $T = \{p_1, \ldots, p_m\}$ and $T_1 = T \setminus \{p_1\}$. Write $n = p_1^e k$ such that $\gcd(p_1, k) = 1$. So $\mathrm{ord}_{p_1}(n) = e$. We observe that

$$\begin{aligned} f_T(n) &= \frac{|p_1^e k|_{p_1} |p_1^e k|_{T_1}}{p_1^e k} \\ &= \frac{1}{p_1^{2e}} f_{T_1}(n). \end{aligned}$$

Then

$$\sum_{n\le N} f_T(n) = \sum_{e=0}^{\lfloor \frac{\log N}{\log p_1} \rfloor} \sum_{\substack{n\le N,\\ \mathrm{ord}_{p_1}(n)=e}} f_T(n) \tag{84}$$

$$= \sum_{e=0}^{\lfloor \frac{\log N}{\log p_1} \rfloor} \frac{1}{p_1^{2e}} \sum_{\substack{n<N/p_1^e,\\ p_1\nmid n}} f_{T_1}(n), \tag{85}$$

We have

$$\sum_{n\le N} f_{T_1}(n) = k_{T_1} \log N + C_{T_1} + O(1/N),$$

where

$$k_{T_1} := k_{f_{T_1}} = \prod_{p\in T_1} \frac{p}{p+1} \quad \text{and} \quad C_{T_1} := C_{f_{T_1}} = k_{T_1} \left(\gamma - \sum_{p\in T_1} \frac{p\log p}{p^2-1}\right),$$

by using the inductive hypothesis.

Applying Lemma 5.6 to the sum $\sum_{n\le N} f_{T_1}(n)$ (that is, with $f = f_{T_1}$ and $E = \{p_1\}$), we get

$$\sum_{\substack{n\le N\\ p_1\nmid n}} f_{T_1}(n) = k_{T_1,E}\log N + C_{T_1,E} + O(1/N),$$

where

$$\begin{aligned} k_{T_1,E} &:= k_{f_{T_1},E} \\ &= k_{T_1}\sum_{D\subseteq E}(-1)^{|D|} f_{T_1}(n_D) \\ &= \left(1-\frac{1}{p_1}\right)k_{T_1}, \end{aligned}$$

and

$$\begin{aligned} C_{T_1,E} &:= C_{f_{T_1},E} \\ &= \sum_{D\subseteq E}(-1)^{|D|}\left(C_{T_1} - k_{T_1}\log(n_D)\right) f_{T_1}(n_D) \\ &= C_{T_1}\left(1-\frac{1}{p_1}\right) + \frac{1}{p_1}k_{T_1}\log p_1 \\ &= k_{T_1}\left(1-\frac{1}{p_1}\right)\gamma - k_{T_1}\left(1-\frac{1}{p_1}\right)\sum_{p\in T_1}\frac{p\log p}{p^2-1} + \frac{1}{p_1}k_{T_1}\log p_1. \end{aligned}$$

Thus

$$\sum_{\substack{n<N/p_1^e\\ p_1\nmid n}} f_{T_1}(n) = k_{T_1,E}\log N - k_{T_1,E}e\log p_1 + C_{T_1,E} + O(p_1^e/N). \tag{86}$$

Substituting (86) into (85), we have

$$\begin{aligned} \sum_{n\le N} f_T(n) &= k_{T_1,E}\log N \sum_{e=0}^{\lfloor \frac{\log N}{\log p_1}\rfloor}\frac{1}{p_1^{2e}} - k_{T_1,E}\log p_1 \sum_{e=0}^{\lfloor \frac{\log N}{\log p_1}\rfloor}\frac{e}{p_1^{2e}} \\ &\quad + C_{T_1,E}\sum_{e=0}^{\lfloor \frac{\log N}{\log p_1}\rfloor}\frac{1}{p_1^{2e}} + \sum_{e=0}^{\lfloor \frac{\log N}{\log p_1}\rfloor}\frac{O(p_1^e/N)}{p_1^{2e}}. \end{aligned}$$

$$\begin{aligned}\left|\sum_{n\le N} f_T(n) - k_T \log N - C_T\right| &= \left|k_{T_1,E}\log N \sum_{e=\lfloor\frac{\log N}{\log p_1}\rfloor+1}^{\infty}\frac{1}{p_1^{2e}}\right| + \left|k_{T_1,E}\log p_1 \sum_{e=\lfloor\frac{\log N}{\log p_1}\rfloor+1}^{\infty}\frac{e}{p_1^{2e}}\right| \\ &\quad + \left|C_{T_1,E}\sum_{e=\lfloor\frac{\log N}{\log p_1}\rfloor+1}^{\infty}\frac{1}{p_1^{2e}}\right| + \sum_{e=0}^{\lfloor\frac{\log N}{\log p_1}\rfloor}\frac{O(p_1^e/N)}{p_1^{2e}} \\ &\le \frac{C_{28}}{N},\end{aligned}$$

for some constant C_{28}.

Here, the inductive hypothesis will be applied in order to get k_T and C_T as follows:

$$\begin{aligned}k_T &= k_{T_1,E}\sum_{e=0}^{\infty}\frac{1}{p_1^{2e}} \\ &= \sum_{e=0}^{\infty}\frac{1}{p_1^{2e}}(1-\frac{1}{p_1})k_{T_1} \\ &= \prod_{p\in T}\frac{p}{p+1},\end{aligned}$$

and

$$\begin{aligned}C_T &= -k_{T_1,E}\log p_1\sum_{e=0}^{\infty}\frac{e}{p_1^{2e}} + C_{T_1,E}\sum_{e=0}^{\infty}\frac{1}{p_1^{2e}} \\ &= -\left(\frac{p_1-1}{p_1}\right)\left(\frac{p_1^2}{(p_1^2-1)^2}\right)k_{T_1}\log p_1 + k_{T_1}\gamma\left(\frac{p_1-1}{p_1}\right)\left(\frac{p_1^2}{p_1^2-1}\right) \\ &\quad -k_{T_1}\left(\frac{p_1-1}{p_1}\right)\left(\frac{p_1^2}{p_1^2-1}\right)\sum_{p\in T_1}\frac{p\log p}{p^2-1} + k_{T_1}\frac{1}{p_1}\left(\frac{p_1^2}{p_1^2-1}\right)\log p_1 \\ &= k_T\frac{p_1}{p_1^2-1}\log p_1 + \gamma k_T + k_T\sum_{p\in T_1}\frac{p\log p}{p^2-1} \\ &= k_T\left(\gamma - \sum_{p\in T}\frac{p\log p}{p^2-1}\right).\end{aligned}$$

Hence we finish this proposition. □

5.3 Finite Sets of Primes

In a paper of Everest, Miles, Stevens, and Ward [8], a dynamical analogue of Mertens' Theorem concerns the expressions like

$$M_\alpha(N) = \sum_{|\tau| \leq N} \phi(|\tau|),$$

where ϕ is some positive function of $|\tau|$ and it has been studied for an ergodic S-integer map α with $|S| < \infty$. They considered $\mathbb{K}$ a number field (as well as $\mathbb{Q}$) and in particular they also have shown the recipe to compute the leading coefficient appearing in Theorem 1.4 of [8] when $\mathbb{K}$ is a field of rational numbers (in principle). Such coefficients may be found explicitly for any finite set S and fixed map α and indeed, they are always rational.

The main goal of this chapter is to find out the leading coefficient for some examples with $|S| = \infty$ and $|S^c| = \infty$ under the same setting as above. Before working out on this purpose, in this section, we shall understand how to get the leading coefficient for $|S| < \infty$ from [8] firstly.

In this setting (that is, for the maps α given by $\zeta = 2$ and $\mathbb{K} = \mathbb{Q}$), we recall that

$$F_\alpha(n) = |2^n - 1| \, |2^n - 1|_S \, .$$

Then consider

$$\begin{aligned} M_\alpha(N) &= \sum_{n \leq N} \frac{1}{n2^n} \sum_{d|n} \mu\left(\frac{n}{d}\right) \left|2^d - 1\right| \left|2^d - 1\right|_S \\ &= \sum_{n \leq N} \frac{(2^n - 1) \, |2^n - 1|_S}{n2^n} + \sum_{n \leq N} \frac{1}{n2^n} \sum_{d|n, d<n} \mu\left(\frac{n}{d}\right) (2^d - 1) \left|2^d - 1\right|_S \\ &= \underbrace{\sum_{n \leq N} \frac{|2^n - 1|_S}{n}}_{F(N)} + R(N), \end{aligned}$$

where

$$R(N) = \sum_{n \le N} \frac{|2^n - 1|_S}{n2^n} + \sum_{n \le N} \frac{1}{n2^n} \sum_{d|n, d<n} \mu\left(\frac{n}{d}\right) (2^d - 1) \left|2^d - 1\right|_S .$$

Lemma 5.8. *For any S,*

$$R(N) = C(S) + O(2^{-\frac{N}{2}}),$$

where $|C(S)| \le 5$.

Proof. We first observe that

$$\sum_{n=1}^{\infty} \frac{|2^n - 1|_S}{n2^n},$$

and

$$\sum_{n=1}^{\infty} \frac{1}{n2^n} \sum_{d|n, d<n} \mu\left(\frac{n}{d}\right) (2^d - 1) \left|2^d - 1\right|_S$$

are bounded by the sums $\sum_{n=1}^{\infty} \frac{1}{2^n}$ and $\sum_{n=1}^{\infty} \frac{1}{2^{n/2}}$, respectively, so they are convergent. Recall that

$$\sum_{n=1}^{\infty} \frac{1}{2^n} = 1, \tag{87}$$

and

$$\sum_{n=1}^{\infty} \frac{1}{2^{n/2}} = \frac{\sqrt{2}}{\sqrt{2} - 1}. \tag{88}$$

Consequently,

$$\sum_{n=1}^{\infty} \frac{|2^n - 1|_S}{n2^n} = C_1(S) \le 1$$

and

$$\sum_{n=1}^{\infty} \frac{1}{n2^n} \sum_{d|n, d<n} \mu\left(\frac{n}{d}\right) (2^d - 1) \left|2^d - 1\right|_S = C_2(S) \le 4,$$

where $C_1(S)$ and $C_2(S)$ are constants depending on S.

Then by (87) and (88), we have $|C_1(S) + C_2(S)| \le 5$.

Next, we consider

$$\left|R(N)-\sum_{n=1}^{\infty}\frac{|2^n-1|_S}{2^n}-\sum_{n=1}^{\infty}\frac{1}{n2^n}\sum_{d|n,d<n}\mu\Big(\frac{n}{d}\Big)(2^d-1)\left|2^d-1\right|_S\right| \leq \sum_{n=N+1}^{\infty}\frac{1}{2^n}+\sum_{n=N+1}^{\infty}\frac{1}{2^{n/2}}$$
$$\leq \frac{\sqrt{2}}{\sqrt{2}-1}2^{-N/2}.$$

Thus

$$R(N)-C_1(S)-C_2(S)=O(2^{-N/2}).$$

Hence

$$R(N)=C(S)+O(2^{-N/2}),$$

where $C(S)=C_1(S)+C_2(S)$. □

This lemma leads us to view the first term $F(N)$ as the main term and $R(N)$ as an error term. Consequently, we will need to focus on only the main term in order to get the leading coefficients. From Proposition 5.3 in [8], for $\mathbb{K}=\mathbb{Q}$ and $|S|<\infty$, $F(N)$ can be written as

$$\sum_{n\leq N}\frac{|2^n-1|_S}{n}=\sum_{T\subseteq S}\sum_{\substack{n\leq N,\ o_T|n\\ m_p\nmid n\forall p\notin T}}\frac{|2^n-1|_T}{n}, \tag{89}$$

where m_p is the multiplicative order of 2 modulo p and $o_T=\operatorname{lcm}\{m_p : p\in T\}$.
To work out on the internal sum on the right hand side in (89), we need to recall Lemma 3.22 and from here on, we will specifically need the formula for $|2^n-1|_p$ for any odd prime number p.

We observe that for each $T\subseteq S$, if $|S|$ is large, then the calculation becomes much more complicated and also we have to spend a long time to complete it. Thus, we try to find another formula for (89) so that the leading coefficients can be computed more easily and more quickly. However, we will still follow the recipe in [8]. The idea

comes from adding a new prime to S_{k-1} (say $S_k = \{p_1, \ldots, p_k\}, k > 0$ and $S_0 = \emptyset$) and then writing the sum $\sum_{n=1}^{N} \frac{|2^n-1|_{S_k}}{n}$ in terms of the previous sum $\sum_{n=1}^{N} \frac{|2^n-1|_{S_{k-1}}}{n}$ and some other terms.

From here on, we shall set some notation so that we can write things down conveniently. Let E be a finite subset of the natural numbers. For $T \subset S$, let

$$\begin{aligned}
k_T &= \text{the leading coefficient in the sum } \sum_{t \le N} \frac{|t|_T}{t}, \\
k_{T,E} &= \text{the leading coefficient in the sum } \sum_{\substack{t \le N \\ m_p \nmid t \ \forall p \in E}} \frac{|t|_T}{t}, \\
K_{\alpha,S} &= \text{the leading coefficient in the sum } \sum_{n \le N} \frac{|2^n-1|_S}{n}, \\
k_S := k_{\alpha,S} &= \text{the leading coefficient in the sum } M_\alpha(N),
\end{aligned}$$

and let us state and prove the result as follows.

Theorem 5.9. *Let S_k be a set of primes having k distinct elements, $k \ge 1$. Write $S_k = \{p_1, \ldots, p_k\} = S_{k-1} \cup \{p_k\}$ and, for any $T \subseteq S_{k-1}$, write $T' = T \cup \{p_k\}$. Then*

$$\sum_{n \le N} \frac{|2^n-1|_{S_k}}{n} = \sum_{n \le N} \frac{|2^n-1|_{S_{k-1}}}{n} - \blacksquare$$

where

$$\blacksquare = \sum_{T \in \mathcal{M}} \frac{|2^{o_{T'}}-1|_T}{o_{T'}} \left(\sum_{\substack{t \le N/o_{T'} \\ m_p \nmid o_{T'} t \ \forall p \in S_k \setminus T'}} \frac{|t|_T}{t} - |o_{T'}|_{p_k} |2^{m_{p_k}}-1|_{p_k} \sum_{\substack{t \le N/o_{T'} \\ m_p \nmid o_{T'} t \ \forall p \in S_k \setminus T'}} \frac{|t|_{T'}}{t} \right), \quad (90)$$

and

$$\mathcal{M} = \{T \subseteq S_{k-1} \ : \ \forall p \in \ S_{k-1} \setminus T, \ m_p \nmid o_{T'}\}.$$

Proof. By (89), we write

$$\sum_{n\le N}\frac{|2^n-1|_{S_{k-1}}}{n} = \sum_{T\subseteq S_{k-1}}\sum_{\substack{n\le N,\ o_T|n\\ m_p\nmid n\forall p\in S_{k-1}\setminus T}}\frac{|2^n-1|_T}{n} \tag{91}$$

$$= \sum_{T\subseteq S_{k-1}}\sum_{\substack{n\le N,\ o_T|n\\ m_p\nmid n\forall p\in S_{k-1}\setminus T, m_{p_k}\nmid n}}\frac{|2^n-1|_T}{n} \tag{92}$$

$$+\sum_{T\subseteq S_{k-1}}\sum_{\substack{n\le N,\ o_T|n\\ m_p\nmid n\forall p\in S_{k-1}\setminus T, m_{p_k}|n}}\frac{|2^n-1|_T}{n}. \tag{93}$$

The sum in (93) may be divided into

$$\sum_{T\in\mathcal{M}}\sum_{\substack{n\le N,\ o_{T'}|n\\ m_p\nmid n\forall p\in S_k\setminus T'}}\frac{|2^n-1|_T}{n}, \tag{94}$$

and

$$\sum_{T\notin\mathcal{M}}\sum_{\substack{n\le N,\ o_{T'}|n\\ m_p\nmid n\forall p\in S_k\setminus T'}}\frac{|2^n-1|_T}{n}. \tag{95}$$

In (95), since $T\notin\mathcal{M}$, it follows that there exists $q\in S_{k-1}\setminus T$ such that $m_q|o_{T'}$. Since $o_{T'}|n$, we get $m_q|n$, which contradicts $m_p\nmid n\ \forall\ p\in S_k\setminus T'$. Thus the sum in (95) is empty.

The sum in (94) is equal to

$$\sum_{T\in\mathcal{M}}\sum_{\substack{n\le N,\ o_{T'}|n\\ m_p\nmid n\forall p\in S_k\setminus T'}}\frac{|2^n-1|_{T'}}{n}+\blacksquare, \tag{96}$$

where

$$\blacksquare=\sum_{T\in\mathcal{M}}\sum_{\substack{n\le N,\ o_{T'}|n\\ m_p\nmid n\forall p\in S_k\setminus T'}}\frac{|2^n-1|_T}{n}-\sum_{T\in\mathcal{M}}\sum_{\substack{n\le N,\ o_{T'}|n\\ m_p\nmid n\forall p\in S_k\setminus T'}}\frac{|2^n-1|_{T'}}{n}. \tag{97}$$

We notice that

$$\mathcal{P}(S_k)=\{\ T,\ T\cup\{p_k\}\ :\ T\in\mathcal{P}(S_{k-1})\ \},$$

where $\mathcal{P}(S_{k-1})$ is the set of all subsets of S_{k-1}.

Thus

$$\sum_{n\le N}\frac{|2^n-1|_{S_k}}{n} = \sum_{T\subseteq S_{k-1}}\sum_{\substack{n\le N,\ o_T|n\\ m_p\nmid n\forall p\in S_k\setminus T}}\frac{|2^n-1|_T}{n} \tag{98}$$

$$+\sum_{T\subseteq S_{k-1}}\sum_{\substack{n\le N,\ o_{T'}|n\\ m_p\nmid n\forall p\in S_k\setminus T'}}\frac{|2^n-1|_{T'}}{n}. \tag{99}$$

We assert that (98) is equal to the expression in (92), while (99) is the first term in (96).

Hence

$$\sum_{n\le N}\frac{|2^n-1|_{S_{k-1}}}{n}=\sum_{n\le N}\frac{|2^n-1|_{S_k}}{n}+\blacksquare.$$

Moreover, by applying Lemma 4.18 to $\blacksquare$, it turns out to be the summation in (90) in the statement of the theorem. □

Corollary 5.10. *In the same situation as Theorem 5.9,*

$$K_{\alpha,S_k}<K_{\alpha,S_{k-1}}.$$

Proof. It is easy to see that $S_{k-1}\in\mathcal{M}$, so $\mathcal{M}\neq\emptyset$. Let $T\in\mathcal{M}$.

By Proposition 5.7 and Lemma 5.6, we have

$$\sum_{\substack{t\le N/o_{T'}\\ m_p\nmid o_{T'}t\ \forall p\in S_k\setminus T'}}\frac{|t|_T}{t}=d_T\log N+C_{29}+O(1/N), \tag{100}$$

and

$$\sum_{\substack{t\le N/o_{T'}\\ m_p\nmid o_{T'}t\ \forall p\in S_k\setminus T'}}\frac{|t|_{T'}}{t}=d_{T'}\log N+C_{30}+O(1/N), \tag{101}$$

for some constants $d_T,\ d_{T'},\ C_{29},\ C_{30}$. Since $|t|_{T'} \le |t|_T$ for all t, $d_{T'} \le d_T$.

From (101) and (100), we get

$$\sum_{\substack{t \le N/o_{T'} \\ m_p \nmid o_{T'} t \ \forall p \in S_k \setminus T'}} \left(\frac{|t|_T}{t} - \frac{|t|_{T'}}{p_k^j t} \right) = \left(d_T - \frac{d_{T'}}{p_k^j} \right) \log N + C_{31} + O(1/N),$$

for some constant C_{31} and $j = \mathrm{ord}_{p_k}(2^{m_{p_k}} - 1) + \mathrm{ord}_{p_k}(o_{T'})$. Obviously, $j \ge 1$. Thus $\frac{d_{T'}}{p_k^j} < d_{T'}$. This implies that $d_T - \frac{d_{T'}}{p_k^j} > 0$. By Theorem 5.9, we obtain that

$$K_{\alpha,S_k} = K_{\alpha,S_{k-1}} - \sum_{T \in \mathcal{M}} \frac{|2^{o_{T'}} - 1|_T}{o_{T'}} \left(d_T - \frac{d_{T'}}{p_k^j} \right).$$

Since all the terms in the sum are strictly positive and $\mathcal{M} \neq \emptyset$,

$$K_{\alpha,S_k} < K_{\alpha,S_{k-1}}.$$

□

The above theorem is illustated by the following examples.

Example 5.11. Let α be the same map as Example 4.6. Then

$$\sum_{n \le N} \frac{|2^n - 1|_3}{n} = \frac{5}{8} \log N + C_{32} + O(1/N),$$

for some constant C_{32}.

Proof. We note that $m_3 = 2$ and $\mathcal{M} = \{\emptyset\}$. By Theorem 5.9, we have

$$\begin{aligned} \sum_{n \le N} \frac{|2^n - 1|_3}{n} &= \sum_{n \le N} \frac{1}{n} - \left(\frac{1}{2} \sum_{t \le N/2} \frac{1}{t} - \frac{1}{2 \times 3} \sum_{t \le N/2} \frac{|t|_3}{t} \right) \\ &= \left(1 - \frac{1}{2} + \frac{3}{24} \right) \log N + C_{32} + O(1/N), \end{aligned}$$

since

$$\sum_{n \le N} \frac{1}{n} = \log N + \gamma + O(1/N), \quad \text{(by Lemma 1.21)}$$

and

$$\sum_{t\leq N/2}\frac{|t|_3}{t}=\frac{3}{4}\log N+C_{33}+O(1/N)\quad\text{(by Proposition 5.7)},$$

for some constant C_{33} □

Example 5.12. Let $S=\{3,5\}$. Let α be the S-integer map dual to $x\mapsto 2x$. Then

$$\sum_{n\leq N}\frac{|2^n-1|_S}{n}=\frac{55}{96}\log N+C_{34}+O(1/N),$$

for some constant C_{34}.

Proof. Note that $m_3=2$, $m_5=4$. We apply Theorem 5.9 with $k=2$, $S_1=\{3\}$, $S_2=\{3,5\}$ and using Example 5.11. We observe that there exists only one set $\{3\}\in\mathcal{M}$, and $\emptyset\notin\mathcal{M}$ because $m_3\mid 4$. For $T=\{3\}$, $T^{'}=\{3,5\}$ and we have $o_{T'}=4$, and $\operatorname{ord}_3(2^{o_{T'}}-1)=\operatorname{ord}_5(2^{o_{T'}}-1)=1$. Replacing these things into the formula in Theorem 5.9, then we get

$$\begin{aligned}\sum_{n\leq N}\frac{|2^n-1|_{\{3,5\}}}{n} &= \sum_{n\leq N}\frac{|2^n-1|_3}{n}\\ &\quad-\left(\frac{1}{4\times 3}\sum_{t\leq N/4}\frac{|t|_3}{t}-\frac{1}{4\times 3\times 5}\sum_{t\leq N/4}\frac{|t|_{\{3,5\}}}{t}\right)\\ &= \left(\frac{5}{8}-\frac{1}{12}\left(\frac{3}{4}\right)+\frac{1}{60}\left(\frac{3}{4}\right)\left(\frac{5}{6}\right)\right)\log N+C_{34}+O(1/N),\end{aligned}$$

as the coefficient of $\log N$ comes from applying Proposition 5.7 to the sum $\sum_{t\leq N/4}\frac{|t|_3}{t}$ and to the sum $\sum_{t\leq N/4}\frac{|t|_{\{3,5\}}}{t}$. □

From the above example, for $T=\{3\}$, $T^{'}=\{3,5\}$, we find that $\operatorname{ord}_3(2^{o_{T'}}-1)$ and $\operatorname{ord}_5(2^{o_{T'}}-1)$ are equal to 1. However, for $p\in T$, $\operatorname{ord}_p(2^{o_{T'}}-1)$ is not neccessarily 1 generally. Recall that

$$\operatorname{ord}_p(2^{o_{T'}}-1)=\operatorname{ord}_p(o_{T'})+\operatorname{ord}_p(2^{m_p}-1).\tag{102}$$

There are two possibilities that may make $\mathrm{ord}_p\,(2^{o_{T'}}-1)\geq 2$ as follows:

1. If there exists a prime number $q\in T^{'}$ such that $p\mid m_q$, then $p\mid o_{T'}$ so by (102) we have

$$\begin{aligned}\mathrm{ord}_p\,(2^{o_{T'}}-1) &= \mathrm{ord}_p(o_{T'})+\mathrm{ord}_p(2^{m_p}-1)\\ &\geq 1+1,\end{aligned}$$

   as $o_{T'}=m_p p^r t$ for some integers $r\geq 1, t$ with $\gcd(p,t)=1$.

2. If $\mathrm{ord}_p\,(2^{m_p}-1)=2$, then by (102) we get $\mathrm{ord}_p\,(2^{o_{T'}}-1)\geq 2$.

Primes for which the last property holds are called *Wieferich prime numbers*. That is, a Wieferich prime number is a prime p such that $2^{p-1}\equiv 1 \bmod p^2$. In 1913, Wieferich Meissner found that 1093 was Wieferich, and in 1922 N.G.W.H. Beeger showed that 3511 was Wieferich as well. Since 1922, no new examples have been found. According to http://mathworld.wolfram.com/WieferichPrime.html, the only known Wieferich primes smaller than 4×10^{20} are 1093 and 3511.

The following example illustrates how the first possibility may happen.

Example 5.13. Under the same condition as the previous examples, change S to be $\{3,7\}$. Then there exists a constant C_{35} with

$$\sum_{n\leq N}\frac{|2^n-1|_{\{3,7\}}}{n}=\frac{269}{576}\log N+C_{35}+O(1/N).$$

Proof. Note that $m_3=2, m_7=3$, and $\mathcal{M}=\{\emptyset,\{3\}\}$. The following table shows the values of the notations appearing in Theorem 5.9.

$T\subseteq\{3\}$	$T^{'}$	$o_{T'}$	$2^{o_{T'}}-1$
$\emptyset$	$\{7\}$	3	7
$\{3\}$	$\{3,7\}$	6	63

Thus $\mathrm{ord}_3(2^6-1)=2$ and $\mathrm{ord}_7(2^6-1)=\mathrm{ord}_7(2^3-1)=1$. By following Theorem 5.9, we have

$$\sum_{n\le N}\frac{|2^n-1|_{\{3,7\}}}{n} = \sum_{n\le N}\frac{|2^n-1|_3}{n} \tag{103}$$

$$- \left(\frac{1}{3}\underbrace{\sum_{\substack{t\le N/3\\ 2\nmid t}}\frac{1}{t}}_{A} - \frac{1}{3\times 7}\underbrace{\sum_{\substack{t\le N/3\\ 2\nmid t}}\frac{|t|_7}{t}}_{B}\right) \tag{104}$$

$$- \left(\frac{1}{6\times 3^2}\underbrace{\sum_{t\le N/6}\frac{|t|_3}{t}}_{C} - \frac{1}{6\times 3^2\times 7}\underbrace{\sum_{t\le N/6}\frac{|t|_{\{3,7\}}}{t}}_{D}\right). \tag{105}$$

For the sum in (103), we already know the coefficient of $\log N$, which is $\frac{5}{8}$. And also, the leading coefficient appearing in the sum $\sum_{t\le N/3}\frac{1}{t}$ is 1 by Lemma 1.21. Proposition 5.7 and Lemma 5.6 yield the other coefficients of $\log N$ in (104) and (105). Applying Proposition 5.7 to $\sum_{t\le N/3}\frac{|t|_7}{t}$, to C and to D, we get

$$k_{\{7\}}=\frac{7}{8},\quad k_{\{3\}}=\frac{3}{4},\quad k_{\{3,7\}}=\frac{3}{4}\times\frac{7}{8}=\frac{21}{32}.$$

Then Lemma 5.6 may be applied to the terms A and B with $k_\emptyset=1$, and $k_{\{7\}}=\frac{7}{8}$ and $E=\{2\}$ so that we can reach

$$k_{\emptyset,\{2\}}=\frac{1}{2},\quad \text{and}\quad k_{\{7\},\{2\}}=\frac{7}{16}.$$

Hence

$$\begin{aligned} K_{\alpha,\{3,7\}} &= \frac{5}{8}-\frac{1}{3}\left(\frac{1}{2}\right)+\frac{1}{3\times 7}\left(\frac{7}{16}\right)-\frac{1}{6\times 3^2}\left(\frac{3}{4}\right)+\frac{1}{6\times 3^2\times 7}\left(\frac{21}{32}\right)\\ &= \frac{269}{576}. \end{aligned}$$

□

5.4 Infinitely Many Primes

Fix p to be a prime and let n be an integer, so that $n = p^e k$ for some $k \in \mathbb{Z}$ such that $p \nmid k$ and $e \geq 0$. Also write

$$S_p = \{l \in \mathbb{P} \ : \ p \mid m_l\},$$

where m_l is the multiplicative order of $2 \pmod{l}$, and

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

the p^{th}cyclotomic polynomial. For each $p \neq 2$, the density of S_p is $\frac{p}{p^2-1}$ [16] and in the case of $p = 2$, we recall that S_2 has density $\frac{17}{24}$.

Lemma 5.14. *For any $e \geq 1$, we have*

$$|2^n - 1|_{S_p} \leq \frac{p^\epsilon}{\Phi_p(2^{p^{e-1}k})},$$

where $\epsilon = \text{ord}_p(2^n - 1)$.

Proof. For each $e \geq 1$, we may first factorize the term $2^n - 1$ as

$$2^n - 1 = \left(2^{p^{e-1}k} - 1\right)\left(\underbrace{2^{(p-1)p^{e-1}k} + 2^{(p-2)p^{e-1}k} + \cdots + 2^{p^{e-1}k} + 1}_{\Phi_p(2^{p^{e-1}k})}\right).$$

We note that $\text{Res}(x - 1, \Phi_p(x)) = p$. By Proposition 3.5.7 and Proposition 3.5.8 in [6], we deduce that the greatest common divisor of both factors of $2^n - 1$ must be either 1 or p.

Consequently, we next claim that if l is any prime except p and $\Phi_p(2^{p^{e-1}k})$ is divisible by l, then l belongs to S_p. Assume that $l \mid \Phi_p(2^{p^{e-1}k})$ and $l \neq p$. If $m_l \mid k$, then $l \mid 2^{p^{e-1}k} - 1$. So

$$l \mid \gcd(2^{p^{e-1}k} - 1, \Phi_p(2^{p^{e-1}k})) = 1 \text{ or } p,$$

which contradicts the assumption that $l \neq p$. Thus $m_l \nmid k$. Suppose $p \nmid m_l$, then $\gcd(p, m_l) = 1$. Since $m_l \mid n = p^e k$, we get $m_l \mid k$, which is impossible. Thus $p \mid m_l$. Hence we can finish the claim as required.

Finally,

$$\begin{aligned}
|2^n - 1|_{S_p} &= \left|2^{p^{e-1}k} - 1\right|_{S_p} \left|\Phi_p(2^{p^{e-1}k})\right|_{S_p} \\
&\leq \left|\Phi_p(2^{p^{e-1}k})\right|_{S_p} \\
&= \frac{1}{|\Phi_p(2^{p^{e-1}k})|_{S_p^c}\, \Phi_p(2^{p^{e-1}k})} \qquad \text{(by Lemma 3.21)} \\
&= \frac{p^\delta}{\Phi_p(2^{p^{e-1}k})} \quad (\because p \in S_p^c \text{ and by applying the above claim})
\end{aligned}$$

where $\delta = \mathrm{ord}_p(\Phi_p(2^{p^{e-1}k}))$.

As we know from Lemma 3.22 that

$$\mathrm{ord}_p(2^n - 1) = \begin{cases} c_p + e & \text{if } m_p \mid n \\ 0 & \text{elsewhere,} \end{cases}$$

where $c_p = \mathrm{ord}_p(2^{m_p} - 1)$ and in fact, $\mathrm{ord}_p(\Phi_p(2^{p^{e-1}k})) \leq \mathrm{ord}_p(2^n - 1)$, it follows that $\delta \leq c_p + e$ if $m_p \mid n$ and otherwise $\delta = 0$. Thus $\delta \leq \epsilon$. □

Lemma 5.15. *For any $e \geq 1$, let*

$$A_e(N) = \sum_{\substack{k \geq \lfloor \frac{N}{p^e} \rfloor + 2 \\ p \nmid k}}^{\infty} \frac{p^\epsilon}{p^e k \Phi_p(2^{p^{e-1}k})}.$$

Then

$$A_e(N) \leq \frac{2p^{c_p}}{2^{N/2} 2^{p^{e-1}}},$$

and $\epsilon \leq c_p + e$ (where ϵ and c_p are defined in the proof of Lemma 5.14*).*

Proof. Let e be a positive integer.

Then

$$\begin{aligned} A_e(N) &\leq \sum_{k \geq \lfloor \frac{N}{p^e} \rfloor + 2}^{\infty} \frac{p^{c_p+e}}{p^e k(2^{(p-1)p^{e-1}k})} \\ &\leq \frac{p^{c_p}}{2^{(p-1)p^{e-1}(\lfloor \frac{N}{p^e} \rfloor + 2)}} \sum_{j=0}^{\infty} \frac{1}{2^{(p-1)p^{e-1}j}} \\ &\leq \frac{2p^{c_p}}{2^{(p-1)p^{e-1}\frac{N}{p^e}+(p-1)p^{e-1}}} \qquad (\text{as} \lfloor \tfrac{N}{p^e} \rfloor \geq \tfrac{N}{p^e} - 1, \quad \text{and} \quad \sum_{j=0}^{\infty} \tfrac{1}{2^{(p-1)p^{e-1}j}} \leq 2) \\ &\leq \frac{2p^{c_p}}{2^{N/2}2^{p^{e-1}}}. \end{aligned}$$

In particular, $A_e(0) \leq \frac{2p^{c_p}}{2^{p^{e-1}}}$. □

Theorem 5.16. *There is a constant C_{36} with*

$$\sum_{n \leq N} \frac{|2^n - 1|_{S_p}}{n} = \left(1 - \frac{1}{p}\right) \log N + C_{36} + O(1/N).$$

Proof. The sum $\sum_{n \leq N} \frac{|2^n-1|_{S_p}}{n}$ may be divided up according to the power of p which divides n as shown below:

$$\sum_{n \leq N} \frac{|2^n - 1|_{S_p}}{n} = \sum_{e=0}^{\lfloor \frac{\log N}{\log p} \rfloor} \sum_{\substack{n<N \\ \text{ord}_p(n)=e}} \frac{|2^n - 1|_{S_p}}{n}. \tag{106}$$

If $e = 0$, $2^k - 1$ is made up only primes outside S_p since $p \nmid k$. In other words, if $l \mid 2^k - 1$, then $l \notin S_p$. Thus $\left|2^k - 1\right|_{S_p} = 1$. Hence the sum in (106) becomes

$$\sum_{n \leq N} \frac{|2^n - 1|_{S_p}}{n} = \sum_{\substack{k<N \\ p \nmid k}} \frac{1}{k} + \sum_{e=1}^{\lfloor \frac{\log N}{\log p} \rfloor} \sum_{\substack{n<N \\ \text{ord}_p(n)=e}} \frac{|2^n - 1|_{S_p}}{n}. \tag{107}$$

For the case $e = 0$, we know the asymptotic expression of the first sum on the right hand side in (107) is equal to

$$\left(1 - \frac{1}{p}\right) \log N + C_{37} + O(1/N).$$

for some constant C_{37} by Lemma 5.6.

For the case $e \geq 1$, we may write

$$\begin{aligned}
\sum_{\substack{1\leq n\leq N\\ \mathrm{ord}_p(n)=e}} \frac{|2^n-1|_{S_p}}{n} &= \sum_{\substack{1\leq n\leq N\\ p^e\mid n, p^{e+1}\nmid n}} \frac{|2^n-1|_{S_p}}{n} \\
&= \sum_{\substack{1\leq k\leq \lfloor \frac{N}{p^e}\rfloor\\ p\nmid k}} \frac{\left|2^{p^e k}-1\right|_{S_p}}{p^e k} \\
&\leq \sum_{\substack{1\leq k\leq \lfloor \frac{N}{p^e}\rfloor+1\\ p\nmid k}} \frac{p^{\epsilon}}{p^e k \Phi_p(2^{p^{e-1}k})} \quad \text{(by Lemma 5.14)} \\
&\leq \frac{p^{c_p}}{\Phi_p(2^{p^{e-1}})} + A_e(0) - A_e(N) \quad (\text{as } \epsilon \leq c_p + e, \text{ by Lemma 5.15}).
\end{aligned}$$

Since $A_e(N) \to 0$ as $N \to \infty$,

$$\begin{aligned}
\sum_{\substack{n=1\\ \mathrm{ord}_p(n)=e}}^{\infty} \frac{|2^n-1|_{S_p}}{n} = \lambda_e &\leq \frac{p^{c_p}}{\Phi_p(2^{p^{e-1}})} + A_e(0) \\
&\leq \frac{3p^{c_p}}{2^{p^{e-1}}}.
\end{aligned}$$

Consequently,

$$\left| \sum_{\substack{1\leq n\leq N\\ \mathrm{ord}_p(n)=e}} \frac{|2^n-1|_{S_p}}{n} - \lambda_e \right| \leq \frac{6p^{c_p}}{2^{p^{e-1}}} + A_e(N).$$

This implies that

$$\sum_{\substack{1\leq n\leq N\\ \mathrm{ord}_p(n)=e}} \frac{|2^n-1|_{S_p}}{n} = \lambda_e + O(2^{-p^{e-1}}) + O(2^{-N/2}\cdot 2^{-p^{e-1}}). \tag{108}$$

Now, we return to consider the sum

$$\sum_{e=1}^{\lfloor \frac{\log N}{\log p}\rfloor} \sum_{\substack{1\leq n\leq N\\ \mathrm{ord}_p(n)=e}} \frac{|2^n-1|_{S_p}}{n}, \tag{109}$$

which converges as $N \to \infty$ because it is bounded by the sum

$$\sum_{e=1}^{\lfloor \frac{\log N}{\log p} \rfloor} \lambda_e \leq 3p^{c_p} \sum_{e=1}^{\frac{\log N}{\log p}} \frac{1}{2^{p^{e-1}}},$$

and this sum converges as $N \to \infty$.

We write the sum in (109) as

$$\sum_{e=1}^{\infty} \sum_{\substack{1 \leq n \leq N \\ \mathrm{ord}_p(n)=e}} \frac{|2^n - 1|_{S_p}}{n} - \sum_{e=\lfloor \frac{\log N}{\log p} \rfloor + 1}^{\infty} \sum_{\substack{1 \leq n \leq N \\ \mathrm{ord}_p(n)=e}} \frac{|2^n - 1|_{S_p}}{n}, \tag{110}$$

and the first sum in (110) converges to a constant C_{38}.

We next substitute (108) to (110) so that we get

$$\begin{aligned} \left| \sum_{e=1}^{\lfloor \frac{\log N}{\log p} \rfloor} \sum_{\substack{1 \leq n \leq N \\ \mathrm{ord}_p(n)=e}} \frac{|2^n - 1|_{S_p}}{n} - C_{38} \right| &\leq \left| \sum_{e=\lfloor \frac{\log N}{\log p} \rfloor + 1}^{\infty} \lambda_e \right| + \left| \sum_{e=\lfloor \frac{\log N}{\log p} \rfloor + 1}^{\infty} O(2^{-p^{e-1}}) \right| \\ &+ \left| \sum_{e=\lfloor \frac{\log N}{\log p} \rfloor + 1}^{\infty} O(2^{-N/2}.2^{-p^{e-1}}) \right| \\ &\leq \frac{C_{39}}{2^N}. \end{aligned}$$

for some constant C_{39}.

Hence

$$\sum_{e=1}^{\lfloor \frac{\log N}{\log p} \rfloor} \sum_{\substack{1 \leq n \leq N \\ \mathrm{ord}_p(n)=e}} \frac{|2^n - 1|_{S_p}}{n} = C_{38} + O(2^{-N}).$$

The main result is completed. □

Remark 5.17. We know that $k_S = 1$ when $S = \emptyset$, and $k_S = 0$ when S is a co-finite subset of primes. In Example 5.13, for $S = \{3, 7\}$, we get $k_S < \frac{1}{2}$. It is natural to assume that k_S might be close to zero when S is large, for example an infinite subset of primes with strictly positive density. Surprisingly, S_2 has density $\frac{17}{24} > \frac{1}{2}$,

but $k_S = \frac{1}{2}$ is large, by Theorem 5.16 in the case $p = 2$. Thus we see that for any S, k_S depends fundamentally on the arithmetic of the primes in S, not just on the density of primes in S.

Bibliography

[1] A. G. Akritas, 'A new method for computing polynomial greatest common divisors and polynomial remainder sequences', *Numer. Math.* **52** (1988), no. 2, 119–127. http://dx.doi.org/10.1007/BF01398685.

[2] T. M. Apostol, *Introduction to analytic number theory* (Springer-Verlag, New York, 1976). Undergraduate Texts in Mathematics.

[3] T. M. Apostol, 'An elementary view of Euler's summation formula', *Amer. Math. Monthly* **106** (1999), no. 5, 409–418. http://dx.doi.org/10.2307/2589145.

[4] R. Bowen, 'Erratum to "Entropy for group endomorphisms and homogeneous spaces"', *Trans. Amer. Math. Soc.* **181** (1973), 509–510.

[5] V. Chothi, G. Everest, and T. Ward, 'S-integer dynamical systems: periodic points', *J. Reine Angew. Math.* **489** (1997), 99–132.

[6] H. Cohen, *Number theory. Vol. I. Tools and Diophantine equations*, in *Graduate Texts in Mathematics* **239** (Springer, New York, 2007).

[7] E. I. Dinaburg, 'A correlation between topological entropy and metric entropy', *Dokl. Akad. Nauk SSSR* **190** (1970), 19–22.

[8] G. Everest, R. Miles, S. Stevens, and T. Ward, 'Orbit-counting in non-hyperbolic dynamical systems', *J. Reine Angew. Math.* **608** (2007), 155–182.

[9] G. Everest, R. Miles, S. Stevens, and T. Ward, 'Dirichlet series for finite combinatorial rank dynamics', *Trans. Amer. Math. Soc.* **362** (2010), 199–227.

[10] G. Everest and T. Ward, *An introduction to number theory*, in *Graduate Texts in Mathematics* **232** (Springer-Verlag London Ltd., London, 2005).

[11] L. W. Goodwyn, 'Comparing topological entropy with measure-theoretic entropy', *Amer. J. Math.* **94** (1972), 366–388.

[12] F. Q. Gouvêa, *p-adic numbers*, in *Universitext* (Springer-Verlag, Berlin, second ed., 1997). An introduction.

[13] R. Gupta and M. R. Murty, 'A remark on Artin's conjecture', *Invent. Math.* **78** (1984), no. 1, 127–130.

[14] L.-S. Hahn and B. Epstein, *Classical complex analysis* (Jones and Bartlett, London, 1996).

[15] G. H. Hardy and E. M. Wright, *Introduction à la théorie des nombres* (Vuibert, Paris, 2007). Translated from the 1979 English original by François Sauvageot and with an introduction by Catherine Goldstein.

[16] H. Hasse, 'Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von durch eine vorgegebene Primzahl $l \neq 2$ *teilbarer bzw. unteilbarer* Ordnung $\pmod p$ ist', *Math. Ann.* **162** (1965/1966), 74–76.

[17] D. R. Heath-Brown, 'Artin's conjecture for primitive roots', *Quart. J. Math. Oxford Ser. (2)* **37** (1986), no. 145, 27–38.

[18] E. Hemmingsen and W. Reddy, 'Expansive homeomorphisms on homogeneous spaces', *Fund. Math.* **64** (1969), 203–207.

[19] C. Hooley, 'On Artin's conjecture', *J. Reine Angew. Math.* **225** (1967), 209–220.

[20] S. Kakutani, 'Examples of ergodic measure preserving transformations which are weakly mising but not strongly mixing', in *Recent advances in topological dynamics (Proc. Conf., Yale Univ., New Haven, Conn., 1972; in honor of Gustav Arnold Hedlund)*, pp. 143–149. Lecture Notes in Math., Vol. 318 (Springer, Berlin, 1973).

[21] J. C. Lagarias, 'Errata to: "The set of primes dividing the Lucas numbers has density 2/3" [Pacific J. Math. **118** (1985), no. 2, 449–461; MR0789184 (86i:11007)]', *Pacific J. Math.* **162** (1994), no. 2, 393–396.

[22] B. Mark Villarino, *Mertens' proof of Mertens' theorem.* `http://arxiv.org/abs/math/0504289`.

[23] M. R. Murty, *Problems in analytic number theory*, in *Graduate Texts in Mathematics* **206** (Springer-Verlag, New York, 2001). Readings in Mathematics.

[24] M. S. M. Noorani, 'Mertens theorem and closed orbits of ergodic toral automorphisms', *Bull. Malaysian Math. Soc. (2)* **22** (1999), no. 2, 127–133.

[25] W. Parry and M. Pollicott, 'An analogue of the prime number theorem for closed orbits of Axiom A flows', *Ann. of Math. (2)* **118** (1983), no. 3, 573–591.

[26] W. Parry, 'An analogue of the prime number theorem for closed orbits of shifts of finite type and their suspensions', *Israel J. Math.* **45** (1983), no. 1, 41–52.

[27] P. Ribenboim, *My numbers, my friends* (Springer-Verlag, New York, 2000). Popular lectures on number theory.

[28] D. Shanks, *Solved and unsolved problems in number theory* (Chelsea Publishing Co., New York, third ed., 1985).

[29] R. Sharp, 'An analogue of Mertens' theorem for closed orbits of Axiom A flows', *Bol. Soc. Brasil. Mat. (N.S.)* **21** (1991), no. 2, 205–229.

[30] V. Stangoe, *Orbit counting far from hyperbolicity* (Ph.D. thesis, University of East Anglia, 1996).

[31] R. P. Stanley, *Enumerative combinatorics. Vol. 1*, in *Cambridge Studies in Advanced Mathematics* **49** (Cambridge University Press, Cambridge, 1997). With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original.

[32] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, in *Cambridge Studies in Advanced Mathematics* **46** (Cambridge University Press, Cambridge, 1995). Translated from the second French edition (1995) by C. B. Thomas.

[33] S. Waddington, 'The prime orbit theorem for quasihyperbolic toral automorphisms', *Monatsh. Math.* **112** (1991), no. 3, 235–248. `http://dx.doi.org/10.1007/BF01297343`.

[34] P. Walters, *An introduction to ergodic theory*, in *Graduate Texts in Mathematics* **79** (Springer-Verlag, New York, 1982).

[35] T. B. Ward, 'Almost all S-integer dynamical systems have many periodic points', *Ergodic Theory Dynam. Systems* **18** (1998), no. 2, 471–486.

[36] T. Ward, 'An uncountable family of group automorphisms, and a typical member', *Bull. London Math. Soc.* **29** (1997), no. 5, 577–584.

[37] A. Weil, *Basic number theory*, in *Classics in Mathematics* (Springer-Verlag, Berlin, 1995). Reprint of the second (1973) edition.