AN ABSTRACT OF THE THESIS OF

SHAMSIAH MOHDZAID for the MASTER OF SCIENCE

in MATHEMATICS presented on JUNE 17, 86

Title: ARITHMETIC FUNCTIONS: AN ALGEBRAIC APPROACH

Abstract approved: Essam Abotteen

The purpose of this thesis is to investigate arithmetic functions from an algebraic point of view. The emphasis is on algebraic structure on the set of arithmetic functions under two different convolution-type product operations, the Dirichlet product (*), and the unitary product (o). This algebraic approach has the advantage that it leads to the development of many classical results in number theory without difficulties and unpleasant computational techniques. The set of arithmetic functions with respect to ordinary addition and Dirichlet product forms a unique factorization domain. However, contrary to Dirichlet product, the set of arithmetic functions with ordinary addition and unitary product is not even an integral domain. Some important arithmetic functions and their unitary analogues will be discussed.

ARITHMETIC FUNCTIONS:
AN ALGEBRAIC APPROACH

A Thesis

Presented to

the Division of Mathematical and Physical Sciences

EMPORIA STATE UNIVERSITY

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

---

by

Shamsiah Mohdzaid

August 1988

Essam Abatteen

Approved for the Major Division

Edward

Approved for the Graduate Council

ACKNOWLEDGMENTS

My greatest thanks to Almighty God for giving me the strength and energy to work on this thesis.

I would also like to express my thanks and appreciation to my professors at Emporia State University, my committee, and especially to my advisor, Dr. Essam Abotteen, for his great support and assistance throughout this study.

This thesis is dedicated to my dearest husband and children, and to all Muslims in the world.

TABLE OF CONTENTS

INTRODUCTION

Sequences of real or complex numbers are often dealt with in number theory. Arithmetic functions are similar to these sequences. To define properly, an arithmetic function is a real- or a complex-valued function whose domain is the set of positive integers. The theory of arithmetic functions has always been one of the most active parts of the theory of numbers. Arithmetic functions play an important role in the study of divisibility properties of integers and the distribution of primes.

The purpose of this thesis is to investigate arithmetic functions from an algebraic point of view. The emphasis in this study is on the algebraic structure of the set of arithmetic functions under two different convolution-type product operations, the Dirichlet product denoted by $*$, and the unitary product which is denoted by $\circ$. The main advantage of the algebraic viewpoint is it leads to the development of many classical results in number theory without difficulties and unpleasant computational techniques. The scope of this thesis allows us only to present the simplest ideas and facts of this extensive topic. For example, no attempt has been made in this study of such an important topic as the asymptotic properties of arithmetic functions.

Arithmetic functions have a lengthy history. In this brief historical introduction, we will give a very short sketch of the history of algebraic theory of arithmetic functions. The early history of arithmetic functions is contained in Dickson's treatise [12].

The Dirichlet product played a prominent role from the very beginning. Many results from the early times involved the convolution of two or more particular arithmetic functions. Early in this century, the Dirichlet product began to be viewed as a binary operation on the set of arithmetic functions. In the work of E. T. Bell [2, 3], and R. Vaidyanathaswamy [25], it was recognized that the arithmetic functions with respect to ordinary addition and Dirichlet product form a commutative ring with identity. The study of the structure of the ring of arithmetic functions has been continued by L. Carlitz [4, 5, 6]. E. Cashwell and C. Everett [7] proved that the ring of arithmetic functions is a unique factorization domain. In addition, the names of Shapiro [20], Gioia [14], Fotino [13], and Subbarao [23], must be cited.

Bell [2] first investigated the theory of arithmetic functions related to Dirichlet product. Later, Vaidyanathaswamy [25] investigated them thoroughly. Vaidyanathaswamy [25] also introduced the unitary product which has been studied extensively by E. Cohen [9, 10]. The Dirichlet product is the most widely known product on the set of arithmetic functions. It has been proven to be a valuable tool in the study of arithmetic functions. The unitary product is one of many generalizations of the Dirichlet product; other generalizations are given by Gioia [14], Davison [11], and others [22, 23].

Chapters 1 and 2 of this thesis deal with the Dirichlet product, while chapters 3 and 4 deal with the unitary product. In chapter 1, we will prove that the set of arithmetic functions with respect to ordinary addition and Dirichlet product forms a unique factorization domain; in this chapter we will also study some basic properties of multiplicative functions. Chapter 2 is concerned with some of the important arithmetic functions of number theory, such as the iota functions, Mobius function, Euler totient function, and several other functions.

The unitary product of arithmetic functions is studied in chapter 3; it is shown that contrary to Dirichlet product, the set of arithmetic functions with ordinary addition and unitary product is not an integral domain, and not a unique factorization domain. The unitary analogues of some of the arithmetic functions we studied in chapter 2 are discussed in chapter 4.

CHAPTER 1

DIRICHLET PRODUCT OF ARITHMETIC FUNCTIONS

1. THE RING OF ARITHMETIC FUNCTIONS (D, +, *)

Definition 1.1:

A real- or a complex-valued function whose domain is the set of positive integers is called an arithmetic function.

Remark:

1. While we assumed that the range of an arithmetic function is some subset of the complex numbers, many results in this study can be easily generalized to the case in which the range is any subset of any field.
2. This definition of arithmetic function seems like a sequence, it should, the two are the same. The difference is in the viewpoint: sequences are usually studied with convergence in mind, while arithmetic functions have stronger connection in the study of divisibility properties of integers and the distribution of primes.

Some of the arithmetic functions with which we shall be dealing are the following:

$\tau(n)$ = the number of positive divisors of n

$\sigma(n)$ = the sum of positive divisors of n

$\phi(n)$ = the number of positive integers $\leq$ n and relatively prime to n.

Now, we are going to consider the collection of all real-valued arithmetic functions, and denote this set by D. There are a number of operations that can be defined on D. For f and g in D, we define four operations:

1. The sum f+g is defined by

$$(f+g)(n) = f(n) + g(n)$$

2. The ordinary product fg is defined by

$$(fg)(n) = f(n)g(n)$$

3. The Dirichlet product (or convolution) f*g is defined by

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

where the summation is over all positive divisors d of n

4. The unitary product f o g is defined by

$$(fog)(n) = \sum_{\substack{d|n \\ (d,n/d)=1}} f(d)g(n/d)$$

Clearly D is closed with respect to each one of these operations. Also it is easy to see that the addition and the ordinary multiplication are commutative and associative.

Remark:

Note that $f*g$ can be expressed as follows:

$$(f*g)(n) = \sum_{d|n} f(d)g(n/d) = \sum_{d|n} f(n/d)g(d) = \sum_{d_1d_2 = n} f(d_1)g(d_2)$$

where d_1 and d_2 in the last summation run over all positive integers whose product is n.

In this chapter, we are concerned with the study of the set D, of real-valued arithmetic functions under ordinary addition and Dirichlet convolution.

Lemma 1.01:

Dirichlet product is commutative and associative.

Proof:

The commutativity of Dirichlet product is clear. To prove the associative property, let f, g, and h belong to D. We must show $(f*g) * h = f * (g*h)$.

Let $F = f*g$ and consider,

$$\begin{aligned}[(f*g) * h](n) &= (F * h)(n) \\ &= \sum_{d_1d_2 = n} F(d_1)h(d_2) \\ &= \sum_{d_1d_2 = n} h(d_2) \sum_{d_3d_4 = d_1} f(d_3)g(d_4) \\ &= \sum_{d_2d_3d_4 = n} f(d_3)g(d_4)h(d_2)\end{aligned}$$

In the same way, if we let $G = g*h$ and consider,

$$\begin{aligned}[f * (g*h)](n) &= (f * G)(n) \\ &= \sum_{d_1d_2 = n} f(d_1)G(d_2) \\ &= \sum_{d_1d_2 = n} f(d_1) \sum_{d_3d_4 = d_2} g(d_3)h(d_4)\end{aligned}$$

$$= \sum_{d_1 d_3 d_4 = n} f(d_1)g(d_3)h(d_4)$$

Hence, $(f*g) * h = f * (g*h)$ which means that Dirichlet product is associative.

We now introduce the identities for these operations. We define the functions θ , ι_0, and ϵ on D by:

$$\theta(n) = 0 \quad (n = 1,2,....)$$

$$\iota_0(n) = 1 \quad (n = 1,2,....)$$

$$\epsilon(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \neq 1 \end{cases}$$

Lemma 1.02:

For all $f \in D$, we have

1. $f + \theta = f$
2. $f \cdot \iota_0 = f$
3. $f * \epsilon = f$

Proof:

Part 1) and 2) are clear. For part 3), let

$$(f* \epsilon)(n) = \sum_{d|n} f(d) \epsilon(n/d)$$

but since $\epsilon(n/d) = 0$ for $d < n$, we have only one nonzero term in the sum, that is when $d = n$, and hence,

$$(f * \epsilon)(n) = \sum_{d|n} f(d) \epsilon(n/d) = f(n)$$

Thus we have θ and ι_0 are identities for addition and the ordinary multiplication respectively, while the function ϵ is the identity for the Dirichlet product.

Theorem 1.1:

(D, +, .) is a commutative ring with identity.

Proof:

It remains to show the distributive law, that is,

$$f(g + h) = fg + fh \quad \text{for all } f, g, h \in D$$

$$\begin{aligned}[f(g + h)](n) &= f(n)(g + h)(n) \\ &= f(n)[g(n) + h(n)] \\ &= f(n)g(n) + f(n)h(n) \\ &= (fg)(n) + (fh)(n) \\ &= [fg + fh](n)\end{aligned}$$

Theorem 1.2:

(D, +, *) is a commutative ring with identity.

Proof:

It remains to show the distributive law. For all f, g, h $\in$ D, we have

$$\begin{aligned}[f * (g+h)](n) &= \sum_{d_1d_2 = n} f(d_1)(g + h)(d_2) \\ &= \sum_{d_1d_2 = n} f(d_1)[g(d_2) + h(d_2)] \\ &= \sum_{d_1d_2 = n} [f(d_1)g(d_2) + f(d_1)h(d_2)] \\ &= \sum_{d_1d_2 = n} f(d_1)g(d_2) + \sum_{d_1d_2 = n} f(d_1)h(d_2) \\ &= (f*g)(n) + (f*h)(n) \\ &= [(f*g) + (f*h)](n)\end{aligned}$$

Thus, the distributive law is satisfied.

It can be easily seen that (D, +, .) is not an integral domain. For, consider the functions f and g in D defined by:

$$f(n) = \begin{cases} 1 & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ is odd} \end{cases}$$

$$g(n) = \begin{cases} 0 & \text{if } n \text{ is even} \\ 1 & \text{if } n \text{ is odd} \end{cases}$$

Neither f nor g is the zero function θ . But, we have $(fg)(n) = f(n)g(n) = 0$ for all integers n, hence $fg = \theta$, that is, f and g are zero divisors, and thus (D, +, .) is not integral domain. On the other hand, (D, +, *) forms an integral domain, but before we prove this, we need to define a norm function on D:

$$N : D \longrightarrow R$$

by $N(\theta) = 0$ and for $f \neq \theta \in D$,

$N(f) = 1/k$ where k is the smallest positive integer for which $f(k) \neq 0$.

<u>Lemma</u> <u>1.03:</u>

For all $f, g \in D$,

$$N(f*g) = N(f)N(g)$$

<u>Proof:</u>

The case where either f or g is the zero function θ , is trivial. Thus we may assume that neither f nor g is θ . Let $N(f) = 1/k$ and $N(g) = 1/m$. By the definition of k and m, we have,

$f(d) \neq 0$ only if $d \geq k$ and $g(d) \neq 0$ only if $d \geq m$.

Now, let us consider,

$g(km/d) \neq 0$ only if $km/d \geq m$ which implies that

$g(km/d) \neq 0$ only if $k \geq d$.

Thus,

$$(f*g)(km) = \sum_{d \mid km} f(d)g(km/d)$$

$$= f(k)g(m) + 0 + \ldots\ldots + 0 \neq 0$$

Hence, $N(f*g) \geq 1/km$ and thus we have

$$N(f*g) \geq N(f)N(g) = 1/km$$

Now we are going to show that $N(f*g) \not> N(f)N(g)$, that is, $N(f*g) \not> 1/km$.

Assume that $N(f*g) = 1/d_1d_2 > 1/km$, then $d_1d_2 < km$ and hence either $d_1 < k$ or $d_2 < m$, and we have $(f*g)(d_1d_2) = 0$, this contradicts that $N(f*g) = 1/d_1d_2$.

Therefore $N(f*g) = N(f)N(g)$.

Now, we state formally

Corollary 1.3:

$(D, +, *)$ is an integral domain.

Proof:

In order to show that D has no zero divisor, we will assume that $f*g = \theta$ in D. By lemma 1.03, we have $N(f*g) = N(f)N(g) = N(\theta) = 0$. This implies that $N(f) = 0$ or $N(g) = 0$. Thus $f = \theta$ or $g = \theta$, hence, D has no zero divisor.

Therefore $(D, +, *)$ is an integral domain.

Definition 1.2:

If for $f \in D$ there exists a function $g \in D$ such that $f*g = g*f = \epsilon$, then g is called the Dirichlet inverse of f.

We denote the Dirichlet inverse of f by f^{-1}.

Lemma 1.04:

A function $f \in D$ is Dirichlet invertible if and only if $f(1) \neq 0$. This is equivalent to say f is Dirichlet invertible if and only if $N(f) = 1$. Moreover the Dirichlet inverse of f is given by the recursion formula

$$f^{-1}(1) = 1/f(1)$$

$$f^{-1}(n) = -\,1/f(1) \sum_{\substack{d \mid n \\ d < n}} f(n/d)f^{-1}(d) \quad \text{for } n > 1$$

Proof:

First assume that f has Dirichlet inverse f^{-1}, then $f*f^{-1} =$, and in particular, $(f*f^{-1})(1) =$ $(1) = 1$, but $(f*f^{-1})(1) = \sum_{d \mid 1} f(d)f^{-1}(1/d) = f(1)f^{-1}(1) = 1$, hence $f(1) \neq 0$.

Conversely, assume that $f(1) \neq 0$. We shall show that the equation $(f*f^{-1})(n) = \epsilon(n)$ has a unique solution for the function values $f^{-1}(n)$.

For $n = 1$, we have $(f*f^{-1})(1) = \epsilon(1) = 1$ which implies that $f(1)f^{-1}(1) = 1$, and thus $f^{-1}(1) = 1/f(1)$, since $f(1) \neq 0$

Now, assume that the function values $f^{-1}(d)$ has been uniquely determined for all $d < n$.

Consider the equation $(f*f^{-1})(n) = \epsilon(n)$. For $n \neq 1$, $(f*f^{-1})(n) = \sum_{\substack{d \mid n \\ d < n}} f(n/d)f^{-1}(d) = 0$. This can be written as

$$f(1)f^{-1}(n) + \sum_{\substack{d \mid n \\ d < n}} f(n/d)f^{-1}(d) = 0.$$

If the values of $f^{-1}(d)$ are known for all divisors $d < n$, then $f^{-1}(n)$ is uniquely determined by

$$f^{-1}(n) = - 1/f(1) \sum_{\substack{d|n \\ d < n}} f(n/d)f^{-1}(d)$$

Theorem 1.4:

Let U be the set of units in D.

i.e. $U = \{ f \in D \mid f(1) \neq 0 \}$. Then $(U,*)$ is an abelian group.

Proof:

Let $f, g \in U$, then $(f * g)(1) = f(1)g(1) \neq 0$, since $f(1) \neq 0$ and $g(1) \neq 0$. Also, if $f \in U$ then $f^{-1} \in U$ follows immediately from lemma 1.04.

2. MULTIPLICATIVE FUNCTIONS

We have shown in section 1 that the set of all real-valued arithmetical functions f with $f(1) \neq 0$ formed an abelian group under Dirichlet product. In this section, we are going to study an important subgroup of this group, the subgroup of multiplicative functions.

Definition 1.2:

An arithmetic function f is said to be multiplicative if f is not identically zero and if $f(mn) = f(m)f(n)$ whenever $(m,n) = 1$.

f is completely multiplicative if $f(mn) = f(m)f(n)$ for all positive integers m, n.

Example:

Let k be a fixed real number and let $f(n) = n^k$. This function is multiplicative.

Now we are going to study some properties of multiplicative functions.

Theorem 1.5:

If f is multiplicative then $f(1) = 1$.

Proof:

Consider, $f(n) = f(n.1) = f(n)f(1)$ since $(n,1) = 1$ for any positive integer n. Since $f \neq \theta$, we have $f(n) \neq 0$ for some n, hence $f(1) = 1$.

Multiplicative functions have one big advantage, that they are completely determined once their values at prime powers are known. That is, if $n = p_1^{e1} p_2^{e2} \ldots . p_r^{er}$ is the prime factorization of n, then since the p_i^{ei} 's are relatively prime in pairs, we have $f(n) = f(p_1^{e1})f(p_2^{e2}) \ldots . f(p_r^{er})$. This can be stated more precisely as follows:

Theorem 1.6:

If f and g are multiplicative functions such that $f(p^i)=g(p^i)$ for all primes p and all positive integers i, then $f(n) = g(n)$ for all positive integers n.

Proof:

The proof of this is by math induction on the number of different prime factors of n.

a) For $k = 1$, i.e when $n = p_1^{e_1}$;

$f(n) = f(p_1^{e_1})$ and $g(n) = g(p_1^{e_1})$, thus $f(n) = g(n)$.

b) Now, assume that $f(m) = g(m)$ for k prime factors of n,

i.e. for $m = p_1^{e_1}\ p_2^{e_2} \ldots p_k^{e_k}$, $f(m) = g(m)$.

For $n = p_1^{e_1}\ p_2^{e_2} \ldots p_k^{e_k}\ p_{k+1}^{e_{k+1}}$,

$$\begin{aligned} f(n) &= f(p_1^{e_1}\ p_2^{e_2} \ldots p_k^{e_k}\ p_{k+1}^{e_{k+1}}) \\ &= f(p_1^{e_1})f(p_2^{e_2}) \ldots f(p_k^{e_k})f(p_{k+1}^{e_{k+1}}) \\ &= f(m)f(p_{k+1}^{e_{k+1}}) \end{aligned}$$

and

$$\begin{aligned} g(n) &= g(p_1^{e_1}\ p_2^{e_2} \ldots p_k^{e_k}\ p_{k+1}^{e_{k+1}}) \\ &= g(p_1^{e_1})g(p_2^{e_2}) \ldots g(p_k^{e_k})g(p_{k+1}^{e_{k+1}}) \\ &= g(m)g(p_{k+1}^{e_{k+1}}) \end{aligned}$$

but $f(m) = g(m)$ and $f(p^i\ ) = g(p^i\ )$, thus

$$f(n) = f(m)f(p_{k+1}^{e_{k+1}}) = g(m)g(p_{k+1}^{e_{k+1}}) \text{ and } f(n) = g(n).$$

Hence $f(n) = g(n)$ for all positive integers n.

Theorem 1.7:

Let f be an arithmetic function such that $f(1) = 1$. Then f is multiplicative if and only if $f(p_1^{e_1} \ldots p_r^{e_r}\ ) = f(p_1^{e_1}) \ldots f(p_r^{e_r})$ for all primes p and all integers $e_i \geq 1$.

Proof:

First, assume that f is multiplicative. Then by definition, $f(p_1^{e_1} \ldots p_r^{e_r}) = f(p_1^{e_1}) \ldots f(p_r^{e_r})$.

Conversely, assume that $f(p_1^{e_1} \ldots p_r^{e_r}) = f(p_1^{e_1}) \ldots f(p_r^{e_r})$. Let m and n be any positive integers such that $(m,n) = 1$. and $m = \prod_{i=1}^{r} p_i^{e_i}$ and $n = \prod_{j=1}^{k} q_j^{f_j}$ where $p_i \neq q_j$ for any i and j.

$$\begin{aligned} f(mn) &= f(p_1^{e_1} \ldots p_r^{e_r}\ q_1^{f_1} \ldots q_k^{f_k}) \\ &= f(p_1^{e_1}) \ldots f(p_r^{e_r}) f(q_1^{f_1}) \ldots f(q_k^{f_k}) \\ &= f(p_1^{e_1} \ldots p_r^{e_r}) f(q_1^{f_1} \ldots q_k^{f_k}) \\ &= f(m)f(n). \end{aligned}$$

Thus f is multiplicative.

Theorem 1.8:

1) The ordinary product of two multiplicative functions is a multiplicative function.

2) The Dirichlet product of two multiplicative functions is a multiplicative function.

Proof:

Part 1) is clear. For part 2), let f and g be two multiplicative functions and $h = f*g$. Let $(m,n) = 1$, then $h(mn) = \sum_{d \mid mn} f(d)g(mn/d)$.

Now, since every divisor d of mn can be written as $d = ab$ where a is a divisor of m and b is a divisor of n; moreover $(a,b) = 1$, $(m/a, n/b) = 1$, and there is a one-to-one correspondence between the set of products ab and the divisor of mn, hence,

$$\begin{aligned} h(mn) &= \sum_{\substack{a|m\\ b|n}} f(ab)g(mn/ab) \\ &= \sum_{\substack{a|m\\ b|n}} f(a)f(b)g(m/a)g(n/b) \\ &= \sum_{a|m} f(a)g(m/a) \sum_{b|n} f(b)g(n/b) \\ &= h(m)h(n) \end{aligned}$$

Therefore, $h = f*g$ is multiplicative.

Theorem 1.9:

If f is multiplicative, then its Dirichlet inverse f^{-1} is also multiplicative.

Proof:

We define a new multiplicative function g as follows: For every prime p and every positive integer e, we let $g(p^e) = f^{-1}(p^e)$ and for $n = \prod_{i=1}^{r} p_i^{e_i}$ we define $g(n) = \prod_{i=1}^{r} g(p_i^{e_i})$. Clearly g is multiplicative, hence by theorem 1.8, $f*g$ is also multiplicative. Now,

$$\begin{aligned} (f*g)(p^e) &= \sum_{d_1 d_2 = p^e} f(d_1)g(d_2) \\ &= \sum_{d_1 d_2 = p^e} f(d_1)f^{-1}(d_2) \\ &= (f*f^{-1})(p^e) \\ &= \epsilon(p^e) \end{aligned}$$

Hence, $f * g = \epsilon$, thus $g = f^{-1}$ and f^{-1} is multiplicative.

Corollary 1.10:

The set of all multiplicative arithmetic functions is an abelian group under the Dirichlet product.

Proof:

Let F be the set of all multiplicative functions. Then the commutativity and associativity holds since Dirichlet product is both commutative and associative; ϵ is the identity; and from theorems 1.8 and 1.9, for any f, g $\in$ F, $(f*g) \in F$ and $f^{-1} \in F$.

Corollary 1.11:

Let f, g and h be arithmetic functions, and suppose $f*g = h$. If any two of the functions are multiplicative, then so is the third.

Proof:

Let $h = f*g$. If f and g are multiplicative, then h is multiplicative by theorem 1.8. Assume that f and h are multiplicative, then $f * g = h$ implies that $f^{-1} * (f*g) = f^{-1} * h$, and $g = f^{-1} * h$ is multiplicative since f^{-1} and h is multiplicative. Similarly, when g and h are multipliative, f is multiplicative.

Corollary 1.12:

If $g = f * \iota_0$, i.e. if $g(n) = \sum_{d|n} f(d)$, then g is multiplicative if and only if f is multiplicative. Moreover, $\sum_{d|n} f(d) = \prod_{i=1}^{r} (\sum_{j=0}^{e_i} f(p_i^j))$ where $n = \prod_{i=1}^{r} p_i^{e_i}$ is the prime factorization of n.

Proof:

First assume that g is multiplicative.

Then, $g = f * \iota_0$ implies that $g * \iota_0^{-1} = (f * \iota_0) * \iota_0^{-1}$ and thus, $f = g * \iota_0^{-1}$ is multiplicative since both g and ι_0^{-1} are multiplicative.

Conversely, assume that f is multiplicative. Then $g = f * \iota_0$ is multiplicative.

Now, for p prime and $e > 0$,

$$(f * \iota_0)(p^e) = \sum_{d \mid p^e} f(d) = f(1) + f(p) + \ldots\ldots + f(p^e)$$

so, for $n = \prod_{i=1}^{r} p_i^{e_i}$,

$$\begin{aligned}(f * \iota_0)(n) &= \prod_{i=1}^{r} (f * \iota_0)(p_i^{e_i}) \\ &= \prod_{i=1}^{r} [\, f(p_i^0) + f(p_i^1) + \ldots\ldots + f(p_i^{e_i}) \,] \\ &= \prod_{i=1}^{r} [\, \sum_{j=0}^{e_i} f(p_i^j) \,].\end{aligned}$$

3. PRIMES AND UNIQUE FACTORIZATION IN (D, +, *)

Since the ring structure of (D, +, *) is analogous to that of the ring of integers Z, it is natural to pose some questions, such as whether (D, +, *) is a unique factorization domain? In this section we are going to prove that (D, +, *) is a unique factorization domain. The proof is based on showing that D is isomorphic to the domain $R[[x_1, x_2, ..x_n, ..]]$ of formal power series over the real field R, in countably many variables and the fact that $R[[x_1, x_2, ..x_n, ...]]$ is a unique factorization domain.

First, we extend the concepts of divisibility and prime numbers in the ring of integers to arbitrary integral domain.

Definition 1.4:

Let R be a commutative ring with identity 1, R is said to be an integral domain if ab = 0 in R implies that a = 0 or b = 0.

Definition 1.5:

If R is an integral domain, an element $b \in R$ is said to be divisible by an element $a \in R$ if there exists $x \in R$ such that $b = a * x$. We denote this by $a|b$. If $a|b$, then we say a is a factor or divisor of b.

Remark:

Unit elements in R divide any element in R. For if u is a unit in R, then for any $a \in R$, we have $a = u * u^{-1} * a$. Sometimes, we refer to the unit elements in R as improper divisors.

Definition 1.6:

Two elements a and b of a domain R are said to be associates if $a = b * u$ for some unit $u \in R$, and we denote this by $a \sim b$.

Theorem 1.13

The relation "$\sim$" of being associates is an equivalence relation on R.

Proof:

Let $a, b, c \in R$.

1) reflexivity--$a \sim a$ since $a = a * \epsilon$ for all $a \in R$.

2) symmetry--$a \sim b$ implies that $a = b * u$ for some unit $u \in R$,

which implies $a * u^{-1} = b * u * u^{-1}$

and $a * u^{-1} = b$

thus $b \sim a$

3) transitivity--$a \sim b$ implies that $a = b * u$ for some unit

$u \in R$ and

$b \sim c$ implies that $b = c * v$ for some unit

$v \in R$

thus $a = (c * v) * u = c * (v * u)$

and $a \sim c$

Therefore "$\sim$" is an equivalence relation.

Thorem 1.14:

In an integral domain R, $a \sim b$ if and only if $a | b$ and $b | a$.

Proof:

First, assume that $a \sim b$. This implies that $a = b * u$ for some unit $u \in R$. Then by definition, $b | a$. Since $a \sim b$ implies $b \sim a$, we can write $b = a * u^{-1}$, which implies that $a | b$.

Conversely, assume that $a | b$ and $b | a$.
$a | b$ implies $b = a * x$ for $x \in R$ and $b | a$ implies $a = b * y$ for $y \in R$. Thus, $a = (a * x) * y = a * (x * y)$. This implies

that $x * y = e$, which means that x and y are inverses of each other.(i.e. x and y are units). Therefore $a \sim b$.

Remarks:

1. If $a|b$, then a divides all the associates of b.
2. The associates of an element a in R are improper divisors of a.

Definition 1.7:

An element a of a domain D is said to be a proper divisor (or factor) of b if $a|b$ but $b \nmid a$. (i.e. in the equation $b = a * c$, c is not a unit in R). We denote this by $a||b$.

Remark:

If u is a unit, and $u = a * b$, then both a and b are units, thus the units of R do not have proper divisors.

Definition 1.8:

Let R be an integral domain.

1. An element c of R is said to be irreducible provided that:
   i) c is a nonzero and nonunit.
   ii) whenever $c = a * b$ for $a, b \in R$, then either a or b is a unit in R.
2. An element p of R is a prime provided that:
   i) p is a nonzero and nonunit.
   ii) If $p|ab$, then $p|a$ or $p|b$.
3. The remaining elements of R, neither θ ,unit, nor primes are called composite.

Theorem 1.15:

If R is an integral domain, then every prime element of R is irreducible.

Proof:

Suppose that $p \in R$ is a prime element. Let $p = a * b$. Since p is a prime and $p|ab$, then $p|a$ or $p|b$. If $p|a$, then we have $a = p * c$ for some $c \in R$. So, $p = (p * c) * b$, and since $p \neq 0$, then $1 = c * b$, and hence b is a unit.

Similarly, if $p|b$, then a is a unit.

Thus, p is irreducible.

Remark:

The converse of this theorem is not true in general.

Theorem 1.16:

Let R be an integral domain. Then

1. Every associate of an irreducible element of R is irreducible.
2. Every associate of a prime element of R is prime.
3. Every associate of a composite element of R is composite.

Proof:

1. Let $a \sim b$ where a is irreducible. Then $a = b * u$ for some unit $u \in R$. This implies $a * u^{-1} = b$, and since a is nonzero and nonunit, then b is nonzero and nonunit. Now, let $b = x * y$ for $x, y \in R$.

Then, $a = (x * y) * u = x * (y * u)$. Since a is irreducible, then either x or $(y * u)$ is a unit. Similarly, we can write $a = (x * y) * u = y * (x * u)$, then either y or $(x * u)$ is a unit. Hence, if $b = x * y$, either x or y is a unit. Therefore, b is irreducible.

2. Let $a \sim b$ where a is prime. Then $a = b * u$ for some unit $u \in R$. This implies $a * u^{-1} = b$, and since a is nonzero and nonunit, then b is nonzero and nonunit.

   Now, let $b \mid (x * y)$ for $x, y \in R$.

   Then, $(x * y) = b * z$ for some $z \in R$, and

   $(x * y) = (a * u^{-1}) * z$, and

   $(x * y) * u = a * z$, which implies

   $a \mid [x * (y * u)]$.

   Since a is prime, then either $a \mid x$ or $a \mid (y * u)$. If $a \mid x$, then $x = (a * r)$ for some $r \in R$, and thus $x = (b * u) * r = b * (u * r)$ implies $b \mid x$. Similarly, if $a \mid (y * u)$ then $(y * u) = (a * s)$ for some $s \in R$, and thus $y = (a * u^{-1}) * s = b * s$ implies $b \mid y$. Hence, if $b \mid (x * y)$ either $b \mid x$ or $b \mid y$.

   Therefore, b is prime.

3. Let $a \sim b$ where a is composite. Then, b is composite follows from parts 1) and 2), and the definition of composite elements.

Definition 1.9:

An integral domain R is said to be a unique factorization domain provided that:

i) Every nonzero nonunit element a of R can be written as a product of a finite number of irreducible elements in R. i.e. $a = c_1c_2...c_n$ with each $c_i \in R$ is irreducible.

ii) If $a = c_1c_2...c_n$ and $a = d_1d_2...d_m$ where c_i and d_j are irreducibles, then $n = m$ and for some permutation σ of $\{1,2,...,n\}$, c_i and $d_{\sigma(i)}$ are associates for every i.

Remark:

Conditions i) and ii) in the definition, implies every irreducible element in a unique factorization domain is prime. Thus, irreducible and prime elements coincide.

Definition 1.10:

An integral domain R is said to satisfy the ascending chain condition if R contains no infinite sequence $a_1, a_2, ...$ with the property that each a_{i+1} is a proper factor of a_i . In other words, if every chain of proper factors

$....a_{i+1} \,||\, a_i \,||\, ... \,||\, a_2 \,||\, a_1 \neq 0$ is finite.

Lemma 1.05:

The integral domain (D, +, *) of arithmetic functions satisfies the ascending chain condition.

Proof:

The proof of this lemma is by contradiction.

Let $f_1 \neq \theta, f_2, ...$ be an infinite sequence in D with the property that each $f_{i+1} \,||\, f_i$, then

$f_i = f_{i+1} * g_i$, where g_i is not a unit, hence

$N(g_i) < 1$ and $N(f_i) = N(f_{i+1})N(g_i) < N(f_{i+1})$ for any i. More generally, we have

$$N(f_1) = N(f_n) \prod_{j=1}^{n-1} N(g_j) \longrightarrow 0, \text{ as } n \longrightarrow \infty .$$

This implies $N(f_1) = 0$ and thus $f_1 = \theta$, which is a contradiction.

Remark:

On the other hand, the descending chain condition for ideals does not hold in (D, +, *).

For k an integer, let D_k be the set of all functions $f \in D$ with $N(f) \leq 1/k$.

i.e. $D_k = \{ f \in D : f(n) = 0 \text{ if } n < k \}$

We want to show that

i) each D_k is an ideal of D

ii) $D = D_1 \supset D_2 \supset D_3 \supset$ ..... with each containment proper.

i) For each k, D_k is an ideal of D.

Let $f, g \in D_k$. Then $f(n) = 0$ if $n < k$ and

$g(m) = 0$ if $m < k$.

Thus, $(f - g)(x) = f(x) - g(x) = 0$ if $x < k$.

Therefore, $f - g \in D_k$.

Now, let $f \in D_k$ and $h \in D$. We have

$$N(f * h) = N(f)N(h) \leq (1/k)\, N(h)$$
$$\leq 1/k, \text{ since } N(h) \leq 1$$

Thus $f * h \in D_k$. Therefore D_k is an ideal of D.

ii) Now, $f \in D_k$ implies that $f(n) = 0$ if $n < k$ and

$g \in D_{k-1}$ implies that $g(n) = 0$ if $n < k-1$

Thus $f \in D_{k-1}$ and hence $D_k \subset D_{k-1}$

Now define, $h(n) = \begin{cases} 0 & \text{if } n < k - 1 \\ 1 & \text{if } n \geq k - 1 \end{cases}$

Thus $h \in D_{k-1}$ but $h \notin D_k$ since $h(k - 1) = 1$.
Hence, $D_k \neq D_{k-1}$

Now, we are going to show that every nonunit element in D has a factorization into irreducible elements.

Theorem 1.17:

Let f be a nonunit element in D. Then,

$$f = g_1 * g_2 * \ldots * g_s$$

where the g_i's are irreducibles.

Proof:

If f is irreducible, there is nothing to prove. Otherwise, let $f = f_1 * h_1$ where f_1 is a proper factor of f. Either f_1 is irreducible or $f_1 = f_2 * h_2$ where f_2 is a proper factor of f_1. We continue this process and obtain a sequence $f, f_1, f_2, \ldots$ where each f_i is a proper factor of f_{i-1} But, since D satisfies the chain condition, this process breaks off after a finite number of steps. If f_n is the last term, f_n is irreducible and $f_n || f$.

We now set $f_n = g_1$ and we write $f = g_1 * f^1$. If f^1 is a unit, f is irreducible, otherwise we have $f^1 = g_2 * f^2$ where g_2 is irreducible. Continuing in this way, we obtain the sequence $f, f^1, f^2, \ldots$ each a proper factor of the preceding one and $f^{i-1} = g_i * f^i$, where g_i is irreducible. This breaks off with an irreducible element $f^{s-1} = g_s$.

Thus $f = g_1 * f^1 = g_1 * g_2 * f^2 = \ldots = g_1 * g_2 * \ldots * g_s$.

Our next objective is to show the uniqueness of factorization into irreducible elements. First, we are going to show that if the uniqueness of factorization fails, it fails in a "simple way".

First, let us divide the set of all nonzero, nonunit elements of D into two classes, the class of normal elements, whose elements are those functions whose factorization into irreducibles is unique, and the class of abnormal elements, whose elements can be factored into irreducibles in two essentially different ways. Since the abnormal elements are nonunits, they all have norm less than 1.

Theorem 1.18:

Let f be an abnormal element of D such that $1/N(f)$ is a least for all abnormal functions. Suppose

$f = g_1 * \dots * g_m = h_1 * \dots * h_n$ are two essentially different factorizations of f into irreducibles g_i, h_j, then $m = n = 2$ and $N(g_1) = N(g_2) = N(h_1) = N(h_2)$.

Proof:

Neither m nor n is equal to 1, since an irreducible is a normal element. Moreover no g_i is the associate of any h_j, for if so, since cancellation holds in D (recall that D is an integral domain), we have

$g_1 * \dots * g_{i-1} * g_{i+1} * \dots * g_m = h_1 * \dots * h_{j-1} * h_{j+1} * \dots * h_n$

and each side is still abnormal. However, since g_i is irreducible, $1/N(g_i) > 1$, thus

$1/N(f) = 1/N(g_1 * \dots * g_m)$

$$= 1/[N(g_1)\ldots N(g_m)$$

$$\geq 1/N(g_1)\ldots 1/N(g_{i-1}).1/N(g_{i+1})\ldots.1/N(g_m)$$

which contradicts the minimality of $1/N(f)$ for abnormal elements. Hence, no g_i is an associate of any h_j .

Without loss of generality, we may assume

$$1/N(g_i) \leq 1/N(g_{i+1}) \quad \text{for all } i = 1,2,\ldots,m-1,$$

$$1/N(h_j) \leq 1/N(h_{j+1}) \quad \text{for all } j = 1,2,\ldots,n-1,$$

and $1/N(h_1) \leq 1/N(g_1)$.

Now,

$$(*) \quad 1/N(f) = 1/N(g_1 * \ldots * g_m)$$

$$\geq 1/N(g_1 * g_2) = 1/N(g_1).1/N(g_2)$$

$$\geq 1/N(g_1).1/N(g_1)$$

$$\geq 1/N(g_1).1/N(h_1) = 1/N(g_1 * h_1)$$

Claim:

Equality must hold throughout (*).

Suppose at least one > holds in (*), so that

$$1/N(f) > 1/N(g_1 * h_1).$$

Consider $F = f - (g_1 * h_1)$. Clearly, $F \neq \theta$, because if $k = 1/N(g_1 * h_1)$, then $f(k) = 0$ and $(g_1 * h_1)(k) \neq 0$, so $F(k) \neq 0$. Also, $f(1) = 0$ since f is not a unit and $g_1(1) = 0$ $h_1(1) = 0$ since g_i , h_i is irreducible, so $(g_1 * h_1)(1) = 0$, hence $F(1) = 0$. Therefore, F is not a unit.

$$1/N(F) = 1/N[f - (g_1 * h_1)]$$

$$= \min \{ 1/N(f), 1/N(g_1 * h_1) \}$$

$$= 1/N(g_1 * h_1) \text{ by our assumption that}$$

$$1/N(f) > 1/N(g_1 * h_1).$$

Thus, $1/N(F) < 1/N(f)$, so F is normal.

Since $g_1 | F$ and $h_1 | F$ and F is normal, it follows that $(g_1 * h_1) | F$, say $F = g_1 * h_1 * G$ for some $G \in D$.

Since $F = f - (g_1 * h_1)$, then

$$(g_1 * h_1 * G) + (g_1 * h_1) = f, \text{ so}$$

$$(g_1 * h_1) * (G + \epsilon) = f, \text{ therefore}$$

$$(g_1 * h_1) | f, \text{ say } g_1 * h_1 * H = f \text{ for some } H \in D.$$

Now, $g_1 * h_1 * H = f = g_1 * \ldots . * g_m$, hence

$$h_1 * H = g_2 * \ldots . * g_m .$$

Since $m > 1$, this product is not the zero function and not a unit, and hence is normal because

$$1/N(g_2 * \ldots * g_m) \leq 1/N(f).$$

Thus, h_1 is an associate of g_i for some $i = 2,\ldots,m-1$, which is a contradiction. Therefore, in (*), the equality holds throughout.

In particular, (*) yields,

$$1/N(g_1).1/N(g_2) = 1/N(g_1).1/N(g_1) = 1/N(g_1).1/N(h_1)$$

or $N(g_1) = N(g_2) = N(h_1)$.

Also, $m = 2$ since (*) says,

$$1/N(g_1 * \ldots . * g_m) = 1/N(g_1 * g_2).$$

But, $1/N(f) = 1/N(g_1 * g_2) = 1/N(g_1)N(g_2)$ and

$$\begin{aligned} 1/N(f) &= 1/N(h_1 * \ldots * h_n) \\ &= 1/N(h_1) \ldots . . 1/N(h_n) \\ &\geq [1/N(h_1)]^n \\ &= [1/N(g_1)]^n \end{aligned}$$

Thus, $[1/N(g_1)]^2 \geq [1/N(g_1)]^n$, so $n \leq 2$, but since $n > 1$, then $n = 2$.

Now, $g_1 * g_2 = f = h_1 * h_2$. Taking norms,

$$N(g_1 * g_2) = N(g_1)N(g_2) = N(h_1)N(h_2) = N(g_1)N(h_2\ )$$

since $N(g_1) \neq 0$, $N(g_2) = N(h_2)$.

Thus, the proof is complete.

4. THE RING OF FORMAL POWER SERIES

For any positive integer k, let

$I_k = \{ \alpha = (n_1, n_2, \ldots, n_k) \mid n_i \in Z^+ \cup \{0\} \}$, and

$x_1, x_2, \ldots, x_n, \ldots$ be a countably infinite number of indeterminates. For each $\alpha \in I_k$, we define x^{α} as

$$x^{\alpha} = x_1^{n1}\ x_2^{n2} \ldots . x_k^{nk} \quad .$$

Let R be the field of real numbers. Then the power series ring $R[[x_1, x_2, ..x_n, \ldots]]$ in indeterminates

$x_1, x_2, .., x_n, \ldots$ over R is defined as the set of all formal sums $\sum\limits_{\alpha \in I_k} a_\alpha x^{\alpha}$, where $a_\alpha = a_{n_1} a_{n_2} \ldots a_{n_k} \in R$ with addition and multiplication defined by

$$\sum a_\alpha x^\alpha + \sum b_\alpha x^\alpha = \sum (a_\alpha + b_\alpha\ ) x^\alpha$$

$$(\sum a_\alpha x^\alpha\ )(\sum b_\alpha x^\alpha\ ) = \sum c_\alpha x^\alpha \quad \text{where} \quad c_\alpha = \sum_{\beta+\gamma=\alpha} a_\beta b_\gamma \ .$$

It is easy to show that the following relations hold for all A, B, and $C \in R[[x_i \mid i \in Z^+]]$:

i) $AB = BA$

ii) $(AB)C = A(BC)$

iii) $A(B + C) = AB + AC$

iv) $1 = \sum\limits_{\alpha \in I_k} a_\alpha x^\alpha$, where $a_0 = 1$, $a_\alpha = 0$ for all $0 \neq \alpha \in I_k$, is a unit element for multiplication.

Thus, we can state formally:

Theorem 1.19:

$R[[x_i \mid i \in Z^+]]$ is a commutative ring with unity.

Now, we are going to show that $R[[x_i \mid i \in Z^+]]$ has no zero divisor.

Given $A = \sum a_\alpha x^\alpha \in R[[x_i \mid i \in Z^+]]$, the terms $a_\alpha x^\alpha$ such that $\sum \alpha = p$ are called the terms in A of total degree p.

Definition 1.11:

The formal power series A_p whose terms of total degree p are those of A and whose other terms are zero, is called the homogenous part of A of degree p.

Definition 1.12:

For every $A \in R[[x_i \mid i \in Z^+]]$, $A \neq 0$, the least integer $p \geq 0$, such that $A_p \neq 0$ is called the order of A, and we denote the order of A by $\omega(A)$.

Theorem 1.20:

$R[[x_i \mid i \in Z^+]]$ is an integral domain.

Proof:

We only need to prove that $R[[x_i \mid i \in Z^+]]$ has no zero divisor.

Let $A = \sum a_\alpha x^\alpha$ and $B = \sum b_\alpha x^\alpha$ be two nonzero elements in $R[[x_i \mid i \in Z^+]]$.

Let $p = \omega(A)$, $q = \omega(B)$, and let $A.B = \sum c_\alpha x^\alpha$ where $c_\alpha = \sum_{\beta+\gamma=\alpha} a_\beta b^\gamma$. Hence, $c_\alpha = 0$ for $\sum \alpha < p + q$ and

$c_\alpha = (A_p.B_q)_\alpha \neq 0$ for $\sum \alpha = p + q$.

Thus $A.B \neq 0$, and the proof is complete.

Theorem 1.21:

The ring of arithmetic function (D, +, *) is isomorphic to the ring of formal power series in countably infinite number of indeterminates $R[[x_i \mid i \in Z^+]]$.

Proof:

Let $\{ p_1, p_2, \ldots \}$ be the set of primes listed in any definite order. Then every integer n can be written uniquely in the form $n = p_1^{e1} p_2^{e2} \ldots.$ and uniquely described by a vector $(e_1, e_2, \ldots.)$ with nonnegative integral components, finitely many of which are nonzero.

Let $\phi : D \longrightarrow R[[x_i \mid i \in Z^+]]$ be given by

$$\phi(f) = \sum f(n)\, x^\alpha$$

where the summation extends over all $\alpha = (e_1, e_2, \ldots)$ where $n = p_1^{e1} p_2^{e2} \ldots.$.

i) Assume that $\phi(f) = \phi(g)$.

This implies that

$$\sum f(n)x^\alpha = \sum g(n)x^\alpha$$

and $f(n) = g(n)$ for all $n \in Z^+$,

and $f = g$.

Thus, ϕ is one-to-one.

ii) To show ϕ is onto, let $\sum a_\alpha x^\alpha \in R[[x_i \mid i \in Z^+]]$, define $f \in D$ by $f(n) = a_\alpha$ for all $n \in Z^+$ where $n = p_1^{e1} p_2^{e2} \ldots.$ and $\alpha = (e_1, e_2, \ldots)$, then $\phi(f) = \sum f(n)x^\alpha = \sum a_\alpha x^\alpha$.

$$\text{iii)}\quad \phi(f + g) = \sum (f + g)(n)x^{\alpha}$$
$$= \sum [f(n) + g(n)]x^{\alpha}$$
$$= \sum [f(n)x^{\alpha} + g(n)x^{\alpha}]$$
$$= \phi(f) + \phi(g).$$

$$\text{iv)}\quad \phi(f * g) = \sum (f * g)(n)x^{\alpha}$$
$$= \sum [\sum_{d_1d_2 = n} f(d_1)g(d_2)]x^{\alpha}$$
$$= \sum [\sum_{d_1d_2 = n} f(d_1)x^{\beta} \sum g(d_2)x^{\gamma}]$$

where $d_1 = p_1^{f_1}p_2^{f_2}..$ and $d_2 = p_1^{h_1}p_2^{h_2}....,$ and $\alpha = \beta + \gamma$

$$= \sum_{d_1} f(d_1)x^{\beta} \quad \sum_{d_2} g(d_2)x^{\gamma}$$
$$= \phi(f)\,\phi(g).$$

Hence, ϕ is an isomorphism.

To prove that (D, +, *) is a unique factorization domain, we need the following theorem whose proof is little involved.[7]

Theorem 1.22:

The ring of formal power series $R[[x_i \mid i \in Z^+]]$ is a unique factorization domain.

Corollary 1.23:

(D, +, *) is a unique factorization domain.

Proof:

Suppose unique factorization into irreducible elements fails in D. By theorem 1.18, we should have an element of D of the form $f * g = h * k$, where f, g, h, and k are irreducibles of the same norm, and f is not associated of either h or k. Under the isomorphism ϕ , this leads to have series of the form $\phi(f)\phi(g) = \phi(h)\phi(k)$ where $\phi(f)$, $\phi(g)$, $\phi(h)$, and $\phi(k)$ are primes in $R[[x_i \mid i \in Z^+]]$ and $\phi(f)$ is not associated with either $\phi(h)$ or $\phi(k)$.

But, this contradicts the fact that $R[[x_i \mid i \in Z^+]]$ is a unique factorization domain. Hence, factorization into irreducible elements is unique in (D, +, *) up to order and units.

Corollary 1.24:

Let $f \in D$ be such that $N(f) = 1/p$, where p is a prime, then f is irreducible in (D, +, *).

Proof:

Since (D, +, *) is a unique factorization domain, every irreducible element in (D, +, *) is also a prime.

Now, to show that if $N(f) = 1/p$, then f is irreducible.

Let $f = g * h$, then $N(f) = N(g)N(h)$. Hence, $p = 1/N(f) = 1/N(g)N(h)$, thus we must have either $1/N(g) = 1$ or $1/N(h) = 1$, thus either g or h is a unit, and hence f is irreducible.

CHAPTER 2

SOME IMPORTANT ARITHMETIC FUNCTIONS

In this chapter, we will be dealing with some of the important arithmetic functions of number theory. By taking advantage of the algebraic structure introduced on the set of arithmetic functions in Chapter 1, we prove many classical results concerning these funtions. The algebraic viewpoint has the obvious advantages of leading to the development of such results without mysterious combinatorial techniques.

The iota functions

First, we are going to introduce a very important class of arithmetic functions, the iota functions. We will see that these functions can be used to build up many of the arithmetic functions in this study.

Definition 2.1:

For any real number k, we define the functions ι_k by

$$\iota_k(n) = n^k \quad \text{for every positive integer } n.$$

We will refer to these functions as the iota functions. In particular, note that $\iota_0(n) = 1$ for every $n \geq 1$. Also we will write ι for ι_1 when no confusion will arise.

Theorem 2.1:

The iota functions are multiplicative.

Proof:

Let $(m,n) = 1$, then by definition 2.1,

$$\begin{aligned} \iota_k(mn) &= (mn)^k \\ &= m^k n^k \\ &= \iota_k(m)\,\iota_k(n) \end{aligned}$$

Thus, ι_k is multiplicative. Also, we can see that ι_k is in fact completely multiplicative.

Theorem 2.2:

The iota functions are Dirichlet invertible and

$$\iota_k^{-1}(n) = \begin{cases} 1 \text{ if } n = 1 \\ (-1)^r\, n^k & \text{if } n \text{ is a product of } r \text{ distinct primes} \\ 0 \quad \text{otherwise} \end{cases}$$

Proof:

For a real number k, $\iota_k(1) = 1 \neq 0$, hence ι_k is invertible. Furthermore, ι_k^{-1} is multiplicative. Thus, by using lemma 1.04, we get

for $n = 1$, $\iota_k^{-1}(1) = 1/\ \iota_k(1) = 1$

and for p prime, $\iota_k^{-1}(p) = -1/\ \iota_k(1) \sum\limits_{\substack{d | p \\ d < p}} \iota_k(p/d)\ \iota_k^{-1}(d)$

$$\begin{aligned} &= -(1)\ \iota_k(p)\ \iota_k^{-1}(1) \\ &= -(1)p^k \end{aligned}$$

and for $e > 1$, $\iota_k^{-1}(p^e) = -1/\ \iota_k(1) \sum\limits_{\substack{d | p^e \\ d < p^e}} \iota_k(p^e/d)\ \iota_k^{-1}(d)$

but $\iota_k^{-1}(d) \neq 0$ only if $d = 1$ or $d = p$, so

$$\begin{aligned} \iota_k^{-1}(p^e) &= (-1)[\iota_k(p^e)\,\iota_k^{-1}(1) + \iota_k(p^{e-1})\iota_k^{-1}(p)] \\ &= -p^{ek} + p^{(e-1)k}.p^k \end{aligned}$$

$$= -p^{ek} + p^{ek}.p^{-k} .p^{k}$$

$$= 0$$

and since ι_k^{-1} is multiplicative, hence for

$1 < n = \prod_{i=1}^{r} p_i^{e_i}$, $\iota_k^{-1}(n) = \prod_{i=1}^{r} \iota_k(p_i^{e_i})$

$$= \begin{cases} \prod_{i=1}^{r} -(1)p_i^{k} & \text{if all } e_i\text{'s} = 1 \\ 0 & \text{otherwise} \end{cases}$$

$$= \begin{cases} (-1)^r(p_1 p_2 \ldots p_r)^k & \text{if all } e_i\text{'s} = 1 \\ 0 & \text{otherwise} \end{cases}$$

$$= \begin{cases} (-1)^r n^k & \text{if all } e_i\text{'s} = 1 \\ 0 & \text{otherwise} \end{cases}$$

The Möbius function

Definition 2.2:

The Möbius function μ is defined to be

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \text{ is not squarefree} \\ (-1)^r & \text{if } n \text{ is a product of } r \text{ distinct primes} \end{cases}$$

Note: squarefree means that if $n = \prod_{i=1}^{r} p_i^{e_i}$, all e_i 's are 1.

Lemma 2.01:

μ is multiplicative.

Proof:

Let $(m,n) = 1$. Then

i) if $m = n = 1$, $\mu(mn) = 1 = \mu(m)\mu(n)$

ii) if either m or n, (or both) are not squarefree,

$\mu(mn) = 0 = \mu(m)\mu(n)$

iii) if m and n are squarefree, then $m = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$, where $p_i \neq q_j$ for all $i = 1,..,r$; $j = 1,...,s$.

$\mu(mn) = (-1)^{r+s} = (-1)^r (-1)^s = \mu(m)\mu(n)$

thus μ is multiplicative.

Theorem 2.3:

The Möbius function μ is the unique arithmetic function such that $\mu * \iota_0 = \epsilon$ i.e. $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \neq 1 \end{cases}$

Proof:

i) Since μ and ι_0 are multiplicative, $(\mu * \iota_0)$ is multiplicative, so

$$(\mu * \iota_0)(1) = \mu(1)\, \iota_0(1) = 1 = \epsilon(1)$$

and for p prime and $e > 0$,

$$\begin{aligned}(\mu * \iota_0)(p^e) &= \mu(1)\,\iota_0(p^e) + \mu(p)\,\iota_0(p^{e-1}) + \\ &\quad \mu(p^2)\,\iota_0(p^{e-2}) + \ldots.. + \\ &\quad \mu(p^{e-1})\,\iota_0(p) + \mu(p^e)\,\iota_0(1) \\ &= (1)(1) + (-1)(1) + 0 + \ldots + 0 + 0 \\ &= 0 \\ &= \epsilon(p^e)\end{aligned}$$

Therefore, $\mu * \iota_0 = \epsilon$

ii) To prove the uniqueness, assume that $\mu * \iota_0 = \bar{\mu} * \iota_0$

Then,

$$\begin{aligned}\mu * \iota_0 &= \bar{\mu} * \iota_0 \\ (\mu * \iota_0) * \iota_0^{-1} &= (\bar{\mu} * \iota_0) * \iota_0^{-1} \\ \mu * (\iota_0 * \iota_0^{-1}) &= \bar{\mu} * (\iota_0 * \iota_0^{-1}) \\ \mu * \epsilon &= \bar{\mu} * \epsilon \\ \mu &= \bar{\mu}\end{aligned}$$

Remark:

Note that μ is the Dirichlet inverse of ι_0 .

Theorem 2.4: (Möbius inversion theorem)

For all arithmetic functions f and g

$g = f * \iota_0$ if and only if $f = \mu * g$

i.e. $g(n) = \sum_{d|n} f(d)$ if and only if $f(n) = \sum_{d|n} \mu(d)g(n/d)$

Proof:

First, assume that $g = f * \iota_0$, then

$$\begin{aligned} \mu * g &= \mu * (f * \iota_0) \\ &= \mu * (\iota_0 * f) \\ &= (\mu * \iota_0) * f \\ &= \epsilon * f \\ &= f \end{aligned}$$

Conversely, assume that $f = \mu * g$, then

$$\begin{aligned} f * \iota_0 &= (\mu * g) * \iota_0 \\ &= (g * \mu) * \iota_0 \\ &= g * (\mu * \iota_0) \\ &= g * \epsilon \\ &= g \end{aligned}$$

Theorem 2.5: (Generalized Möbius inversion theorem)

If f, g, and h are arithmetic functions, and $h(1) \neq 0$ then $g = f * h$ if and only if $f = g * h^{-1}$.

i.e. $g(n) = \sum_{d|n} f(d)h(n/d)$ if and only if $f(n) = \sum_{d|n} g(d)h^{-1}(n/d)$

Proof:

First, assume that $g = f * h$,then

$$\begin{aligned} g * h &= (f * h) * h^{-1} \\ &= f * (h * h^{-1}) \\ &= f * \epsilon \\ &= f \end{aligned}$$

Conversely, assume that $f = g * h^{-1}$, then

$$\begin{aligned} f * h &= (g * h^{-1}) * h \\ &= g * (h^{-1} * h) \\ &= g * \epsilon \\ &= g \end{aligned}$$

Note that if $h = \iota_0$ in this theorem, then we have the classical Möbius inversion formula.

Number and sum of divisors

Definition 2.3:

For positive integers n, we define the following functions:

i) $\tau(n)$ is the number of positive divisors of n

ii) $\sigma(n)$ is the sum of positive divisors of n

iii) $\sigma_k(n)$ is the sum of the kth powers of positive divisors of n, where k is any real number.

Note that $\tau(n)$ and $\sigma(n)$ are special cases of $\sigma_k(n)$.

i.e. $\tau(n) = \sigma_0(n)$ and $\sigma(n) = \sigma_1(n)$

We can write these functions in terms of the iota functions:

$$\tau(n) = (\iota_0 * \iota_0)(n) = \sum_{d|n} 1$$

$$\sigma(n) = (\iota_0 * \iota)(n) = \sum_{d|n} d$$

$$\sigma_k(n) = (\iota_0 * \iota_k)(n) = \sum_{d|n} d^k$$

Theorem 2.6:

σ_k is multiplicative.

Proof:

Since ι_k is multiplicative, then $\sigma_k = \iota_0 * \iota_k$ is multiplicative.

Corollary 2.7:

The functions τ and σ are multiplicative.

Proof:

Since τ and σ are special cases of σ_k, hence, τ and σ are multiplicative.

Theorem 2.8:

For any prime p and any positive integer e, we have

$$\sigma_k(p^e) = \sum_{i=0}^{e} p^{ik} = \begin{cases} e+1 & \text{if } k = 0 \\ \dfrac{p^{k(e+1)} - 1}{p^k - 1} & \text{if } k \neq 0 \end{cases}$$

Proof:

$$\begin{aligned} \sigma_k(p^e) &= (\iota_0 * \iota_k)(p^e) \\ &= \sum_{d|p^e} d^k \\ &= 1 + p^k + p^{2k} + \dots + p^{ek} \\ &= \sum_{i=0}^{e} p^{ik} \end{aligned}$$

hence, by using sum of geometric progression with common ratio p^k , we have

$$\sigma_k(p^e) = \begin{cases} e + 1 & \text{if } k = 0 \\ \dfrac{p^{k(e+1)} - 1}{p^k - 1} & \text{if } k \neq 0 \end{cases}$$

Since σ_k is multiplicative, then when $n = \prod_{i=1}^{r} p_i^{e_i}$ we get

Corollary 2.9:

$$\sigma_k(n) = \begin{cases} \prod_{i=1}^{r} (e_i + 1) & \text{if } k = 0 \\ \prod_{i=1}^{r} \dfrac{p_i^{k(e_i+1)} - 1}{p_i^k - 1} & \text{if } k \neq 0 \end{cases}$$

Corollary 2.10:

If $n = \prod_{i=1}^{r} p_i^{e_i}$, then $\tau(n) = \prod_{i=1}^{r} (e_i + 1)$. Also $\tau(1) = 1$.

Proof:

$$\tau(1) = \sum_{d|1} 1 = 1 \text{ and } \tau(n) = \sigma_0(n) = \prod_{i=1}^{r} (e_i + 1).$$

Corollary 2.11:

If $n = \prod_{i=1}^{r} p_i^{e_i}$, then $\sigma(n) = \prod_{i=1}^{r} \dfrac{p_i^{e_i+1} - 1}{p_i - 1}$

Proof:

$$\sigma(n) = \sigma_1(n) = \prod_{i=1}^{r} \frac{p_i^{e_i+1} - 1}{p_i - 1}$$

It is easy to derive various identities involving the arithmetic functions σ_k and μ .

Theorem 2.12:

For any positive integer n,

$\sigma_k * \mu = \iota_k$. i.e. $\sum_{d|n} \sigma_k(d)\mu(n/d) = n^k$

Proof:

By definition, $\sigma_k = \iota_0 * \iota_k$, thus

$$\sigma_k * \iota_0^{-1} = \iota_0 * \iota_k * \iota_0^{-1}$$

$$\sigma_k * \mu = \iota_k * \epsilon$$

$$\sigma_k * \mu = \iota_k$$

Corollary 2.13:

For any positive integer n, we have

i) $\tau * \mu = \iota_0$ i.e. $\sum_{d|n} \tau(d)\mu(n/d) = 1$

ii) $\sigma * \mu = \iota$ i.e. $\sum_{d|n} \sigma(d)\mu(n/d) = n$

iii) $\sigma * \iota_0 = \tau * \iota$ i.e. $\sum_{d|n} \sigma(d) = \sum_{d|n} (n/d)\,\tau(d)$

Proof:

i) $\tau * \mu = \sigma_0 * \mu = \iota_0$

ii) $\sigma * \mu = \sigma_1 * \mu = \iota$

iii) $\sigma * \iota_0 = (\iota_0 * \iota) * \iota_0$

$= (\iota_0 * \iota_0) * \iota$

$= \tau * \iota$

We also have

Theorem 2.14:

For any positive integer n,

i) $\sum_{d|n} d\,\sigma(d) = \sum_{d|n} (n/d)^2 \sigma(d)$

ii) $\sum\limits_{d|n} \sigma(d)\sigma(n/d) = \sum\limits_{d|n} d\, \tau(d)\, \tau(n/d)$

Proof:

i) Since $\sum\limits_{d|n} (n/d)^2 \sigma(d)$ is equivalent to $(\iota_2 * \sigma)(n)$, and both ι_2 and σ are multiplicative, we can just look at its value at p^e, where p prime and $e > 0$.

$$\begin{aligned}
(\iota_2 * \sigma)(p^e) &= \sum_{d|p^e} \sigma(d)(p^e/d)^2 \\
&= \sigma(1)p^{2e} + \sigma(p)p^{2(e-1)} + \dots + \sigma(p^{e-2})p^4 \\
&\quad + \sigma(p^{e-1})p^2 + \sigma(p^e) \\
&= p^{2e} + (1+p)p^{2(e-1)} + \dots + (1 + p + \dots + p^{e-2})\, p^4 \\
&\quad + (1 + p + \dots + p^{e-1})p^2 + (1 + p + \dots + p^e) \\
&= p^{2e} + (p^{2e-2} + p^{2e-2}) + \dots + (p^4 + p^5 + \dots + p^{e+2}) \\
&\quad + (p^2 + p^3 + \dots + p^{2e-2}) + (1 + p^2 + \dots + p^e) \\
&= 1 + (p + p^2) + (p^2 + p^3 + p^4) + \dots + \\
&\quad (p^{e-1} + p^e + \dots + p^{2e-2}) + (p^e + p^{e+1} + \dots + p^{2e})
\end{aligned}$$

and

$$\begin{aligned}
\sum_{d|p^e} d\,\sigma(d) &= \sigma(1) + p\,\sigma(p) + p^2\sigma(p^2) + \dots + \\
&\quad p^{e-1}\sigma(p^{e-1}) + p^e\sigma(p^e) \\
&= 1 + p(1+p) + p^2(1 + p + p^2) + \dots + \\
&\quad p^{e-1}(1 + p + \dots + p^{e-1}) + p^e(1 + p + \dots p^e) \\
&= 1 + (p + p^2) + (p^2 + p^3 + p^4) + \dots + \\
&\quad (p^{e-1} + p^e + \dots + p^{2e-2}) + (p^e + p^{e+1} + \dots + p^{2e})
\end{aligned}$$

Thus $\sum\limits_{d|n} d\, \sigma(d) = \sum\limits_{d|n} (n/d)^2 \sigma(d)$

ii) Similarly, since $\sum\limits_{d|n} \sigma(d)\,\sigma(n/d)$ is equivalent to $(\sigma * \sigma)(n)$, then

$$
\begin{aligned}
(\sigma * \sigma)(p^e) &= \sum_{d|p^e} \sigma(d)\ \sigma(p^e/d) \\
&= \sigma(1)\sigma(p^e) + \sigma(p)\sigma(p^{e-1}) + \ldots\ldots + \\
&\quad\ \sigma(p^{e-1})\sigma(p) + \sigma(p^e)\sigma(1) \\
&= (1 + p + \ldots\ldots + p^e) + (1 + p)(1 + p + \ldots + p^{e-1}) \\
&\quad\ + \ldots\ldots + (1 + p + \ldots + p^{e-1})(1 + p) + \\
&\quad\ (1 + p + \ldots\ldots + p^e) \\
&= (1 + p + \ldots\ldots + p^e) + [(1 + p + \ldots\ldots + p^{e-1}) + \\
&\quad\ (p + p^2 + \ldots\ldots + p^e)] + \ldots + [(1 + p + \ldots + p^{e-1}) \\
&\quad\ + (p + p^2 + \ldots + p^e)] + (1 + p + \ldots + p^e) \\
&= (e + 1) + 2ep + \ldots\ldots + 2ep^{e-1} + (e + 1)p^e
\end{aligned}
$$

and

$$
\begin{aligned}
\sum_{d|p^e} d\,\tau(d)\,\tau(p^e/d) &= \tau(1)\tau(p^e) + p\ \tau(p)\tau(p^{e-1}) + \ldots\ldots + \\
&\quad\ p^{e-1}\,\tau(p^{e-1})\,\tau(p) + p^e\,\tau(p^e)\,\tau(1) \\
&= (e + 1) + p(2)e + \ldots\ldots + p^{e-1}(e)2 + \\
&\quad\ p^e(e + 1) \\
&= (e + 1) + 2ep + \ldots\ldots + 2ep^{e-1} + (e + 1)p
\end{aligned}
$$

Thus $\sum\limits_{d|n} \sigma(d)\,\sigma(n/d) = \sum\limits_{d|n} d\ \tau(d)\ \tau(n/d)$

<u>Euler's function</u>

<u>Definition 2.4:</u>

We define Euler's function ϕ by

$\phi * \iota_0 = \iota$ i.e. $\sum\limits_{d|n} \phi(d) = n$

By Möbius inversion theorem,

$\phi = \iota * \mu$ i.e. $\phi(n) = \sum_{d|n} d\mu(n/d)$

Since ι and μ are multiplicative, it follows that ϕ is multiplicative.

Theorem 2.15:

For $n > 1$, we have $\phi(n) = n \prod_{p|n}(1 - 1/p)$

Proof:

If p is prime and $e > 0$, then

$$\begin{aligned}\phi(p^e) &= (\iota * \mu)(p^e)\\ &= \iota(1)\mu(p^e) + \iota(p)\mu(p^{e-1}) + \iota(p^2)\mu(p^{e-2}) + \ldots\ldots + \\ &\quad \iota(p^{e-1})\mu(p) + \iota(p^e)\mu(1)\\ &= 0 + 0 + 0 + \ldots + p^{e-1}(-1) + p^e\\ &= -p^{e-1} + p^e\\ &= p^e(1 - 1/p)\end{aligned}$$

Then, if $1 < n = \prod_{i=1}^{r} p_i^{e_i}$,

$$\begin{aligned}\phi(n) &= \prod_{i=1}^{r} \phi(p_i^{e_i})\\ &= \prod_{i=1}^{r} p_i^{e_i}(1 - 1/p_i)\\ &= p_1^{e_1}\ldots p_r^{e_r}(1 - 1/p_1)(1 - 1/p_2)\ldots(1 - 1/p_r)\\ &= n \prod_{p|n}(1 - 1/p)\end{aligned}$$

Ordinarily, the Euler function $\phi(n)$ is defined to be the number of integers m, where $1 \leq m \leq n$ and such that $(m,n) = 1$.

To show the equivalence of the two definitions, consider the function γ defined for each positive integer n by

$$\gamma(n) = \text{number of integers } 1 \leq m \leq n \text{ with } (m,n) = 1.$$

First, we will prove the following lemma

Lemma 2.02:

If $d|n$, let $S_d = \{ mn/d \mid 1 \leq m \leq d$ and $(m,d) = 1 \}$ If $d|n$, $e|n$ and $d \neq e$, then $S_d \cap S_e = \phi$ and $\bigcup_{d|n} S_d = \{ 1,2,\ldots,n \}$. That is, $\{ S_d \mid d|n \}$ is a partition of $\{ 1,2,\ldots.,n \}$.

Proof:

Let $d|n$, $e|n$ and $d \neq e$, then

$S_d = \{ mn/d \mid 1 \leq m \leq d$ and $(m,d) = 1 \}$ and

$S_e = \{ rn/e \mid 1 \leq r \leq e$ and $(r,e) = 1 \}$

Suppose $S_d \cap S_e \neq \phi$, then there is an integer t where $t = mn/d$ and $t = rn/e$ with $1 \leq m \leq d$, $1 \leq r \leq e$, $(m,d) = 1$, $(r,e) = 1$. Thus

$(m,d) = 1$ implies that $(mn/d, dn/d) = n/d$ which implies

$$(t,n) = n/d$$

Similarly,

$(r,e) = 1$ implies that $(rn/e, en/e) = n/e$ which implies

$$(t,n) = n/e$$

$(t,n) = n/d$ and $(t,n) = n/e$ implies $d = e$, which is impossible. Therefore, if $d \neq e$, $S_d \cap S_e = \phi$

Now, let $t \in \{ 1,2,\ldots,n \}$. We will show that $t \in S_d$ for some d where $d|n$.

For some integer k, let $k = (t,n)$.

This implies that $k|t$ and $k|n$, thus $t = kb$ and $n = kd$ where

$1 \leq b \leq t$ and $1 \leq d \leq n$. From this, we get $t = bn/d$, but $1 \leq t \leq n$, so $1 \leq b \leq t \leq d \leq n$ and thus $1 \leq b \leq d$. Also, $k = (t,n)$ implies $k = (kb,kd)$ which implies $1 = (b,d)$.

Since $t = bn/d$ where $1 \leq b \leq d$ and $(b,d) = 1$, then $t \in S_d$

Now, we will show that $S_d \subset \{ 1,2,\ldots,n \}$ when $d|n$. $S_d = \{ mn/d \mid 1 \leq m \leq d \text{ and } (m,d) = 1 \}$. So, we need to show that $1 \leq mn/d \leq n$. i.e. $d \leq mn$ and $mn \leq nd$.

$mn \leq nd$ implies that $m \leq d$, which is true from the definition of S_d. $d \leq mn$ if and only if $1 \leq mk$ where $k = n/d$ and $k \geq 1$. Thus $d \leq mn$ if and only if $m \geq 1$, which is true. Thus $S_d \subset \{ 1,2,\ldots,n \}$.

Therefore, $\bigcup_{d|n} S_d = \{ 1,2,\ldots,n \}$

Now, since the collections of the subsets S_d is a partition of $\{ 1,2,\ldots,n \}$, the number of elements in $\{ 1,2,\ldots,n \}$ is the sum of the number of elements in S_d.

Since S_d has $\gamma(d)$ elements, we have $\sum_{d|n} \gamma(d) = n$.

Therefore, by Möbius inversion theorem, we have $\gamma = \iota * \mu$, and we see that $\gamma = \phi$.

Summarizing these results, we have

Theorem 2.16:

The number of integers m such that $(m,n) = 1$ and $1 \leq m \leq n$ is $\phi(n)$.

Corollary 2.17:

Any cyclic group of order n has $\phi(n)$ generators.

Proof:

Any cyclic group of order n is isomorphic to $(Z_n ,+)$. Thus we will look at the generators of $(Z_n,+)$.

The units in Z_n are $U_n = \{ [a] \in Z_n \mid (a,n) = 1 \}$ thus $\mid U_n \mid = \phi(n)$.

Claim:

Every unit in Z_n is a generator for $(Z_n,+)$.

Proof of claim:

Let $Z_n = \{ [1],[2],....,[n-1],[n] \}$. Assume that $[a] \in Z_n$ is a unit in Z_n. Since $[a]$ is a unit, $(a,n) = 1$. Thus $< [a] > = \{ [a], 2[a] ,....., n[a] \}$

We will show $r[a] \neq s[a]$ for all $1 \leq r,s \leq n$, if $r \neq s$.

Assume $r[a] = s[a]$. This implies $[ra] = [sa]$

and $ra \equiv sa \pmod n$

$(ra - sa) \equiv 0 \pmod n$

$a(r - s) \equiv 0 \pmod n$

thus $n \mid a(r - s)$

and $n \mid (r - s)$ since $n \nmid a$

but this is impossible since $(r - s) < n$. Contradiction, and thus $r[a] \neq s[a]$.

Therefore, every unit in Z_n is a generator for $(Z_n,+)$.

Theorem 2.18:

The following identities hold among the functions ϕ, τ, σ, and ι.

i) $\phi * \tau = \sigma$

ii) $\phi * \sigma = \iota * \iota$

or more generally, we have

iii) $\phi * \sigma_k = \iota * \iota_k$

Proof:

We will prove part iii) only since parts i) and ii) follow from it.

iii) $\phi * \sigma_k = (\iota * \mu) * \sigma_k = \iota * (\mu * \sigma_k) = \iota * \iota_k$

To sum up the fact that most familiar arithmetic functions namely τ , σ , ϕ , and μ can be build up from the functions ι_0 and ι , we state the following theorem

Theorem 2.19:

The group generated by ι_0 and ι is the `smallest' subgroup of the group of units of arithmetic functions in D with values in Z under the Dirichlet product which contains the following classical arithmetic functions:

$\epsilon = \iota^{-1} * \iota$: the Dirichlet identity

$\mu = \iota_0^{-1}$: Mobius function

$\tau = \iota_0 * \iota_0$: number of divisors

$\sigma = \iota * \iota_0$: sum of divisors

$\phi = \iota * \iota_0^{-1}$: Euler's function

Jordan function

The Euler ϕ-function is an example of a wider class of functions called the class of totient functions.

Definition 2.5:

An arithmetic function f is a totient if it can be written as $f = g * h^{-1}$ where g and h are completely multiplicative functions.

Clearly, the Euler ϕ-function is a totient since

$$\phi = \iota * \mu = \iota * \iota_0^{-1}$$

where both ι and ι_0 are completely multiplicative functions.

As an example of a totient function, we will consider the Jordan totient J_k as one of many generalizations of the Euler ϕ-function.

Definition 2.6:

For any positive integer k, the kth order Jordan totient function J_k is defined by $J_k = \iota_k * \mu$. It follows from the definition that $J_k(n) = \sum_{d|n} \mu(d)(n/d)$

Theorem 2.10:

For any integer $k \geq 1$, J_k is a totient.

Proof:

Since $J_k = \iota_k * \mu = \iota_k * \iota_0^{-1}$ where both ι_k and ι_0 are completely multiplicative functions, then J_k is a totient.

Theorem 2.11:

J_k is multiplicative.

Proof:

Since $J_k = \iota_k * \mu$ where both ι_k and μ are multiplicative functions, then J_k is multiplicative.

Note that $J_1 = \iota * \mu = \phi$

Theorem 2.12:

$J_k(1) = 1$ and if $1 < n = \prod_{i=1}^{r} p_i^{e_i}$, then

$$J_k(n) = n^k \prod_{i=1}^{r} (1 - 1/p_i^k)$$

Proof:

$$J_k(1) = (\iota_k * \mu)(1) = \iota_k(1)\mu(1) = 1$$

For p prime and $e > 0$,

$$\begin{aligned} J_k(p^e) &= (\iota_k * \mu)(p^e) \\ &= \iota_k(1)\mu(p^e) + \iota_k(p)\mu(p^{e-1}) + \ldots + \iota_k(p^{e-1})\mu(p) \\ &\quad + \iota_k(p^e)\mu(1) \\ &= 0 + 0 + \ldots\ldots + p^{(e-1)k}(-1) + p^{ek} \\ &= -p^{(e-1)k} + p^{ek} \\ &= p^{ek}(1 - 1/p^k) \end{aligned}$$

so, if $1 < n = \prod_{i=1}^{r} p_i^{e_i}$,

$$\begin{aligned} J_k(n) = \prod_{i=1}^{r} J_k(p_i^{e_i}) &= p_1^{e_1k} \ldots p_r^{e_rk} \prod_{i=1}^{r}(1 - 1/p_i^k) \\ &= n^k \prod_{i=1}^{r}(1 - 1/p_i^k) \end{aligned}$$

Theorem 2.13:

For any positive integer n, $\sum_{d|n} J_k(d) = n^k$.

Proof:

By definition, $J_k(n) = \sum_{d|n} \mu(d)(n/d)^k$, thus by Möbius inversion theorem, $\sum_{d|n} J_k(d) = n^k$.

Theorem 2.14:

$J_k(n)$ equals the number of ordered k-tuples of integers $(x_1, x_2, \ldots, x_k)$ such that $1 \leq x_i \leq n$ for $i = 1, 2, \ldots, k$ and

$\gcd(x_1,x_2,\ldots x_k,n) = 1$.

To prove this theorem, we will make use of the following well known combinatorial principle:

Inclusion-exclusion principle

If $A_1 ,\ldots A_t$ are subsets of a finite set S then the number of elements of the set

$$|S \setminus (A_1 \cup A_2 \cup \ldots \cup A_t)| = |S| + \sum_{j=1}^{t} (-1)^j \sum_{1 \leq i_1 \leq \ldots \leq i_j \leq t} |(A_{i_1} \cap \ldots \cap A_{i_j})|$$

The proof of this formula can be found in [24].

Proof of theorem 2.14:

Let γ_k be defined by

$\gamma_k(n)$ = number of ordered k-tuples of integers $(x_1,\ldots,x_k)$ such that $1 \leq x_i \leq n$, $i = 1,2,\ldots,k$ and $\gcd(x_1,\ldots,x_k,n) = 1$.

Let $S = \{ (x_1,\ldots,x_k) \mid 1 \leq x_i \leq n,\ i = 1,2,\ldots,k \}$ and

$A_i = \{ (x_1,\ldots,x_k) \in S \mid p_i \mid \gcd(x_1,\ldots,x_k) \}$ where

$n = p_1^{e1} \ldots p_r^{er}$

If $(x_1 ,\ldots,x_k) \in A_i$, then $\gcd(x_1,\ldots,x_k ,n) \neq 1$, because each x_i , $i = 1,\ldots,k$ are multiples of p_i . Thus $\gamma_k(n) = | S \setminus (A_1 \cup A_2 \cup \ldots \cup A_r) |$.

Claim:

$| (A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_j}) | = (n/p_{i_1} \ldots p_{i_j})^k$, $1 \leq i_j \leq r$.

To prove the claim, we will look at special cases, that is when $i = 1$ and $i = 2$. From there, we can see that it works for all $1 \leq i_j \leq r$.

For $i = 1$,

$A_1 = \{ (x_1,\ldots,x_k) \in S \mid p_1 \mid \gcd(x_1,\ldots,x_k) \}$

$$= \{ (p_1,2p_1,\ldots.,(n/p_1)p_1) \text{ X } (p_1,2p_1,\ldots.,(n/p_1)p_1) \text{ X}\ldots.\text{X } (p_1,2p_1,\ldots.,(n/p_1)p_1) \}$$

$$= \{ (p_1 ,p_1 ,\ldots.,p_1), (p_1,2p_1 ,2p_1 ,\ldots 2p_1),\ldots.., ((n/p_1)p_1,(n/p_1)p_1,\ldots.,(n/p_1)p_1) \}$$

thus, $|A_1| = (n/p_1)^k$.

Now, we will look at $|A_1 \cap A_2|$

$$A_1 \cap A_2 = \{ (x_1,\ldots.,x_k) \in S \mid p_1 | \gcd(x_1,\ldots,x_k) \text{ and } p_2 | \gcd(x_1,\ldots,x_k) \}$$

$$= \{ (p_1p_2,2p_1p_2,\ldots,(n/p_1p_2)p_1p_2) \text{ X } (p_1p_2,2p_1p_2,\ldots,(n/p_1p_2)p_1p_2) \text{ X }\ldots\ldots\text{X } (p_1p_2,2p_1p_2,\ldots,(n/p_1p_2)p_1p_2) \}$$

$$= \{ (p_1p_2,p_1p_2,\ldots,p_1p_2), (p_1p_2,2p_1p_2,\ldots,2p_1p_2),\ldots, ((n/p_1p_2)p_1p_2,(n/p_1p_2)p_1p_2,\ldots..,(n/p_1p_2)p_1p_2) \}$$

thus $|A_1 \cap A_2| = (n/p_1p_2)^k$.

Therefore, in general,

$$|(A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_j})| = (n/p_{i_1}\ldots.p_{i_j})^k \quad , 1 \leq i_j \leq r.$$

Using the inclusion-exclusion principle,

$$\gamma_k(n) = n^k + \sum_{j=1}^{r} (-1)^j \sum_{1 \leq i_1 \leq \ldots. \leq i_j \leq r} (n/p_{i_1}\ldots\ldots p_{i_j})^k$$

$$= \sum_{d|n} (n/d)^k \mu(d)$$

$$= \sum_{d|n} d^k \mu(n/d)$$

$$= (\iota_k * \mu)(n)$$

$$= J_k(n)$$

Therefore, $\gamma_k = J_k$.

Now, we will give an example to illustrate the theorem and its proof.

Example:

Let $n = 6 = 2.3$, and $S = \{(x_1,x_2) \mid 1 \leq x_i \leq 6,\ i = 1,2\}$ then $A_1 = \{ (2,2),(2,4),(2,6),(4,2),(4,4),(4,6),(6,2),(6,4),$ $(6,6) \}$

$A_2 = \{ (3,3),(3,6),(6,3),(6,6) \}$

$A_1 \cup A_2 = \{ (2,2),(2,4),(2,6),(4,2),(4,4),(4,6),(6,2),(6,4),$ $(6,6),(3,3),(3,6),(6,3) \}$

Thus, $S \setminus (A_1 \cup A_2)$ are the ordered pairs that are not both multiples of 2 or 3. That is, the $\gcd(x_1,x_2,6) = 1$. Then, $\gamma_2(6) = | S \setminus (A_1 \cup A_2) | = 24$.

Also, $A_1 \cap A_2 = \{ (6,6) \}$, $| A_1 \cap A_2 | = 1$, and

$(n/p_1p_2)^2 = (6/2.3)^2 = 1$, thus

$| A_1 \cap A_2 | = (n/p_1p_2)^2$.

$$
\begin{aligned}
\text{Now, } J_2(6) &= \sum_{d \mid 6} \mu(d)(6/d)^2 \\
&= \mu(1)(6)^2 + \mu(2)(3)^2 + \mu(3)(2)^2 + \mu(6) \\
&= 36 - 9 - 4 + 1 \\
&= 24
\end{aligned}
$$

Therefore, $\gamma_2(6) = J_2(6)$.

Theorem 2.15:

Let $\{ F_k(n) \mid k \in Z \}$ be a set of nonzero completely multiplicative arithmetical functions such that

$F_k(n).F_j(n) = F_{k+j}\ (n)$ and let

$\Psi_k(n) = (\mu * F_k)(n)$.

Then, $F_k(n) = [F_j * (\Psi_{k-j} . F_j)](n)$.

Proof:

$$\begin{aligned}[F_j * (\Psi_{k-j} \cdot F_j)](n) &= \sum_{d|n} (\Psi_{k-j} \cdot F_j)(n/d)F_j(d) \\ &= \sum_{d|n} \Psi_{k-j} (n/d)F_j(n/d)F_j(d) \\ &= F_j(n) \sum_{d|n} \Psi_{k-j}(n/d) \\ &= F_j(n)(\iota_0 * \Psi_{k-j})(n) \\ &= F_j(n)[F_{k-j} (n)] \\ &= F_k(n)\end{aligned}$$

Corollary 2.16: (Gegenbauer)

$$(J_k * J_j^{-1})(n) = J_{k-j} (n) \iota_j(n)$$

Proof:

By definition, $J_k * \iota_j = (\mu * \iota_k) * \iota_j$

$$\begin{aligned} &= \iota_k * (\mu * \iota_j) \\ &= \iota_k * J_j \end{aligned}$$

hence, $J_k * J_j^{-1} = \iota_k * \iota_j^{-1}$. Then by substituting $F_k(n) = \iota_k(n)$ in theorem 2.15, we have

$J_{k-j} (n) = (\mu * \iota_{k-j})(n)$ and

$(J_k * J_j^{-1})(n) = (\iota_k * \iota_j^{-1})(n) = J_{k-j} (n) \iota_j (n).$

Also, $J_k * \sigma_j = (\mu * \iota_k) * (\iota_0 * \iota_j)$

$$\begin{aligned} &= (\mu * \iota_j) * (\iota_0 * \iota_k) \\ &= J_j * \sigma_k \end{aligned}$$

so, $J_k * J_j^{-1} = \sigma_k * \sigma_j^{-1}.$

Thus we get

Corollary 2.17: (Negoes)

$$(\sigma_k * \sigma_j^{-1})(n) = J_{k-j} (n) \iota_j(n).$$

Liouville's function

Definition 2.7:

We define Liouville's function $\lambda(n)$ as follows

$$\lambda(1) = 1$$

$$\lambda(n) = (-1)^{e_1+\ldots+e_r} \quad \text{if } n = \prod_{i=1}^{r} p_i^{e_i}$$

Theorem 2.18:

For every $n \geq 1$, we have

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

or equivalently $\lambda(n) = \sum_{d^2|n} \mu(n/d^2)$

moreover, $\lambda^{-1}(n) = |\mu(n)|$ for all n.

Proof:

Let $g(n) = \sum_{d|n} \lambda(d)$, then g is multiplicative, so we can compute $g(p^e)$ for p prime and $e > 0$.

$$g(p^e) = \sum_{d|p^e} \lambda(d)$$

$$= \lambda(1) + \lambda(p) + \ldots + \lambda(p^{e-1}) + \lambda(p^e)$$

$$= 1 + (-1) + (-1)^2 + \ldots + (-1)^{e-1} + (-1)^e$$

$$= \begin{cases} 0 & \text{if } e \text{ is odd} \\ 1 & \text{if } e \text{ is even} \end{cases}$$

so, if $n = \prod_{i=1}^{r} p_i^{e_i}$,

$$g(n) = \prod_{i=1}^{r} g(p_i^{e_i}) = \begin{cases} 0 & \text{if one of the } e_i \text{ is odd} \\ 1 & \text{if all } e_i \text{ are even} \end{cases}$$

This implies that

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

By Möbius inversion theorem,

$$\lambda(n) = \sum_{d|n}\mu(n/d)g(d) \quad \text{but} \quad g(d) = \begin{cases} 1 & \text{if } d \text{ is a square} \\ 0 & \text{otherwise} \end{cases}$$

hence, $\lambda(n) = \sum_{d^2|n}\mu(n/d^2)$

Now, let $\lambda * |\mu| = \epsilon$

$$(\lambda * |\mu|)(1) = \lambda(1)|\mu(1)| = 1$$

and for p prime, e > 0,

$$\begin{aligned}(\lambda * |\mu|)(p^e) &= \lambda(1)|\mu(p^e)| + \lambda(p)|\mu(p^{e-1})| \\ &\quad +\ldots+ \lambda(p^{e-1})|\mu(p)| + \lambda(p^e)|\mu(1)| \\ &= 0 + 0 +\ldots+ (-1)^{e-1}|(-1)| + (-1)^e \\ &= (-1)^{e-1} + (-1)^e \\ &= -(-1)^e + (-1)^e \\ &= 0\end{aligned}$$

since λ and μ are multiplicative , hence when $n = \prod_{i=1}^{r} p_i^{e_i}$, $(\lambda * |\mu|)(n) = 0$. Thus $\lambda^{-1}(n) = |\mu(n)|$

Theorem 2.19:

If $n = \prod_{i=1}^{r} p_i^{e_i}$, then

i) $\sum_{d|n}\mu(d)\lambda(d) = 2^r$

ii) $\sum_{d|n}\mu(d)\lambda(n/d) = (-1)^{e_1+\ldots+e_r}2^r = \lambda(n)2^r$

Proof:

i) For p prime and e > 0,

$$\sum_{d|p^e}\mu(d)\lambda(d) = \mu(1)\lambda(1) + \mu(p)\lambda(p) + \ldots + \mu(p^e)\lambda(p^e)$$
$$= 1 + (-1)(-1) + \ldots\ldots + 0$$
$$= 2$$

thus for $n = \prod_{i=1}^{r} p_i^{e_i}$,

$$\sum_{d|n}\mu(d)\lambda(d) = \underset{r \text{ times}}{2\ldots\ldots2} = 2^r$$

ii) For p prime, and e > 0,

$$\sum_{d|p^e}\mu(d)\lambda(p^e/d) = \mu(1)\lambda(p^e) + \mu(p)\lambda(p^{e-1}) + \ldots + \mu(p^e)\lambda(1)$$
$$= (-1)^e + (-1)(-1)^{e-1} + 0 + \ldots\ldots + 0$$
$$= (-1)^e + (-1)(-1)^{e-1}$$
$$= (-1)^e + (-1)^e$$
$$= 2(-1)^e$$

thus for $n = \prod_{i=1}^{r} p_i^{e_i}$,

$$\sum_{d|n}\mu(d)\lambda(n/d) = \prod_{i=1}^{r} 2(-1)^{e_i} = 2^r\ (-1)^{e_1+\ldots+e_r} = \lambda(n)2^r$$

The Mangoldt function

This arithmetic function is important in the study of problems concerning distribution of primes.

Definition 2.8:

For every integer $n \geq 1$, we define the Mangoldt function

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

Theorem 2.20:

If $n \geq 1$, we have

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

ii) $(\mu * \log)(n) = \Lambda(n)$

i.e. $\Lambda(n) = \sum_{d|n} \mu(d)\log(n/d) = -\sum_{d|n} \mu(d)\log(d)$

Proof:

i) If $n = 1$, $\log 1 = 0$ and $\sum_{d|1} \Lambda(d) = \Lambda(1) = 0$

Assume $n > 1$, let $n = \prod_{i=1}^{r} p_i^{e_i}$ then

$$\log n = \log \prod_{i=1}^{r} p_i^{e_i}$$

$$= \log p_1^{e_1} + \log p_2^{e_2} + \ldots\ldots + \log p_r^{e_r}$$

$$= \sum_{i=1}^{r} \log p_i^{e_i}$$

$$= \sum_{i=1}^{r} e_i \log p_i$$

Note that the only nonzero terms in the sum of $\sum_{d|n} \Lambda(d)$ are the divisors d in the form p_i^m for $m = 1,2,\ldots,e_i$ and $i = 1,2,\ldots,r$. Therefore,

$$\sum_{d|n} \Lambda(d) = \sum_{i=1}^{r} \sum_{m=1}^{e_i} \Lambda(p_i^m)$$

$$= \sum_{i=1}^{r} \sum_{m=1}^{e_i} \log p_i$$

$$= \sum_{i=1}^{r} e_i \log p_i$$

$$= \log n$$

ii) $(\mu * \log)(n) = [\mu * (\Lambda * \iota_0)](n)$

$$= [\mu * \iota_0 * \Lambda](n)$$

$$= [(\iota_0^{-1} * \iota_0) * \Lambda](n)$$

$$= [\epsilon * \Lambda](n)$$

$$= \Lambda(n)$$

From part i), log n = $\sum_{d|n} \Lambda(d)$

and by Möbius inversion theorem,

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

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

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

but, $\sum_{d|n} \mu(d)\log(n) = \log(n) \sum_{d|n} \mu(d)$

$$= \log n \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \neq 1 \end{cases}$$

$$= 0$$

hence, $\Lambda(n) = -\sum_{d|n} \mu(d)\log(d)$

CHAPTER 3

UNITARY PRODUCT OF ARITHMETIC FUNCTIONS

In this chapter, we will study one of many generalizations of the Dirichlet product, that is the unitary product of arithmetic function. Our treatment of the unitary product here will follow the pattern we already laid out for the Dirichlet product.

Definition 3.1:

A positive divisor d of the positive integer n is called a unitary divisor of n if $(d,n/d) = 1$.

We denote the fact that d is a unitary divisor of n by $d||n$.

We shall now prove some important properties of unitary divisors.

Lemma 3.01:

If $a||b$ and $b||c$, then $a||c$.

Proof:

By definition, $a||b$ implies $b = ax$ for some integer x and $(a,b/a) = 1$, and $b||c$ implies $c = by$ for some integer y and $(b,c/b) = 1$. Thus, $c = (ax)y = a(xy)$, and since $a|b$ then $(a, c/b) = 1$. Now, $(a,b/a) = 1$ and $(a,c/b) = 1$ implies $(a,bc/ab) = (a,c/a) = 1$. Therefore, $a||c$.

Definition 3.2:

Let n and m be two positive integers, with $n = \prod_{i=1}^{r} p_i^{e_i}$, and $m = \prod_{i=1}^{r} p_i^{f_i}$, e_i, $f_i \geq 0$. Then we define

$$<n,m> = \prod_{i=1}^{r} p_i^{\delta(e_i,f_i)} \text{ where } \delta(e,f) = \begin{cases} 0 \text{ if } e \neq f \\ e \text{ if } e = f \end{cases}$$

Lemma 3.02:

<n,m> is a unitary divisor of n and of m.

Proof:

Let $n = \prod_{i=1}^{r} p^{e_i}$ and $m = \prod_{i=1}^{r} p^{f_i}$. So, by definition, $n/<n,m> = (p^{e_1} \ldots . p^{e_r})/(p^{\delta(e_1,f_1)} \ldots p^{\delta(e_r,f_r)})$, but each $p^{\delta(e_i,f_i)}$ divides p^{e_i}, hence n/<n,m> is an integer which implies that <n,m>|n.

Similarly, $m/<n,m> = (p^{f_1} \ldots . p^{f_r})/(p^{\delta(e_1,f_1)} \ldots p^{\delta(e_r,f_r)})$ is an integer, thus <n,m>|m.

Now, we will show that (<n,m>,n/<n,m>) = 1 and (<n,m>,m/<n,m>) = 1.

Let $n = p_1^{e_1} \ldots p_k^{e_k} p_j^{e_j} \ldots p_r^{e_r}$ and $m = p_1^{f_1} \ldots p_k^{f_k} p_j^{f_j} \ldots p_r^{f_r}$. Then,

(<n,m>,n/<n,m>)

$= (p^{\delta(e_1,f_1)} \ldots p^{\delta(e_r,f_r)}, (p^{e_1} \ldots . p^{e_r})/p^{\delta(e_1,f_1)} \ldots p^{\delta(e_r,f_r)})$

$$= \begin{cases} (1, p_1^{e_1} \dots p_r^{e_r}) & \text{if } \delta(e_i, f_i) = 0 \\ & \text{for all } i = 1,\dots,r \\ (p_1^{e_1} \dots p_r^{e_r}, 1) & \text{if } \delta(e_i, f_i) = e \\ & \text{for all } i = 1,\dots,r \\ (p_1^{e_1} \dots p_k^{e_k}, p_j^{e_j} \dots p_r^{e_r}) & \text{if } \delta(e_i, f_i) = e \text{ for } i = 1,..,k \\ & \text{and } \delta(e_i, f_i) = 0 \text{ for } i = j,..,r \end{cases}$$

$$= 1$$

Similarly, $(\langle n,m\rangle, m/\langle n,m\rangle) = 1$.

Therefore, $\langle n,m\rangle || n$ and $\langle n,m\rangle || m$.

<u>Lemma 3.03:</u>

$a || \langle b,c\rangle$ if and only if $a || b$ and $a || c$.

<u>Proof:</u>

First, assume $a||b$ and $a||c$. Then

$a||b$ implies $b = ax$ for some integer x and $(a, b/a) = 1$ and $a||c$ implies $c = ay$ for some integer y and $(a, c/a) = 1$. Thus, $\langle b,c\rangle = \langle ax,ay\rangle = a\langle x,y\rangle$ implies $\langle b,c\rangle/a = \langle x,y\rangle$, hence $a|\langle b,c\rangle$.

Now, we have $(a,b/a) = (a,x) = 1$ and $(a,c/a) = (a,y) = 1$ hence, $(a,\langle x,y\rangle) = 1$, i.e. $(a,\langle b,c\rangle/a) = 1$.

Thus, $a||\langle b,c\rangle$.

Conversely, assume $a||\langle b,c\rangle$. Since $\langle b,c\rangle||b$ and $\langle b,c\rangle||c$ then by lemma 3.01, $a||b$ and $a||c$.

Lemma 3.04:

Let m and n be two relatively prime positive integers and $d||mn$, then $d = ab$ where $a||m$ and $b||n$.

Proof:

Let $(m,n) = 1$ and $d||mn$.

Let $m = \prod_{i=1}^{r} p_i^{e_i}$ and $n = \prod_{j=1}^{s} q_j^{f_j}$ where $p_i \neq q_j$ for all $i = 1,..,r$ and $j = 1,...s$. Since $d||mn$, then $d=(\prod_{i=1}^{r} p_i^{\alpha_i})(\prod_{j=1}^{s} q_j^{\beta_j})$ where $0 \leq \alpha_i \leq e_i$, $0 \leq \beta_j \leq f_j$. Take $a = \prod_{i=1}^{r} p_i^{\alpha_i}$ and $b = \prod_{j=1}^{s} q_j^{\beta_j}$. Thus $a|m$ and $b|n$.

Now, since $(d,mn/d) = (ab,mn/ab) = 1$, then $(ab)x + (mn/ab)y = 1$ for some integer x and y. Thus, $a(bx) + (m/a)(n/b)y = 1$ implies $(a,m/a) = 1$. Similarly, $b(ax) + (n/b)(m/a)y = 1$ implies $(b,n/b) = 1$.

Therefore, $d = ab$ where $a||m$ and $b||n$.

Definition 3.3:

The unitary product (or convolution) of two arithmetic funtions f and g is defined for all positive integers n by

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

Now, we are going to study some properties of the unitary product. Let $(\Delta, \circ)$ be the set of all real-valued arithmetic functions together with the unitary product.

Remark:

Note that the unitary product $(f \circ g)$ can be expressed as follows

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

Now, let d_1 be a unitary divisor of n. Thus, $d_1|n$ and $(d_1, n/d_1) = 1$; let $n/d_1 = d_2$, then $n = d_1d_2$ and $(d_1, n/d_1) = (d_1, d_1d_2/d_1) = (d_1, d_2) = 1$. So,

$$(f \circ g)(n) = \sum_{\substack{d_1d_2 = n \\ (d_1,d_2) = 1}} f(d_1)g(d_2)$$

where d_1 and d_2 run over all positive integers whose product is n and are relatively prime.

Lemma 3.05:

The unitary product is commutative and associative.

Proof:

The commutativity of unitary product is clear. Let f, g, $h \in \Delta$. We need to show that $(f \circ g) \circ h = f \circ (g \circ h)$. Let $F = f \circ g$, then,

$$[\,(f \circ g) \circ h\,](n) = (F \circ h)(n)$$
$$= \sum_{d||n} F(d)h(n/d)$$
$$= \sum_{\substack{d_1d_2 = n \\ (d_1,d_2) = 1}} F(d_1)h(d_2)$$
$$= \sum_{\substack{d_1d_2 = n \\ (d_1,d_2) = 1}} h(d_2) \quad \sum_{\substack{d_3d_4 = d_1 \\ (d_3,d_4) = 1}} f(d_3)g(d_4)$$
$$= \sum_{\substack{d_2d_3d_4 = n \\ (d_2,d_3,d_4) = 1}} f(d_3)g(d_4)h(d_2)$$

In the same way, if we let $G = g \circ h$,

$$\begin{aligned}[f \circ (g \circ h)](n) &= (f \circ G)(n) \\ &= \sum_{d \| n} f(d)G(n/d) \\ &= \sum_{\substack{d_1d_2 = n \\ (d_1,d_2) = 1}} f(d_1)G(d_2) \\ &= \sum_{\substack{d_1d_2 = n \\ (d_1,d_2) = 1}} f(d_1) \sum_{\substack{d_3d_4 = d_2 \\ (d_3,d_4) = 1}} g(d_3)h(d_4) \\ &= \sum_{\substack{d_1d_3d_4 = n \\ (d_1,d_3,d_4) = 1}} f(d_1)g(d_3)h(d_4)\end{aligned}$$

Hence, $(f \circ g) \circ h = f \circ (g \circ h)$ and hence the unitary product is associative.

Lemma 3.06:

For all $f \in \Delta$, we have

$$f \circ \epsilon = f \text{ , where } \quad \epsilon(n) = \begin{cases} 1 & \text{if } n = 1 \\ o & \text{if } n \neq 1 \end{cases}$$

Proof:

$(f \circ \epsilon)(n) = \sum_{d \| n} f(d)\,\epsilon(n/d) = f(n)$ since $\epsilon(n/d) = 0$ for all $d < n$ and $\epsilon(1) = 1$.

Thus the function ϵ is the identity for the unitary product.

Theorem 3.1:

$(\Delta, +, \circ)$ is a commutative ring with identity.

Proof:

It remains to show the distributive law. i.e, $f \circ (g + h) = (f \circ g) + (f \circ h)$.

$$\begin{aligned}
[\,f \circ (g + h)\,](n) &= \sum_{\substack{d_1d_2 = n \\ (d_1,d_2) = 1}} f(d_1)(g + h)(d_2) \\
&= \sum_{\substack{d_1d_2 = n \\ (d_1,d_2) = 1}} f(d_1)[g(d_2) + h(d_2)] \\
&= \sum_{\substack{d_1d_2 = n \\ (d_1,d_2) = 1}} [f(d_1)g(d_2) + f(d_1)h(d_2)] \\
&= \sum_{\substack{d_1d_2 = n \\ (d_1,d_2) = 1}} f(d_1)g(d_2) + \sum_{\substack{d_1d_2 = n \\ (d_1,d_2) = 1}} f(d_1)h(d_2) \\
&= [(f \circ g) + (f \circ h)](n)
\end{aligned}$$

Therefore, the distributive law is satisfied.

Recall in Chapter 1 that $N(\theta) = 0$ and for $f \neq \theta \in \Delta$, $N(f) = 1/k$ where k is the smallest positive integer for which $f(k) \neq 0$.

<u>Lemma 3.07:</u>

For all $f, g \in \Delta$ we have

i) $N(f \circ g) \leq N(f)N(g)$

ii) $N(f \circ g) = N(f)N(g)$ if $1/N(f)$ and $1/N(g)$ are relatively prime.

<u>Proof:</u>

Assume that neither f nor g is θ.

Let $N(f) = 1/k$ and $N(g) = 1/m$. By definition,

$f(d) \neq 0$ only if $d \geq k$ and

$g(d) \neq 0$ only if $d \geq m$. So,

$g(km/d) \neq 0$ only if $km/d \geq m$. i.e. when $k \geq d$.

Consider $(f \circ g)(km) = \sum_{d \| km} f(d)g(km/d)$

but the only time when $f(d) \neq 0$ and $g(km/d) \neq 0$ is when $d = k$, which implies that $(k,m) = 1$. Therefore,

$$(f \circ g)(km) = \sum_{d||km} f(d)g(km/d)$$

$$= \begin{cases} 0 & \text{if } (k,m) \neq 1 \\ f(k)g(m) & \text{if } (k,m) = 1 \end{cases}$$

i) $(f \circ g)(km) = 0$ implies that $N(f \circ g) \leq 1/km = N(f)N(g)$. Is there exist $h < km$ such that $(f \circ g)(h) \neq 0$? We will show that there doesn't exist such h, by contradiction.

Assume that there exists $h < km$ such that $(f \circ g)(h) \neq 0$. Then $(f \circ g)(h) = \sum_{d||h} f(d)g(h/d)$, but $f(d) \neq 0$ only if $d \geq k$ and $g(h/d) \neq 0$ only if $h/d \geq m$ which implies that $km > h \geq md$, thus $k \geq d$. Therefore, $f(d)g(h/d) \neq 0$ only if $d = k$, and since $h/d = h/k < m$, thus $g(h/k) = 0$. This implies $(f \circ g)(h) = f(k)g(h/k) = 0$ which is a contradiction.

Now, we will show the equality when $(k,m) = 1$.

ii) $(f \circ g)(km) = f(k)g(m)$ if $(k,m) = 1$ implies that $N(f \circ g) \geq N(f)N(g) = 1/km$. By similar argument used in lemma 1.03, $N(f \circ g) \not> N(f)N(g)$. Thus,

$$N(f \circ g) = N(f)N(g).$$

From Chapter 1, we find out that (D, +, *) forms an integral domain. However, (Δ, +, o) is not an integral domain. We will give an example that shows $f \neq \theta \in \Delta$, but $f \circ f = \theta$.

Example:

$$f(n) = \begin{cases} 1 & \text{if } n = 2 \\ 0 & \text{otherwise} \end{cases}$$

$(f \circ f)(n) = \sum_{d||n} f(d)f(n/d) \neq 0$ only if $d = 2$ and $n/d = 2$, and thus $(d,n/d) = 2 \neq 1$ which contradicts the definition of unitary product.

Particularly, $(f \circ f)(2) = \sum_{d||2} f(d)f(2/d)$

$$= f(1)f(2) + f(2)f(1)$$

$$= 0.$$

Therefore, $(\Delta, +, \circ)$ is not an integral domain.

Definition 3.4:

If for $f \in \Delta$, there exists a funtion $g \in \Delta$ such that $f \circ g = g \circ f = \epsilon$, then g is called the unitary inverse of f.

In the next lemma, we characterize unitary invertible functions and give a recursion formula for the inverse.

Lemma 3.08:

A function $f \in \Delta$ is unitary invertible if and only if $f(1) \neq 0$. This is equivalent to say f is invertible if and only if $N(f) = 1$. Moreover, the unitary inverse of f is given by

$$f^{-1}(1) = 1/f(1)$$

$$f^{-1}(n) = -1/f(1) \sum_{\substack{d||n \\ d < n}} f(n/d)f^{-1}(d) \quad \text{for } n > 1$$

Proof:

First, assume that $f \in \Delta$ has unitary inverse f^{-1} , then $f \circ f^{-1} = \epsilon$. In particular,

$$(f \circ f^{-1})(1) = \sum_{d||1} f(d)f^{-1}(1/d)$$

$$= f(1)f^{-1}(1) = \epsilon(1) = 1$$

hence, $f(1) \neq 0$.

Conversely, assume that $f(1) \neq 0$.

For $n = 1$, $(f \circ f^{-1})(1) = \sum_{d||1} f(d)f^{-1}(1/d)$

$$= f(1)f^{-1}(1)$$

$$= \epsilon(1)$$

$$= 1$$

thus, $f(1)f^{-1}(1) = 1$ which implies that $f^{-1}(1) = 1/f(1)$ since $f(1) \neq 0$.

Now, assume that the function values $f^{-1}(d)$ has been uniquely determined for all $d < n$.

Consider, $(f \circ f^{-1})(n) = \epsilon(n)$.

For $n \neq 1$, $(f \circ f^{-1})(n) = \sum_{\substack{d||n \\ d < n}} f(n/d)f^{-1}(d) = \epsilon(n) = 0$ and this can be written as $f(1)f^{-1}(n) + \sum_{\substack{d||n \\ d < n}} f(n/d)f^{-1}(d) = 0$.

If the values of $f^{-1}(d)$ are known for all divisors $d < n$ then $f^{-1}(n)$ is uniquely determined by

$$f^{-1}(n) = - 1/f(1) \sum_{\substack{d||n \\ d < n}} f(n/d)f^{-1}(d)$$

Theorem 3.2:

Let U be the set of units in Δ. i.e. $U = \{ f \in \Delta \mid f(1) \neq 0 \}$, then (U,o) is an abelian group.

Proof:

Let $f, g \in U$, then $(f \circ g)(1) = f(1)g(1) \neq 0$ since $f(1) \neq 0$ and $g(1) \neq 0$. Also, if $f \in U$, then $f^{-1} \in U$ follows immediately from lemma 3.08.

In chapter 1, we also find out that (D, +, *) is a unique factorization domain, but (Δ, +, o) is not. Before we give an example showing that (Δ, +, o) is not a unique factorization domain, we want to recall the definition of divisibility in an integral domain.

Definition 3.5:

Two elements a and b of a domain R are said to be associates if $a = b \circ u$ for some unit $u \in R$, and denoted by $a \sim b$.

Lemma 3.09:

If $f \in \Delta$ is such that $1/N(f) = p^{\alpha}$ where p is a prime and $\alpha \geq 1$, then f is irreducible.

Proof:

Let $f = g \circ h$. Since $N(f) = 1/p^{\alpha}$ then $f(p^{\alpha}) \neq 0$, and hence $(g \circ h)(p^{\alpha}) \neq 0$. Thus

$$(g \circ h)(p^{\alpha}) = \sum_{d \| p^{\alpha}} g(d)h(p^{\alpha}/d)$$

$$= g(1)h(p^{\alpha}) + g(p^{\alpha})h(1)$$
$$\neq 0$$

hence, at least one of the terms is nonvanishing. So, either $g(1) \neq 0$ or $h(1) \neq 0$. Therefore, either g or h is a unit.

In the next example we will show unique factorization does not hold in the ring (Δ, +, o).

Example:

Let $f(n) = \begin{cases} 1 & \text{if } n = 2,4,5 \\ 0 & \text{otherwise} \end{cases}$

$g(n) = \begin{cases} -1 & \text{if } n = 2 \\ 1 & \text{if } n = 5 \\ 0 & \text{otherwise} \end{cases}$

$h(n) = \begin{cases} 1 & \text{if } n = 4 \\ 0 & \text{otherwise} \end{cases}$

$z(n) = \begin{cases} 1 & \text{if } n = 5 \\ 0 & \text{otherwise} \end{cases}$

Thus $N(f) = 1/2$, $N(g) = 1/2$, $N(h) = 1/4$, $N(z) = 1/5$. Clearly, one can see that f and g are not associates to h and z; as an example, if we assume that f is associate to h, then by definition $f = h \circ u$ for some unit u, and $N(f) = N(h \circ u) = N(h)N(u) = N(h)$, which is not true.

Therefore, lemma 3.09 implies that f, g, h, and z are nonassociates irreducibles.

Now, we will show $f \circ g = h \circ z \neq \theta$.

$(f \circ g)(n) = \sum_{d||n} f(d)g(n/d)$, but $f(d) \neq 0$ only if $d = 2, 4$, or 5 and $g(n/d) \neq 0$ only if $n/d = 2$ or 5. Then since $(d, n/d) = 1$, we will choose $d = 4$ and $n/d = 5$, hence, $n = 20$. Thus,

$$\begin{aligned}(f \circ g)(20) &= \sum_{d||20} f(d)g(20/d) \\ &= f(4)g(5) \\ &= 1.\end{aligned}$$

Similarly, for $(h \circ z)(n) = \sum_{d||n} h(d)z(n/d)$, $h(d) \neq 0$ only if $d = 4$ and $z(n/d) \neq 0$ only if $n/d = 5$. Therefore, $n = 20$ and

$$\begin{aligned}(h \circ z)(20) &= \sum_{d||20} h(d)z(20/d) \\ &= h(4)z(5) \\ &= 1\end{aligned}$$

Hence, $f \circ g = h \circ z \neq \theta$, and thus $(\Delta, +, \circ)$ is not a unique factorization domain.

Similarly like $(D, +, *)$, $(\Delta, +, \circ)$ does not satisfy the descending chain condition for ideals.

Theorem 3.3:

$(\Delta, +, \circ)$ does not satisfy the descending chain condition for ideals.

Proof:

For k an integer, let Δ_k be the set of all functions

$f \in \Delta$ with $N(f) \leq 1/k$.

i.e. $\Delta_k = \{ f \in \Delta : f(n) = 0 \text{ if } n < k \}$

We want to show that

i) each Δ_k is an ideal of Δ

ii) $\Delta = \Delta_1 \supset \Delta_2 \supset \Delta_3 \supset$ ...... with each containment proper.

i) For each k, Δ_k is an ideal of Δ.

Let f, $g \in \Delta_k$. Then $f(n) = 0$ if $n < k$ and

$g(m) = 0$ if $m < k$.

Thus, $(f - g)(x) = f(x) - g(x) = 0$ if $x < k$. Therefore, $f - g \in \Delta_k$.

Now, let $f \in \Delta_k$ and $h \in \Delta$. We have

$$\begin{aligned} N(f \circ h) &\leq N(f)N(h) \\ &\leq (1/k)\, N(h) \\ &\leq 1/k \quad , \text{ since } N(h) \leq 1 \end{aligned}$$

thus $f \circ h \in \Delta_k$. Therefore Δ_k is an ideal of Δ.

ii) Now, $f \in \Delta_k$ implies that $f(n) = 0$ if $n < k$ and

$g \in \Delta_k$ implies that $g(n) = 0$ if $n < k-1$

thus $f \in \Delta_{k-1}$ and hence $\Delta_k \subset \Delta_{k-1}$

Now, define

$$h(n) = \begin{cases} 0 & \text{if } n < k - 1 \\ 1 & \text{if } n \geq k - 1 \end{cases}$$

thus $h \in \Delta_{k-1}$ but $h \notin \Delta_k$ since $h(k - 1) = 1$.

Hence, $\Delta_k \neq \Delta_{k-1}$

Next, we are going to study the behavior of multiplicative function under unitary product.

Theorem 3.4:

The unitary product of two multiplicative functions is a multiplicative function.

Proof:

Let f and g be two multiplicative functions and $h = f \circ g$. Let $(m,n) = 1$, then

$$\begin{aligned} h(mn) &= \sum_{d \| mn} f(d)g(mn/d) \\ &= \sum_{\substack{a \| m \\ b \| n}} f(ab)g(mn/ab) && \text{since } d \text{ can be written as } d = ab \text{ where } a \| m \text{ and } b \| n \\ &= \sum_{\substack{a \| m \\ b \| n}} f(a)f(b)g(m/a)g(n/b) && \text{since } (a,b) = 1 \text{ and } (m/a,n/b) = 1 \\ &= \sum_{a \| m} f(a)g(m/a) \sum_{b \| n} f(b)g(n/b) \\ &= h(m)h(n) \end{aligned}$$

hence h is multiplicative.

Theorem 3.5:

If f is multiplicative, then its unitary inverse f^{-1} is also multiplicative.

Proof:

We define a new multiplicative function g as follows: For every prime p and every $e > 0$, we let $g(p^e) = f^{-1}(p^e)$ and for $n = \prod_{i=1}^{r} p_i^{e_i}$, we define $g(n) = \prod_{i=1}^{r} g(p_i^{e_i})$. Clearly, g is multiplicative, hence $f \circ g$ is multiplicative.

Now, $$(f \circ g)(p^e) = \sum_{\substack{d_1d_2 = p^e \\ (d_1,d_2) = 1}} f(d_1)g(d_2)$$

$$= \sum_{\substack{d_1d_2 = p^e \\ (d_1,d_2) = 1}} f(d_1)f^{-1}(d_2)$$

$$= (f \circ f^{-1})(p^e)$$

$$= \epsilon(p^e)$$

Since $f \circ g = \epsilon$, thus $g = f^{-1}$ and f^{-1} is multiplicative.

Theorem 3.6:

The set of all multiplicative functions is an abelian group under unitary product.

Proof:

Let F be the set of all multiplicative functions. Then the commutativity and associativity holds since unitary product are both commutative and associative; ϵ is the identity; and from theorem 3.4 and 3.5, for any $f, g \in F$ $(f \circ g) \in F$ and $f^{-1} \in F$.

Corollary 3.7:

Let f, g, and h be arithmetic functions, and suppose $f \circ g = h$. If any two of the functions are multiplicative then so is the third.

Proof:

Let $h = f \circ g$. If f and g are multiplicative, then h is multiplicative by theorem 3.4. Assume that f and h are multiplicative, then $f \circ g = h$ implies that $f^{-1} \circ (f \circ g) = f^{-1} \circ h$, and $f^{-1} \circ h$ is multiplicative since f^{-1} is multiplicative by theorem 3.5. Similarly, when g and h are multiplicative, f is multiplicative.

Corollary 3.8:

If $g = f \circ \iota_0$, i.e. if $g(n) = \sum_{d||n} f(d)$, then g is multiplicative if and only if f is multiplicative. Moreover, $\sum_{d||n} f(d) = \prod_{i=1}^{r} (f(1) + f(p_i^{e_i}))$ where $n = \prod_{i=1}^{r} p_i^{e_i}$.

Proof:

First, assume that g is multiplicative. Then, $g = f \circ \iota_0$ implies that $g \circ \iota_0^{-1} = f \circ \iota_0 \circ \iota_0^{-1}$ and thus $f = g \circ \iota_0^{-1}$ is multiplicative since g and ι_0^{-1} are both multiplicative.

Conversely, assume that f is multiplicative. Then, $g = f \circ \iota_0$ is multiplicative.

Now, for p prime and and $e > 0$,

$$(f \circ \iota_0)(p^e) = \sum_{d||p^e} f(d)$$

$$= f(1) + f(p^e)$$

Thus, if $n = \prod_{i=1}^{r} p_i^{e_i}$,

$$(f \circ \iota_0)(n) = \prod_{i=1}^{r} [f(1) + f(p_i^{e_i})]$$

CHAPTER 4

THE UNITARY ANALOGUES OF SOME ARITHMETIC FUNCTIONS

Here, we introduce new arithmetical functions which may be regarded as the unitary analogues of some of the well-known classical functions. Among these functions, we have corresponding to the Euler ϕ-function, the unitary totient ϕ^* is introduced. The unitary analogue μ^* to the Möbius function μ is also defined. A unitary analogue of the Möbius inversion formula is also proved.

Definition 4.1:

Let $n = p_1^{e_1} \ldots p_r^{e_r}$ be the canonical factorization of n. We define $\omega(n) = r$ with $\omega(1) = 0$. Then $\omega(n)$ is the number of distinct prime divisors of n.

Number and sum of unitary divisors

Definition 4.2:

For positive integers n, we define the following functions:

i) $\tau^*(n)$ is the number of unitary divisors of n

ii) $\sigma^*(n)$ is the sum of unitary divisors of n

iii) $\sigma_k^*(n)$ is the sum of kth powers of unitary divisors of n where k is any real number.

Example:

As examples, we will find the values of $\tau^*(12)$,

$\sigma^*(12)$, and $\sigma_k^*(12)$. The unitary divisors of 12 are 1, 3, 4, and 12, thus

i) $\tau^*(12) = 4$

ii) $\sigma^*(12) = 1 + 3 + 4 + 12 = 20$

iii) $\sigma_k^*(12) = 1 + 3^k + 4^k + 12^k$

Note that $\tau^*(n)$ and $\sigma^*(n)$ are special cases of $\sigma_k^*(n)$ i.e. $\tau^*(n) = \sigma_0^*(n)$ and $\sigma^*(n) = \sigma_1^*(n)$. Also, in terms of the iota functions, they can be written as

i) $\tau^*(n) = (\iota_0 \circ \iota_0)(n)$

ii) $\sigma^*(n) = (\iota_0 \circ \iota)(n)$

iii) $\sigma_k^*(n) = (\iota_0 \circ \iota_k)(n)$

Theorem 4.1:

σ_k^* is multiplicative.

Proof:

Since the unitary product of two multiplicative functions is multiplicative, and $\sigma_k^* = \iota_0 \circ \iota_k$, hence σ_k^* is multiplicative.

Also, since τ^* and σ^* are special cases of σ_k^*, they are multiplicative.

Theorem 4.2:

If $n = \prod_{i=1}^{r} p_i^{e_i}$, $e_i > 0$, then

$$\sigma_k^*(n) = \begin{cases} 1 & \text{if } n = 1 \\ n^k \prod_{i=1}^{r} (1 + 1/p_i^{ke_i}) & \text{if } n > 1 \end{cases}$$

Proof:

$\sigma_k^*(1) = (\iota_0 \circ \iota_k)(1) = \iota_0(1)\ \iota_k(1) = 1.$

For p prime and e > 0,

$$\sigma_k^*(p^e) = (\iota_0 \circ \iota_k)(p^e)$$

$$= \sum_{d||p^e} \iota_0(d)\ \iota_k(p^e/d)$$

$$= \iota_0(1)\ \iota_k(p^e) + \iota_0(p^e)\ \iota_k(1)$$

$$= p^{ke} + 1$$

$$= 1 + p^{ke}$$

Since σ_k^* is multiplicative, then for $1 < n = \prod_{i=1}^{r} p_i^{e_i}$,

$$\sigma_k^*(n) = \prod_{i=1}^{r} (1 + p_i^{ke_i})$$

$$= n^k \prod_{i=1}^{r} (1 + 1/p_i^{ke_i})$$

Corollary 4.3:

If $1 < n = \prod_{i=1}^{r} p_i^{e_i}$, then

i) $\tau^*(n) = \prod_{i=1}^{r} 2 = 2^{\omega(n)}$

ii) $\sigma^*(n) = \prod_{i=1}^{r} (1 + p_i^{e_i})$

Proof:

i) $\tau^*(n) = \sigma_0^*(n) = \prod_{i=1}^{r} (1 + p_i^{(0)e_i})$

$$= \prod_{i=1}^{r} (1 + 1)$$

$$= \prod_{i=1}^{r} 2$$

$$= 2^{\omega(n)}$$

ii) $\sigma^*(n) = \sigma_1^*(n) = \prod_{i=1}^{r} (1 + p_i^{(1)e_i})$

$$= \prod_{i=1}^{r} (1 + p_i^{e_i})$$

The unitary Möbius function

Definition 4.3:

We define the unitary analogue of Möbius function $\mu^*(n)$ by

$$\mu^*(1) = 1 \quad \text{and} \quad \mu^*(n) = (-1)^{\omega(n)}$$

Theorem 4.4:

μ^* is multiplicative.

Proof:

Let $(m,n) = 1$, then $n = \prod_{i=1}^{r} p_i^{e_i}$ and $m = \prod_{j=1}^{s} q_j^{f_j}$, where $p_i \neq q_j$ for all $i = 1,\dots,r$; $j = 1,\dots,s$.

$$\begin{aligned} \text{Then } \mu^*(mn) &= (-1)^{\omega(mn)} \\ &= (-1)^{s+r} \\ &= (-1)^{s} \ (-1)^{r} \\ &= (-1)^{\omega(m)} \ (-1)^{\omega(n)} \\ &= \mu^*(m) \ \mu^*(n) \end{aligned}$$

Thus, μ^* is multiplicative.

Theorem 4.5:

$$\mu^* \circ \iota_0 = \epsilon \qquad \text{i.e.} \sum_{d\|n} \mu^*(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \neq 1 \end{cases}$$

Proof:

$$(\mu^* \circ \iota_0)(1) = \mu^*(1) \ \iota_0(1) = 1.$$

For p prime and $e > 0$,

$$(\mu^* \circ \iota_0)(p^e) = \sum_{d\|p^e} \mu^*(d) \ \iota_0(p^e/d)$$

$$= \mu^*(1) + \mu^*(p^e)$$

$$= 1 + (-1)$$

$$= 0.$$

Since μ^* is multiplicative, for $1 < n = \prod_{i=1}^{r} p_i^{e_i}$,

$(\mu^* \circ \iota_0)(n) = 0.$

Thus $\mu^* \circ \iota_0 = \epsilon$.

Theorem 4.6: (Möbius inversion theorem)

For all arithmetic functions f and g,

$$g = f \circ \iota_0 \text{ if and only if } f = \mu^* \circ g.$$

i.e. $g(n) = \sum_{d||n} f(d)$ if and only if $f(n) = \sum_{d||n} \mu^*(d)g(n/d)$

Proof:

First, assume that $g = f \circ \iota_0$, then

$$\begin{aligned}\mu^* \circ g &= \mu^* \circ (f \circ \iota_0) \\ &= \mu^* \circ (\iota_0 \circ f) \\ &= (\mu^* \circ \iota_0) \circ f \\ &= \epsilon \circ f \\ &= f\end{aligned}$$

Conversely, assume that $f = \mu^* \circ g$, then

$$\begin{aligned}f \circ \iota_0 &= (\mu^* \circ g) \circ \iota_0 \\ &= (g \circ \mu^*) \circ \iota_0 \\ &= g \circ (\mu^* \circ \iota_0) \\ &= g \circ \epsilon \\ &= g\end{aligned}$$

Theorem 4.7: (Generalized Möbius inversion theorem)

If f, g and h are arithmetic functions, and $h(1) \neq 0$

then, $g = f \circ h$ if and only if $f = g \circ h^{-1}$.

i.e. $g(n) = \sum_{d||n} f(d)h(n/d)$ if and only if $f(n) = \sum_{d||n} g(d)h^{-1}(n/d)$

Proof:

First, assume that $g = f \circ h$, then

$$\begin{aligned} g \circ h^{-1} &= (f \circ h) \circ h^{-1} \\ &= f \circ (h \circ h^{-1}) \\ &= f \circ \epsilon \\ &= f \end{aligned}$$

Conversely, assume that $f = g \circ h^{-1}$, then

$$\begin{aligned} f \circ h &= (g \circ h^{-1}) \circ h \\ &= g \circ (h^{-1} \circ h) \\ &= g \circ \epsilon \\ &= g \end{aligned}$$

Note that if $h = \iota_0$ in this theorem, then we have the classical Möbius inversion theorem.

The unitary ϕ_k^*-function

Definition 4.4:

For k a positive integer, we define the unitary ϕ_k^*-function by $\phi_k^* = \mu^* \circ \iota_k$ i.e. $\phi_k^*(n) = \sum_{d||n} \mu^*(d)(n/d)^k$

Since μ^* and ι_k are multiplicative, ϕ_k^* is multiplicative.

Corresponding to Euler ϕ-function, the unitary totient ϕ^* is a special case of ϕ_k^*. It is defined by

$\phi^* = \phi_1^* = \mu^* \circ \iota$ i.e. $\phi^*(n) = \sum_{d||n} \mu^*(d)(n/d)$

Theorem 4.8:

If $n = \prod_{i=1}^{r} p_i^{e_i}$, $e_i > 0$, then

$$\phi_k^*(n) = \begin{cases} 1 & \text{if } n = 1 \\ n^k \prod_{i=1}^{r} (1 - 1/p_i^{ke_i}) & \text{if } n > 1 \end{cases}$$

Proof:

$$\phi_k^*(1) = \sum_{d||1} \mu^*(d)(1/d)^k = \mu^*(1) = 1$$

For p prime and $e > 0$,

$$\phi_k^*(p^e) = \sum_{d||p^e} \mu^*(d)(p^e/d)^k$$

$$= \mu^*(1)(p^{ke}) + \mu^*(p^e)$$

$$= p^{ke} + (-1)$$

Since ϕ_k^* is multiplicative, then for $1 < n = \prod_{i=1}^{r} p_i^{e_i}$,

$$\phi_k^*(n) = \prod_{i=1}^{r} (p_i^{ke_i} - 1)$$

$$= n^k \prod_{i=1}^{r} (1 - 1/p_i^{ke_i})$$

Corollary 4.9:

$$\phi^*(n) = \phi_1^*(n) = \prod_{i=1}^{r} (p_i^{e_i} - 1)$$

Theorem 4.10:

$$\phi^* \circ \iota_0 = \iota \qquad \text{i.e.} \quad \sum_{d||n} \phi^*(d) = n$$

Proof:

$$\phi^* \circ \iota_0 = (\mu^* \circ \iota) \circ \iota_0$$

$$= (\mu^* \circ \iota_0) \circ \iota$$

$$= \epsilon \circ \iota$$

$$= \iota$$

Theorem 4.11:

Let $\{ F_k(n) \mid k \in Z \}$, be a set of nonzero multiplicative functions, such that $F_k(n).F_j(n) = F_{k+j}(n)$ and let $\Psi_k(n) = (\mu^* \circ F_k)(n)$, then

$$F_k(n) = [F_j \circ (\Psi_{k-j} F_j)](n).$$

Proof:

$$\begin{aligned}[F_j \circ (\Psi_{k-j} F_j)](n) &= \sum_{d||n} (\Psi_{k-j} F_j)(n/d) F_j(d) \\ &= \sum_{d||n} \Psi_{k-j}(n/d) F_j(n/d) F_j(d) \\ &= F_j(n) \sum_{d||n} \Psi_{k-j}(n/d) \\ &= F_j(n)[\iota_0 \circ \Psi_{k-j}](n) \\ &= F_j(n)[F_{k-j}(n)] \\ &= F_k(n)\end{aligned}$$

Corollary 4.12:

$$(\phi_k^* \circ \phi_j^{*-1})(n) = \phi^*_{k-j}(n) \quad \iota_j(n)$$

Proof:

By definition,

$$\begin{aligned}\phi_k^* \circ \iota_j &= (\mu^* \circ \iota_k) \circ \iota_j \\ &= \iota_k \circ (\mu^* \circ \iota_j) \\ &= \iota_k \circ \phi_j^*\end{aligned}$$

hence $\phi_k^* \circ \phi_j^{*-1} = \iota_k \circ \iota_j^{-1}$. Then by substituting $F_k(n) = \iota_k(n)$ in theorem 4.11, we have

$$\phi^*_{k-j}(n) = (\mu^* \circ \iota_{k-j})(n) \text{ and}$$

$$(\phi_k^* \circ \phi_j^{*-1})(n) = (\iota_k \circ \iota_j^{-1})(n) = \phi^*_{k-j}(n) \quad \iota_j(n).$$

Also,

$$\begin{aligned}\phi_k^* \circ \sigma_j^* &= (\mu^* \circ \iota_k) \circ (\iota_0 \circ \iota_j) \\ &= (\mu^* \circ \iota_j) \circ (\iota_0 \circ \iota_k) \\ &= \phi_j^* \circ \sigma_k^*\end{aligned}$$

so, $\phi_k^* \circ \phi_j^{*-1} = \sigma_k^* \circ \sigma_j^{*-1}$.

Thus we get

<u>Corollary</u> <u>4.13:</u>

$$(\sigma_k^* \circ \sigma_j^{*-1})(n) = \phi_{k-j}^*(n) \quad \iota_j(n)$$

SUMMARY AND CONCLUSION

The object of this paper has been to study arithmetic functions from an algebraic point of view. The emphasis has been on two ring structures on the set of arithmetic functions. This algebraic approach of studying arithmetic functions has the advantage that it leads to the development of many classical results in number theory without difficulties and unpleasant computational techniques.

As we have proven in chapter 1, the set of arithmetic functions with respect to ordinary addition and Dirichlet product forms a unique factorization domain. In this chapter, we also study some basic properties of multiplicative functions. Some of the important arithmetic functions of number theory, such as the iota functions, Mobius function, Euler totient function, and several other functions have been studied in chapter 2.

In chapter 3, we found out that contrary to Dirichlet product, the set of arithmetic functions with ordinary addition and unitary product is not an integral domain, and not a unique factorization domain. The unitary analogues of some of the arithmetic functions studied in chapter 2, have been discussed in chapter 4.

In conclusion, we suggest that the results of this paper could be extended in two ways. One way would be the extension of the Dirichlet and unitary convolutions to k-convolution [11, 14, 10], and then to determine the conditions under which the set of arithmetic functions has the structure of a ring or a unique factorization domain with respect to k-convolution. A second way would be to define k-convolution analogues of the well-known classical arithmetical functions and the study of their properties.

BIBLIOGRAPHY

[1] Apostol, Tom M. Introduction to Analytic Number Theory. New York: Springer-Verlag, 1976.

[2] Bell, E. T. "An Arithmetical Theory of Certain Numerical Functions." Univ. of Washington Publications in Mathematics 1, no. 1 (1915).

[3] ---. "An Outline of a Theory of Arithmetic Functions." Journal Indian Mathematics Society 17 (1928): 249-260.

[4] Carlitz, L. "Rings of Arithmetic Functions." Pacific Journal Mathematics 14 (1964): 1165-1171.

[5] ---. "Arithmetic Functions in an Unusual Setting." American Mathematics Monthly 73 (1966): 582-590.

[6] ---. "Arithmetical Functions in an Unusual Setting II." Duke Mathematics Journal 34 (1967): 757-759.

[7] Cashwell, E., and C. Everett. "The Ring of Number-Theoretic Functions." Pacific Journal of Mathematics 9 (1959): 975-985.

[8] ---. "Formal Power Series." Pacific Journal of Mathematics 13 (1963): 45-64.

[9] Cohen, E. "Arithmetical Functions Associated with the Unitary Divisors of an Integer." Mathematische Zeitschrift 74 (1960): 66-80.

[10] ---. "Unitary Products of Arithmetical Functions." Acta Arithimatica 7 (1961): 29-38.

[11] Davison, T. M. K. "On Arithmetic Convolutions." Canadian Mathematics Bulletin 9 (1966): 287-296.

[12] Dickson, Leonard E. History of the Theory of Numbers. 3 vols. New York: Chelsea Publishing Co., 1952.

[13] Fotino, Ingrid Popa. "Generalized Convolution Ring of Arithmetic Functions." Pacific Journal of Mathematics 61, no. 1 (1975): 103-116.

[14] Gioia, A. A. "The K-Product of Arithmetic Functions." Canadian Journal Mathematics 17 (1965): 970-976.

[15] Gioia, A. A., and Donald L. Goldsmith, eds. "The Theory of Arithmetic Functions." Proceedings of the Conference at Western Michigan University, April 29-May 1, 1971, no. 251. Lecture Notes in Mathematics: A Collection of Informal Reports and Seminars. Berlin: Springer-Verlag, 1972.

[16] Herstein, I. N. Abstract Algebra. New York: Macmillan, 1986.

[17] Jager, H. "The Unitary Analogues of Some Identities for Certain Arithmetical Functions." Koninkijke Nederlandse Akademie van Wetenschappen. Proceedings. Series A. Mathematical Science 64 (1961): 508-515.

[18] Mc Carthy, Paul J. Introduction to Arithmetic Functions. New York: Springer-Verlag, 1986.

[19] Niven, I., and Herbert S. Zuckerman. An Introduction to the Theory of Numbers. 4th ed. New York: John Wiley & Sons, 1980.

[20] Shapiro, H. N. "On the Convolution Ring of Arithmetic Functions." Communications on Pure and Applied Mathematics 25 (1972): 287-336.

[21] ---. Introduction to the Theory of Numbers. New York: John Wiley & Sons, 1983.

[22] Smith, David A. "Generalized Arithmetic Function Algebras." Gioia "The Theory of Arithmetic Functions." 205-245.

[23] Subbarao, M. V. "On Some Arithmetic Convolutions." Gioia "The Theory of Arithmetic Functions." 247-271.

[24] Tucker, Alan. Applied Combinatorics. New York: John Wiley & Sons, 1980.

[25] Vaidyanathaswamy, R. "The Theory of Multiplicative Arithmetic Functions." Trans American Mathematics Society 33 (1931): 579-662.

[26] Wall, Charles R. Selected Topics in Elementary Number Theory. Columbia, S. C.: Univ. of South Carolina Press, 1974.