The Theory of Multiplicative Arithmetical Functions

by

Karen T.I. Ho B.Sc.

A Thesis

submitted to the Faculty of Graduate Studies and Research

in partial fulfilment of the requirements for the

Degree of Master of Science

Department of Mathematics,

McGill University,

Montreal.

April 1967.

ACKNOWLEDGEMENT

I should like to express my utmost thanks to Professor H. Schwerdtfeger for the assisstance he has given me in the preparation of this thesis.

CONTENTS

Introduction

The theory of numbers, dated as early as the time of Pythagoras, is a branch of mathematics which, unexpectedly, has caught the interest on one extreme of nearly every noted mathematician and on the other of amateurs who show absolutely no interest at all in any other part of mathematics. On this account, the theory of numbers may be considered as a separate branch of mathematics. Indeed its development took place often independently of the development of other branches of mathematics.

In this thesis, we shall deal only with arithmetical functions which play a very important role in number theory in proving many of its identities, in setting up inversion formulas..... etc.

Chapter I is introductory in character. It deals with some of the fundamental concepts concerning arithmetical functions; it describes how they are defined and how their operations function.

Chapter II is devoted to the discussion of some of the most important and frequently used arithmetical functions with emphasis stressed on the Möbius function whose properties are developed in the third chapter.

The last chapter deals with " inversion ", one of the most important results on arithmetical functions. Here we introduce a few inversion formulas apart from the fundamental principle. However, for an account of the literature of the theory of inversion, one can refer to Dickson's " History of the Theory of Numbers " Vol. I pg 441 - 449.

CHAPTER I

CALCULUS OF MULTIPLICATIVE FUNCTIONS

Before going into the calculus of multiplicative arithmetical functions, we should get ourselves acquainted with some fundamental concepts of arithmetical functions.

Definition 1 : An arithmetical function $f(n)$ is defined as a function which takes a real (or complex) value for all integral values > 0 of its argument.

Definition 2:: A function $f(n)$ is called a numerical function of n if $f(1) \neq 0$, and if $f(n)$ takes a real (or complex) value for each non-zero positive integral value of its argument.

From the definitions given above, we note that by removing from the definition of a numerical function the restriction that the function shall not vanish when the argument is unity, we obtain the definition of an arithmetical function. The class of all arithmetical functions, therefore, includes that of all numerical functions. Hence, all the properties of the class of arithmetical functions also can be applied to the class of numerical functions.

Definition 3 : An arithmetical function $f(n)$ is called multiplicative if

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

whenever m is relatively prime to n .

Since unity is both prime to and a divisor of every number at the same time, thus by the definition of multiplicativity,

it is obvious that for any multiplicative function $f(n)$, $f(1) = 1$.

$\because$ $f(m) = f(m.1) = f(m)\, f(1)$

$\Rightarrow$ $f(1) = 1$

§ The elements of a multiplicative arithmetical function

In resolving the argument n of a multiplicative function $f(n)$ into their prime factors,

i.e. $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$ $\quad (p_1 < p_2 < \ldots\ldots < p_r)$

we then have

$$f(n) = \prod_{i=1}^{r} f(p_i^{\alpha_i})$$

By the element of the multiplicative function $f(n)$ to the base p_i, we shall mean the aggregate of values $f(p_i^{a})$ for all zero and positive integral values of a. Thus the elements of a multiplicative function completely determine the function.

Definition 4: The multiplicative function $f(n)$ will be called a linear function if the equation

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

holds not merely when m is relatively prime to n, but for all values of m, n.

Definition 5: A generating series of $f(n)$ to the base p_i is defined by

$$f_{(p_i)}(x) = \sum_{m=0}^{\infty} f(p_i^{m})\, x^m$$

Thus, the generating series to the base p of a linear function $f(n)$ is

$$f_{(p)}(x) = f(1) + f(p)\, x + f(p^2)\, x^2 + \ldots\ldots$$

$$f_{(p)}(x) = 1 + f(p)\,x + f(p^2)\,x^2 + \cdots\cdots$$

$$= 1 + f(p)\,x + \left[f(p)\right]^2 x^2 + \cdots\cdots$$

$$= \frac{1}{1 - ax} \quad , \qquad \text{if } f(p) = a$$

By using the generating series as the representative of the corresponding element of the function, it is then much more convenient in explaining the processes of the calculus we are going to discuss shortly.

§ Elementary functions

The elementary functions we are going to consider may be generally classified into four groups. They are all multiplicative.

A. The I - functions,

$$I_g(m) = m^g$$

B. The E - functions,

$$E_g(m) = g^{\nu}$$ where ν is the number of distinct prime factors of m.

Among the E - functions, those which occur most frequently are E_0 , E_1, E_{-1} and E_2. We shall simply write E for E_1. The function E_0 vanishes for all values of its argument, excepting unit value, for which it takes the value 1, i.e. $E_0(1) = 1$. The function $E = E_1$ takes the same value 1 for all values of its argument .

C. The λ - function,

$$\lambda_g(m) = g^{\nu}$$ where ν is the total number of prime factors of m.

Among the λ - functions, the most important is λ_{-1}, which we shall write simply as λ .

D. $\pi_g(m)$, $\epsilon_g(m)$ - functions,

$$\pi_g(m) = \begin{cases} 0 & \text{if} \quad a^g/m \quad (\ a > 0\ ) \\ 1 & \text{otherwise} \end{cases}$$

$$\epsilon_g(m) = \begin{cases} 1 & \text{if} \quad m = a^g \quad (\ a > 0\ ) \\ 0 & \text{otherwise} \end{cases}$$

§ The processes of the calculus

The calculus of multiplicative arithmetical functions consists of four processes. They are applicable to all arithmetical functions generally, but they have one common characteristic property — yielding only multiplicative functions when applied to multiplicative functions. The four processes are:

I. multiplication of functions

II. composition of functions

III. inversion of functions

IV. compounding of functions.

We shall consider the processes individually.

Multiplication

Let $f_1(n)$ and $f_2(n)$ be two multiplicative functions of n, their product denoted by

$$(f_1 \times f_2)(m) = f_1(n)\ f_2(n)$$

is again a multiplicative function of n.

The generating series of $(f_1 \times f_2)(n)$ to the base p thus is given by

$$(f_1 \times f_2)_{(p)}(x) = 1 + (\alpha_1 \beta_1)\, x + (\alpha_2 \beta_2)\, x^2 + \ldots$$

where $f_{1\,(p)}(x) = 1 + \alpha_1 x + \alpha_2 x^2 + \ldots\ldots$

and $f_{2\,(p)}(x) = 1 + \beta_1 x + \beta_2 x^2 + \ldots\ldots$

are the generating series of $f_1(n)$ and $f_2(n)$ to the base p, respectively.

It is clear that the multiplication thus defined is asso-ciative and commutative. For,

$$\begin{aligned}\left[(f_1 \times f_2)(n) \times f_3 \right](n) &= \left[f_1(n)\, f_2(n) \times f_3 \right](n) \\ &= f_1(n)\, f_2(n)\, f_3(n) \\ &= \left[f_1 \times f_2(n)\, f_3(n) \right](n) \\ &= \left[f_1 \times (f_2 \times f_3) \right](n)\end{aligned}$$

and $$\begin{aligned}(f_1 \times f_2)(n) &= f_1(n)\, f_2(n) \\ &= f_2(n)\, f_1(n) \\ &= (f_2 \times f_1)(n)\end{aligned}$$

If we take for f_2 the elementary function $E_g(n)$ and if the generating series of $f_1(n)$ to any base p (a prime) is given by

$$f_{1(p)}(x) = 1 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + \ldots\ldots$$

we then have

$$(f_1 \times E_g)_{(p)}(x) = 1 + (\alpha_1 g)x + (\alpha_2 g)x^2 + (\alpha_3 g)x^3 + \ldots\ldots$$

as

$$\begin{aligned}E_{g(p)}(x) &= 1 + E_g(p)\, x + E_g(p^2)\, x^2 + E_g(p^3)\, x^3 + \ldots\ldots \\ &= 1 + g x + g x^2 + g x^3 + \ldots\ldots\end{aligned}$$

In particular, when $g = 1$,

$$(f_1 \times E)_{(p)}(x) = 1 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + \ldots$$

$$= f_{1\,(p)}(x)$$

$$\therefore (f_1 \times E)(n) = f_1(n)$$

when $g = 0$,

$$(f_1 \times E_0)_{(p)}(x) = 1 + (\alpha_1 \cdot 0)\, x + (\alpha_2 \cdot 0)\, x^2 + \ldots.$$

$$= 1$$

as

$$E_{0\,(p)}(x) = E_0(1) + E_0(p)\, x + E_0(p^2)\, x^2 + \ldots.$$

$$= 1 + 0 + 0 + \ldots\ldots$$

$$= 1$$

$$\therefore (f_1 \times E_0)(n) = E_0(n)$$

Thus, E and E_0 behave just like unity and zero, with respect to multiplication here.

Composition

E. T. Bell [4] has termed this as " ideal multiplication" in order to distinguish it from the ordinary multiplication of functions.

By the composition of two arithmetical functions f_1 and f_2, we shall mean the process of forming the function defined by

$$f(n) = \sum_{d/n} f_1(d)\; f_2\left(\frac{n}{d}\right)$$

We shall denote f by $f_1 \cdot f_2$ and call it the composite of f_1 and f_2.

The generating series of the composite $(f_1 \cdot f_2)(n)$ to the base p is given by

$$(f_1 \cdot f_2)_{(p)}(x) = f_{1(p)}(x) \times f_{2(p)}(x)$$

the product of the generating series of f_1 and f_2 to the same base p.

The function E_0 plays a special role in composition. We have

$$f \cdot E_0 = f$$

$$E_0^k = \underbrace{E_0 \cdot E_0 \cdot \ldots \cdot E_0}_{k \text{ times}} = E_0$$

Since the generating series of E_0 to any base is 1. In multiplication, we have seen that E_0 behaves like a zero element. So here $f \cdot E_0 = f$ suggests that composition can be considered analogous to addition, again with E_0 behaving as a zero element. Like addition, composition is associative and commutative, but unlike addition, it is not distributive unrestrictedly with multiplication. However, it has a restricted distributivity described by

Theorem 1 Multiplication is distributive with composition if the multiplier is a linear function.

Proof : Let the multiplier be $\varphi(n)$, a linear function.

$$\left[(\varphi \times f_1) \cdot (\varphi \times f_2)\right](n) = \sum_{d/n} \varphi(d)\, f_1(d)\, \varphi\left(\frac{n}{d}\right) f_2\left(\frac{n}{d}\right)$$

$$= \sum_{d/n} \varphi(n)\, f_1(d)\, f_2\left(\frac{n}{d}\right)$$

(by definition of linear function)

$$= \left[\varphi \times (f_1 \cdot f_2)\right](n)$$

Inversion

The inverse $f^{-1}(n)$ of $f(n)$ is defined as the function such that

$$(f \cdot f^{-1})(n) = E_0(n)$$

Since every generating series of $E_0(n)$ is equal to 1, we can say that

$$f_{(p)}(x) \times f_{(p)}^{-1}(x) = 1$$

where $f_{(p)}(x)$ and $f_{(p)}^{-1}(x)$ are the generating series of $f(n)$ and $f^{-1}(n)$ to the base p, respectively.

Moreover, if $f_1 \cdot f_2 = f_3 \cdot f_4$, by performing composition by f_4^{-1} on both sides,

i.e. $$f_1 \cdot f_2 \cdot f_4^{-1} = f_3 \cdot f_4 \cdot f_4^{-1}$$

we have

$$f_1 \cdot f_2 \cdot f_4^{-1} = f_3 \cdot E_0 = f_3$$

Theorem 2 Composition is distributive with inversion, that is, the inverse of the composite of any two arithmetical functions is equal to the composite of their inverses.

Proof:

The generating series to base p of the inverse of the composite of f_1, f_2 is

$$\left[f_{1(p)}(x) \times f_{2(p)}(x) \right]^{-1},$$

and the generating series to the same base p of the composite of their inverses is

$$\left[f_{1(p)}(x)^{-1} \times f_{2(p)}(x)^{-1} \right] .$$

$$\because \left[f_{1(p)}(x) \times f_{2(p)}(x) \right]^{-1} = \left[f_{1(p)}(x)^{-1} \times f_{2(p)}(x)^{-1} \right]$$

$$\left[f_1 \cdot f_2 \right]^{-1} = f_1^{-1} \cdot f_2^{-1}$$

Thus the theorem is proved .

From theorem 2, it follows also that

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

$$f^{m+n} = f^m \cdot f^n$$

(m , n can be positive or negative integers)

Another important property of inversion is given by

Theorem 3 The inverse of $\varphi \times f$ is $\varphi \times f^{-1}$, if φ is a linear function.

Proof : $(\varphi \times f) \cdot (\varphi \times f^{-1}) = \varphi \times (f \cdot f^{-1})$ (by theorem 1)

$$= \varphi \times E_0$$

$$= E_0$$

Thus the inverse of any linear function φ is $\varphi \times E^{-1}$, as φ can be written as the product $\varphi \times E$.

The theory of inversion will be discussed in more detail in chapter 3 .

Compounding :

The compound of two multiplicative functions $f_1(n)$ and $f_2(n)$, denoted by $f_1 \oplus f_2$ is defined as follows,

$$(f_1 \oplus f_2)(n) = \sum f_1(\delta) \; f_2\left(\frac{n}{\delta}\right)$$

with the summation runs through all those divisors δ of n such that δ and $\frac{n}{\delta}$ are relatively prime to each other.

Let the generating series of f_1 and f_2 be written in the form

$$f_{1(p)}(x) = 1 + \alpha_1 x + \alpha_2 x^2 + \ldots\ldots$$

$$f_{2(p)}(x) = 1 + \beta_1 x + \beta_2 x^2 + \ldots\ldots$$

It follows that the generating series of the compound $f_1 \oplus f_2$ is as follows

$$(f_1 \oplus f_2)_{(p)}(x) = 1 + (\alpha_1 + \beta_1) x + (\alpha_2 + \beta_2) x^2 + \ldots$$

Thus the generating series of a compound is equal to the sum of the generating series, to the same base, of the functions compounded, except for the constant term, which is equal to 1 , as is always the case with all multiplicative functions.

Clearly the process of compounding is associative and commutative, since addition is so in the generating series of the functions compounded.

Theorem 4

Multiplication is distributive with compounding.

Proof : The distributive property can be established by means of the generating series. Now, suppose the generating series of f_1 , f_2 and ϕ , to the base p, are

$$f_{1\,(p)}(x) = 1 + \alpha_1 x + \alpha_2 x^2 + \ldots\ldots$$

$$f_{2\,(p)}(x) = 1 + \beta_1 x + \beta_2 x^2 + \ldots\ldots$$

$$\phi_{(p)}(x) = 1 + \gamma_1 x + \gamma_2 x^2 + \ldots\ldots$$

respectively.

$$\left[(\phi \times f_1) \oplus (\phi \times f_2)\right]_{(p)}(x) = 1 + (\gamma_1\alpha_1 + \gamma_1\beta_1)x + (\gamma_2\alpha_2 + \gamma_2\beta_2)x^2 + \ldots\ldots$$

which is actually the same as

$$\left[\phi \times (f_1 \oplus f_2)\right]_{(p)}(x) = 1 + \gamma_1(\alpha_1 + \beta_1)x + \gamma_2(\alpha_2 + \beta_2)x^2 + \ldots\ldots$$

$$= 1 + (\gamma_1\alpha_1 + \gamma_1\beta_1)x + (\gamma_2\alpha_2 + \gamma_2\beta_2)x^2 + \ldots\ldots$$

$$\therefore \phi \times (f_1 \oplus f_2) = (\phi \times f_1) \oplus (\phi \times f_2)$$

Theorem 5

$$\phi \cdot (f_1 \oplus f_2) = \left[(\phi \cdot f_1) \oplus (\phi \cdot f_2)\right] \oplus (E_{-1} \times \phi)$$

Proof :

$$\left[\phi \cdot (f_1 \oplus f_2)\right]_{(p)}(x)$$

$$= \phi_{(p)}(x) \times \left[f_{1\,(p)}(x) + f_{2\,(p)}(x) - 1\right]$$

$$= \phi_{(p)}(x) \times f_{1\,(p)}(x) + \phi_{(p)}(x) \times f_{2\,(p)}(x) - \phi_{(p)}(x)$$

$$= (\phi \cdot f_1)_{(p)}(x) + (\phi \cdot f_2)_{(p)}(x) + (E_{-1} \times \phi)_{(p)}(x) - 2$$

$$\sim (\phi \cdot f_1)_{(p)}(x) + (\phi \cdot f_2)_{(p)}(x) + (E_{-1} \times \phi)_{(p)}(x)$$

$$\therefore \phi \cdot (f_1 \oplus f_2) = \left[(\phi \cdot f_1) \oplus (\phi \cdot f_2) \right] \oplus (E_{-1} \times \phi)$$

This theorem is fundamental and can be generalized to the case where there are more than two functions in question.

i.e.

$$\phi \cdot (f_1 \oplus f_2 \oplus \ldots\ldots \oplus f_t)$$
$$= \sum_{i=1}^{t} (\phi \cdot f_i) \oplus (E_{1-t} \times \phi)$$

where $\sum_{i=1}^{t} (\phi \cdot f_i)$ denotes

$$(\phi \cdot f_1) \oplus (\phi \cdot f_2) \oplus \ldots\ldots \oplus (\phi \cdot f_t)$$

Definition 6 The conjugate function of $f(n)$, denoted by conj $f(n)$ is defined as follows

$$f(n) \oplus \text{conj } f(n) = E_0(n)$$

or alternatively, conj $f(n)$ can be defined by

$$\text{conj } f(n) = f(n) \times E_{-1}(n)$$

For, if the generating series of $f(n)$ to the base p is

$$f_{(p)}(x) = 1 + \alpha_1 x + \alpha_2 x^2 + \ldots\ldots$$

owing to the fact that $E_{0\,(p)}(x) = 1$, the generating series of conj $f(n)$ to the same base p os obviously equal to

$$1 - \alpha_1 x - \alpha_2 x^2 - \ldots\ldots$$

which is the same as the generating series of $f(n) \times E_{-1}(n)$, as

$$E_{-1\,(p)}(x) = E_{-1}(0) + E_{-1}(p)\, x + E_{-1}(p^2)\, x^2 + \ldots\ldots$$
$$= 1 - x - x^2 - x^3 - \ldots\ldots$$

The conjugate function has evidently the following properties:

I. conj conj $f(n) = f(n)$

Proof:

$$\text{conj conj } f(n) = \text{conj } f(n) \times E_{-1}(n)$$

$$= f(n) \times E_{-1}(n) \times E_{-1}(n)$$

$$\because E_{-1}(n) = \begin{cases} 1 & \text{if } n \text{ has an even number of different prime factors of } n. \\ -1 & \text{if } n \text{ has an odd number of different prime factors of } n. \end{cases}$$

So, in both cases

$$E_{-1}(n) \times E_{-1}(n) = 1$$

$$\therefore \text{conj conj } f(n) = f(n)$$

II. $\text{conj } (f_1 \times f_2) = (\text{conj } f_1) \times f_2 = f_1 \times (\text{conj } f_2)$

Proof : $\text{conj } (f_1 \times f_2) = (f_1 \times f_2) \times E_{-1}$

$$(\text{conj } f_1) \times f_2 = (f_1 \times E_{-1}) \times f_2$$

$$f_1 \times (\text{conj } f_2) = f_1 \times (f_2 \times E_{-1})$$

Since multiplication is commutative and associative,

$\therefore$ they are all equal .

III. $\text{conj } (f_1 \oplus f_2) = \text{conj } f_1 \oplus \text{conj } f_2$

Proof : $\text{conj } (f_1 \oplus f_2) = (f_1 \oplus f_2) \times E_{-1}$ ..... (1)

Since multiplication is distributed by compounding , which has been proved formerly , $\therefore$ (1) has become

$$= (f_1 \times E_{-1}) \oplus (f_2 \times E_{-1})$$

$$= \text{conj } f_1 \oplus \text{conj } f_2$$ (by definition of conjugate function)

We conclude this chapter by giving a few lemmas on multiplicative functions, which will be useful in the later development of this thesis. The proofs of the first two lemmas are too trivial to be written out, so we just state them without giving proofs.

Lemma 1 Given that $f(n)$ is a multiplicative function.

Then $$f(1) = 0 \Rightarrow f(n) = 0 \text{ for all } n$$

and

$$f(1) \neq 0 \Rightarrow f(1) = 1$$

Lemma 2 If $f(n)$ is an arithmetical function such that

$$\sum_{d/n} f(d) = 0 \quad \text{for all } n$$

then $f(n) = 0$ for all n

Lemma 3 If $f(n)$ is a multiplicative function and

$$F(n) = \sum_{d/n} f(d)$$

then $F(n)$ is also multiplicative.

Proof : Suppose $(m, n) = 1$; and m and n can be resolved in the following manner such that

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

$$n = q_1^{\beta_1} q_2^{\beta_2} \cdots\cdots q_s^{\beta_s}$$

where the α's and β's are positive integers, and the p's and q's are distinct primes. The positive divisors d_1 of m are just the numbers $d_i = p_1^{\gamma_1} p_2^{\gamma_2} \cdots\cdots p_r^{\gamma_r}$

for all possible choices of the γ's with $0 \leq \gamma_i \leq \alpha_i$.

Similarly the positive divisors d_2 of n are such that

$$d_2 = q_1^{\delta_1} q_2^{\delta_2} \cdots\cdots q_s^{\delta_s}$$

where $0 \leq \delta_i \leq \beta_i$.

Hence as d_1 runs through all positive divisors of m, d_2 runs through all positive divisors of n, their product $d_1 d_2$ runs through the values

$$d = d_1 d_2 = p_1^{\gamma_1} p_2^{\gamma_2} \cdots\cdots p_r^{\gamma_r} q_1^{\delta_1} q_2^{\delta_2} \cdots\cdots q_s^{\delta_s}$$

where $0 \leq \gamma_i \leq \alpha_i$, $0 \leq \delta_i \leq \beta_i$.

But since $(m,n) = 1$, therefore the values d are just all the positive divisors of $mn = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$.

i.e. $$\sum_{d_1/m} \sum_{d_2/m} f(d_1, d_2) = \sum_{d/mn} f(d)$$

Clearly $(d_1, d_2) = 1$, we then have

$$\begin{aligned} F(mn) &= \sum_{d/mn} f(d) \\ &= \sum_{d_1/m} \sum_{d_2/n} f(d_1 d_2) \\ &= \sum_{d_1/m} \sum_{d_2/n} f(d_1) f(d_2) , \quad (\text{by the multiplicativity of } f(m)) \\ &= \sum_{d_1/m} f(d_1) \sum_{d_2/n} f(d_2) \\ &= F(m) F(n) \end{aligned}$$

CHAPTER II

SOME IMPORTANT ARITHMETICAL FUNCTIONS

In this chapter, we shall deal with some important, frequently used arithmetical functions and discuss their properties.

§ τ-function $\tau(n)$

Definition 1: $\tau(n)$ is defined as the number of different positive divisors of n.

It can be written in the form

$$\tau(n) = \sum_{d/n} 1$$

Obviously, by use of lemma 3 of Chapter I, we can prove easily that $\tau(n)$ is multiplicative. Since $\tau(n) = \sum_{d/n} 1$ is of the form $\sum_{d/n} f(d)$ and since $f(n) = 1$ is multiplicative, thus it implies that $\tau(n)$ is multiplicative also.

The following is a very fundamental theorem on $\tau(n)$, seen in almost every text book of the theory of numbers.

Theorem 1: If $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$, then

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

Proof: Since p_i's are the primes,

$$\therefore \tau(p_i) = 1 + 1$$

$$\tau(p_i^{\alpha_i}) = \alpha_i + 1$$

where the $\alpha_i + 1$ positive divisors of $p_i^{\alpha_i}$ are $1, p_i, p_i^2, \ldots, p_i^{\alpha_i}$.

Since $\tau(n)$ is multiplicative,

$$\therefore \tau(n) = \tau(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r})$$

$$= \prod_{i=1}^{r} \tau(p_i^{\alpha_i})$$

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

Some identities involving $\tau(n)$

I. $$\tau(n) = n - \sum_{h=1}^{n-1} t(n-h, h)$$

Before proving the stated identity, some definitions and lemmas have to be introduced.

Definition 2: $t(n-h, h)$ is defined to be the number of divisors of $n-h$, of which all are greater than h with n, h being integers and $n > h \geq 0$.

Definition 3: $$A(n,x) = \begin{cases} 1 & \text{if } n \equiv 0 \pmod{x} \\ 0 & \text{if } n \not\equiv 0 \pmod{x} \end{cases}$$

where n, x are both positive integers.

From the definitions above, we can see that $t(n,0) = \tau(n)$, and

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

$$= t(n+1, 0)$$

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

$$\Rightarrow \sum_{x=1}^{n} A(n+1, x) = t(n+1, 0) - 1 \qquad \ldots\ldots\ldots(1)$$

Lemma 1: $t(n-h, h) = t(n+1 - (h+1), h+1) + A(n+1, h+1)$

Proof: From the definitions given above, it is seen that

$$t(n-h, h) = t(n-h, h+1) + A(n-h, h+1)$$

or $$t(n-h, h) = t(n+1 - (h+1), h+1) + A(n-h, h+1)$$

$\because$ $$n-h \equiv n+1 \mod(h+1)$$

and by the property that

$$n \equiv n' \mod x,$$

implies $A(n, x) = A(n', x)$, (trivial from the definition of $A(n, x)$).

we can write

$$t(n-h, h) = t(n+1 - (h+1), h+1) + A (n+1, h+1)$$

Lemma 2:

$$n = \sum_{h=0}^{n-1} t(n-h, h) \quad \ldots\ldots\ldots(2)$$

Proof:
We proceed to prove by mathematical induction.

When n=1, (2) is seen to be true

as $1 = t(1, 0)$

Now, assume (2) is true when n=k,

i.e. $$k = \sum_{h=0}^{k-1} t(k-h, h) \quad \ldots\ldots\ldots(3)$$

If we can prove that (3) implies

$$k+1 = \sum_{h=0}^{k} t(k+1-h, h)$$

then the proof of this lemma is complete.

By putting a summation sign over the result of lemma1, we have

$$\sum_{h=0}^{k-1} t(\, k-h,\, h\,) = \sum_{h=0}^{k-1} t(\, k+1-(h+1),\, h+1\,) + \sum_{h=0}^{k-1} A(\, k+1,\, h+1\,)$$

Here, put $h+1 = x$, and substitute (3) in, we get

$$k = \sum_{x=1}^{k} t(\, k+1-x,\, x\,) + \sum_{x=1}^{k} A(\, k+1,\, x\,)$$

$$= \sum_{x=1}^{k} t(\, k+1-x,\, x\,) + t(\, k+1,\, 0\,) - 1 \qquad (\text{by (1)})$$

$$k+1 = \sum_{x=0}^{k} t(\, k+1-x,\, x\,)$$

Thus the lemma is proved.

Now, we come to the proof of the above stated identity on $\tau(n)$ itself.

Proof: From lemma 2,

$$n = \sum_{h=0}^{n-1} t(\, n-h,\, h\,)$$

$$= \sum_{h=1}^{n-1} t(\, n-h,\, h\,) + t(\, n,\, 0\,)$$

$\because\ t(\, n,\, 0) = \tau(n)$

$$\therefore\ \tau(n) = n - \sum_{h=1}^{n-1} t(\, n-h,\, h\,)$$

Checking the validity of this identity, we can substitute $n = 23$ in as an example,

$$\tau(23) = 23 - \sum_{h=1}^{22} t(\, 23-h,\, h\,)$$

$$\tau(23) = 23 - \left[t(22, 1) + t(21, 2) + \ldots\ldots + t(12, 11) \right]$$
$$= 23 - \left[3+3+4+1+3+1+2+1+1+1+1 \right]$$
$$= 23 - 21$$
$$= 2$$

which is actually the number of divisors of 23.

II. $\tau \cdot E_2 = \tau \times \tau$ .....(4)

$\tau \times \tau(n)$ is the number of divisor-pairs of n. Let r_1, r_2 be two divisors of n, $m = [r_1, r_2]$ be the least common multiple and $g = (r_1, r_2)$ be the greatest common divisor. We now try to group the divisor-pairs in such a manner that, for every group, $\frac{m}{g}$ is a fixed divisor r of n. Obviously, for each group, g is an arbitrary divisor of $\frac{n}{r}$ while r_1, r_2 must be of the form gm_1, gm_2, where $m_1 m_2 = r$ and $(m_1, m_2) = 1$. Thus the number of divisor pairs in the group specified by r is $\tau(\frac{n}{r}) E_2(r)$

$\therefore \quad \tau \cdot E_2 = \tau \times \tau$

III. $\tau(n) = \sum \left[\tau(r) \right]^2 \lambda(\frac{n}{r}) E_2(\frac{n}{r})$

Before proving this, we have to derive a few other relations first.

$$E_2 = E.\lambda^{-1} \quad .....(5)$$

To prove (5), we note that $E.\lambda^{-1}(n)$ enumerates all the divisors of n which contain no squared factor, thus is equal to $E_2(n)$. (by definition of E_2).

$$E_2 \times \lambda = E_2^{-1} \quad .....(6)$$

The relation (6) is a consequence of (5). For,

$$E_2 \times \lambda = \lambda \times (E.\lambda^{-1}) \qquad (\text{ by (5) })$$
$$= (\lambda \times E) \,.\, (\lambda \times \lambda^{-1}) \qquad (\text{ by theorem 1 of Chapter I })$$
$$= \lambda \,.\, (\lambda \times \lambda^{-1})$$
$$= \lambda \,.E^{-1}$$
$$= E_2^{-1} \qquad (\text{ by the distributive property of inversion by composition })$$

Now we can write

$$(\tau \times \tau) \,.\, (E_2 \times \lambda) = (\tau \times \tau) \,.\, E_2^{-1}$$
$$= (\tau \,.E_2) \,.\, E_2^{-1} \qquad (\text{ by (4) })$$
$$= \tau$$

i.e. $\tau(n) = \sum [\tau(r)]^2 \lambda\left(\frac{n}{r}\right) E_2\left(\frac{n}{r}\right)$

IV. $\sum \tau(r_1)\,\tau(r_2) = [\tau(n)]^3$

where the summation runs through all r_1, r_2 with n as their least common multiple.

To prove this, we have to introduce the notion of " block factors of n " first. By a block factor r of n, we shall mean a factor r which is relatively prime to $\frac{n}{r}$. Two factors r_1, r_2 which have n as their least common multiple can be put in the form

$$r_1 = xyp$$
$$r_2 = xzq$$

where n = xyz with x, y, z all being block factors and p, q are factors of y and z respectively, having no common block-factor with them.

$$\therefore \tau(r_1)\tau(r_2) = \tau(x)\,\tau(y)\,\tau(p)\,\tau(x)\,\tau(z)\,\tau(q)$$
$$= \tau(n)\,\tau(x)\,\tau(p)\,\tau(q)$$

Thus $\sum \tau(r_1)\,\tau(r_2)$ is of the form

$\tau(n) \sum \tau(r)$ where each r occurs as many times as $\frac{n}{r}$

can be expressed as the product of relatively prime factors.

i.e. $\sum \tau(r_1)\,\tau(r_2) = \tau(n) \times \left[\tau(r) \,.\, E_2(\frac{n}{r})\right]$

$= \tau(n) \times \tau(n) \times \tau(n)$ (by (4))

$= \left[\tau(n)\right]^3$

§ τ_k - function $\tau_k(n)$

It is easy to see that an alternate definition of $\tau(n)$ can be worded as follows.

Definition 4: $\tau(n)$ is equal to the number of all possible factorizations of n into a product of 2 factors. This can be further generalized to form $\tau_k(n)$ which may be defined as the number of all possible factorizations of n into a product of k factors.

Obviously,

Lemma 3: $\tau_k(n)$ is a multilpicative function.

i.e. $\tau_k(mn) = \tau_k(m)\tau_k(n)$

where $(m, n) = 1$

Proof: Suppose m and n can be factorized in the following manner,

$$m = f_1 f_2 \ldots\ldots f_k$$

$$n = g_1 g_2 \ldots\ldots g_k$$

then the corresponding factorization

$$mn = (f_1 g_1)(f_2 g_2) \ldots\ldots (f_k g_k) \text{ exists.}$$

If we are given a factorization

$$mn = q_1 q_2 \ldots\ldots q_k,$$

then it follows that the f's and the g's are uniquely determined by the equalities

$$q_i = f_i g_i \qquad (i = 1,2,\ldots\ldots,k)$$

Thus it follows that

$$\tau_k(mn) = \tau_k(m)\ \tau_k(n).$$

Lemma 4:

$$\tau_k(p_i^{\alpha_i}) = \frac{(\alpha_i + k - 1)!}{\alpha_i !\ (k-1)!} \qquad \ldots\ldots\ldots(1)$$

Proof: Here, we shall prove the lemma by mathematical induction.

Clearly (1) holds when k=1 and k=2.

For, when k=1,

$$\tau_1(p_i^{\alpha_i}) = 1,$$

$$\therefore \quad 1 = \frac{(\alpha_i + 1 - 1)!}{\alpha_i !\ 0!} = 1;$$

when k=2,

$$\tau_2(p_i^{\alpha_i}) = \alpha_i + 1$$

$$\therefore \quad \alpha_i + 1 = \frac{(\alpha_i + 2 - 1)!}{\alpha_i !\ (2-1)!} = \frac{(\alpha_i + 1)!}{\alpha_i !} = \alpha_i + 1$$

Now, assume (1) is true for k-1

$$\text{i.e.} \quad \tau_{k-1}(p_i^{\alpha_i}) = \frac{(\alpha_i + k - 2)!}{\alpha_i !\ (k-2)!}$$

We shall prove that it is also valid for k.

To obtain all factorizations of $p_i^{\alpha_i}$ into k factors, we can take each of the factorizations of $p_i^{\alpha_i}$ into k-1 factors first and then in each case, factorize the first factor in all possible ways into two other factors. Then among the factorizations of $p_i^{\alpha_i}$

into k factors, we distinguish these where the first factor is p_i^e with e arbitrary ($0 \leq e \leq k-1$). Thus there are $\tau_1(p_i^e)$ times $\tau_{k-1}(p_i^{\alpha_i - e})$ factorizations with the same first factor. By putting a summation over e with e ranges from 0 to α_i , we then get all the factorizations of $p_i^{\alpha_i}$ into k factors.

$$\therefore \quad \tau_k(p_i^{\alpha_i}) = \sum_{e=0}^{\alpha_i} \tau_1(p_i^e) \cdot \tau_{k-1}(p_i^{\alpha_i - e})$$

$$\therefore \tau_{k-1}(p_i^{\alpha_i - e}) = \frac{(\alpha_i - e + k - 2)!}{(\alpha_i - e)!\ (k-2)!} \quad \text{(by assumption)}$$

$$\text{and} \quad \tau_1(p_i^e) = 1$$

$$\therefore \quad \tau_k(p_i^{\alpha_i}) = \sum_{e=0}^{\alpha_i} \tau_{k-1}(p_i^{\alpha_i - e})$$

$$= \sum_{e=0}^{\alpha_i} \frac{(\alpha_i - e + k - 2)!}{(\alpha_i - e)!\ (k-2)!}$$

$$= \frac{(\alpha_i + k - 1)!}{\alpha_i!\ (k-1)!}$$

Thus, the lemma is proved.

<u>Theorem 2</u>: $$\tau_k(n) = \frac{1}{[(k-1)!]^r} \prod_{i=1}^{r} \frac{(\alpha_i + k - 1)!}{\alpha_i!}$$

when $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$ with the p's being primes.

Proof: $\tau_k(n)$ is a multiplicative function

$$\therefore \tau_k(n) = \prod_{i=1}^{r} \tau_k(p_i^{\alpha_i})$$

$$= \prod_{i=1}^{r} \frac{(\alpha_i + k - 1)!}{\alpha_i ! (k-1)!} \quad \text{(by lemma 4).}$$

$$= \frac{1}{[(k-1)!]^r} \prod_{i=1}^{r} \frac{(\alpha_i + k - 1)!}{\alpha_i !}$$

§ σ - function $\sigma(n)$

Definition 5: $\sigma(n)$ is defined as the sum of the positive divisors of n.

By definition, $\sigma(n)$ can be written as

$$\sigma(n) = \sum_{d/n} d$$

$\sigma(n)$ is also a multiplicative function. For applying lemma 3 of Chapter 1, with $f(n) = n$, $F(n) = \sigma(n)$, and since $f(n) = n$ is multiplicative, so it follows that $\sigma(n)$ is as well.

The following is a well-known relation of $\sigma(n)$.

Theorem 3:

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

and $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$ being the canonical factorization of n.

Proof: $\sigma(n)$ is multiplicative,

$$\therefore \sigma(n) = \prod_{i=1}^{r} (p_i^{\alpha_i})$$

But the divisors of $p_i^{\alpha_i}$ are $1, p_i, p_i^2, \ldots\ldots p_i^{\alpha_i}$ and $1, p_i, p_i^2, \ldots\ldots p_i^{\alpha_i}$ is a geometric progression with a common ratio of p_i.

$$\therefore \quad 1 + p_i + p_i^2 + \ldots\ldots + p_i^{\alpha_i} = \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

$$\therefore \quad \sigma(n) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

Equations involving $\sigma(n)$

A. Makowski [20] gave some results concerning the equations

(a) $\sigma(x) = \sigma(x+1)$

(b) $\sigma(x+2) = \sigma(x) + 2$

He found that equation (a) has only 9 solutions in positive integers $x \leq 10{,}000$; They are $x = 14, 206, 957, 1334, 1364, 1634, 2685, 2974$ and 4364.

The equation (b) is satisfied by integers x such that both x and x+2 are primes. This equation has only 3 solutions in integers $x \leq 9998$ where x is composite, namely, $x = 434, 8575$ and 8825.

§ ϕ - function $\phi(n)$

Definition 6: $\phi(n)$ is defined as the number of integers not greater than and prime to n; i.e. the number of values of i such that

$$0 < i \leq n \quad \text{with} \quad (i, n) = 1$$

Before we proceed to prove that $\phi(n)$ is multiplicative, it is note-worthy to introduce the idea of residue system.

Definition 7: A complete residue system (mod m) is defined as a set of integers $a_1, a_2, \ldots . a_m$ such that

(1) if $i \neq j$, then $a_i \not\equiv a_j \pmod m$

(2) if a is any integer, there is an index i with $1 \leq i \leq m$

for which

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

e.g. The set $\{1,2,.....,m-1,m\}$ is an example of a complete residue sysyem (mod m).

Definition 8 ; A reduced residue system is a set of integers a_1, a_2, ……,a_h incongruent (mod m) such that if a is any integer prime to m, there is an index i, $1 \leq i \leq h$ for which $a \equiv a_i \pmod{m}$. In other words, a reduced residue system is a set of representatives, one from each of the residue classes containing integers prime to m.

e.g. The set $\{1,5,7,11,13,17\}$ is an example of a reduced residue system (mod 18).

Lemma 5: Let (m,n) = 1. Suppose that a runs through a complete set of residues (mod m) and a' through a complete set of residues (mod n). Then a'm + an runs through a complete set of residues (mod mn).

Proof: There are mn numbers of a'm + an.

Assume

$$a_1'm + a_1n \equiv a_2'm + a_2n \pmod{mn}$$

then

$$a_1'm \equiv a_2'm \pmod{n}$$

$\because$ $(m,n) = 1$

$\therefore$ $a_1' \equiv a_2' \pmod{n}$

Similarly, we can get

$$a_1 \equiv a_2 \pmod{m}$$

Thus a contradiction arises. Since a runs through a complete set of residues (mod m) and a' runs through a complete set of

residues (mod n), so

$$a_1 \not\equiv a_2 \pmod{m}$$
$$a_1' \not\equiv a_2' \pmod{n}$$

therefore, we conclude that all the mn are all incongruent and thus form a complete residue system (mod mn).

Theorem 4: $\phi(n)$ is multiplicative.

i.e. $\phi(mn) = \phi(m)\phi(n)$ where $(m,n) = 1$

Proof: Let $\phi(m)$ be p and $r_1, r_2, \ldots r_p$ be a reduced residue system (mod m). Similarly let $\phi(n)$ be q and $s_1, s_2, \ldots s_q$ be a reduced residue system (mod n). If x is in a reduced residue system (mod mn), then $(x,m) = 1$, $(x,n) = 1$, since $(m,n) = 1$; and hence $x \equiv r_i \pmod{m}$, $x \equiv s_j \pmod{n}$ for some i and j. Conversely, if $x \equiv r_i \pmod{m}$ and $x \equiv s_j \pmod{n}$ then $(x, mn) = 1$. Thus the reduced residue system (mod mn) can be obtained by determining all the x's such that $x \equiv r_i \pmod{m}$ and $x \equiv s_j \pmod{n}$ for some i and j. According to Chinese Remainder Theorem, each pair of i,j determines only one x (mod mn), i.e. different pairs of i, j give different x (mod mn). But there are pq pairs of these i,j, therefore the reduced residue system (mod mn) has $pq = \phi(m)\phi(n)$ elements. Hence we have

$$\phi(mn) = \phi(m)\phi(n).$$

Theorem 5:
$$\phi(n) = n \prod_{p/n} \left(1 - \frac{1}{p} \right)$$

where the product ranges over all the distinct primes which divide n.

Proof: Since $\phi(n)$ is multiplicative, and if $n = \prod_{i=1}^{r} p_i^{\alpha_i}$

then
$$\phi(n) = \prod_{i=1}^{r} \phi\left(p_i^{\alpha_i} \right)$$

We can evaluate $\phi(p_i^{\alpha_i})$ directly. All the positive integers not exceeding $p_i^{\alpha_i}$ are prime to $p_i^{\alpha_i}$ except the multiples of p_i, and there are just $p_i^{\alpha_i-1}$ of these.

Hence,

$$\phi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i-1} = p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)$$

$$\therefore \quad \phi(n) = \prod_{i=1}^{r} \phi(p_i^{\alpha_i})$$

$$= \prod_{i=1}^{r} p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)$$

$$= \prod_{i=1}^{r} p_i^{\alpha_i} \cdot \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)$$

$$= n\prod_{p/n}\left(1 - \frac{1}{p}\right)$$

Theorem 6: $\sum_{d/n} \phi(d) = n$

Proof: Let $d_1, d_2, \ldots, d_k$ be the positive divisors of n. We group the integers a's, $(1 \le a \le n)$ into classes $C(d_1), \ldots, C(d_k)$, putting an integer a into the class $C(d_i)$ if $(a,n) = d_i$. The number of elements in $C(d_i)$ is then

$$\sum_{\substack{a \le n \\ (a,n)=d_i}} 1$$

and since every integer up to n is in exactly one of the classes,

$$\therefore \quad \sum_{d_i/n} \sum_{\substack{a \le n \\ (a,n)=d_i}} 1 = n$$

The number of the integers a's is exactly equal to the

number of integers b's such that $b \leq \frac{n}{d_i}$ and $(b, \frac{n}{d_i}) = 1$. From the definition of $\phi(n)$, the number of b's is clearly $\phi(\frac{n}{d_i})$. Thus,

$$\sum_{d_i/n} \phi\left(\frac{n}{d_i}\right) = n$$

which is equivalent to the theorem; since, as d_i runs over the divisors of n, $\frac{n}{d_i}$ also runs over these same divisors, but just in reverse order.

$$\therefore \sum_{d_i/n} \phi(d_i) = n$$

Generalizations of $\phi(n)$

I. An alternate definition of $\phi(n)$ would be as follows,

Definition 9: $\phi(n)$ is defined as the number of ordered pairs $\langle x,y \rangle$ for which $x+y = n$, $1 \leq x \leq n$, and x,y both being relatively prime to n. It is easy to see that this definition of $\phi(n)$ is equivalent to the one given above.(see definition 6).

The following is a generalization of the definition of the Euler's ϕ - function, suggested by S.K. Stein [1].

Definition 10: The function $\phi(n,m)$ with $m \geq 0$ is defined as the number of ordered pairs $\langle x,y \rangle$ for which $x+y = n+m$, $1 \leq x \leq n$ and x,y, both being relatively prime to n.

Specifically, when $m = 0$, $\phi(n,m)$ would be the same as $\phi(n)$.

The multiplicativity of $\phi(n,m)$ is not as obvious as that of $\phi(n)$.

Lemma 6: $\phi(n,m)$ is multiplicative,

i.e. $\phi(ab,m) = \phi(a,m)\phi(b,m)$

if $(a,b) = 1$

Proof: Let $S_1 = \{x_1, \ldots, x_{\phi(a,m)}\}$ be the set of all values of x for which $x+y = a+m$, $1 \leq x \leq a$, and x and y both being relatively prime to a. Now, if $(a,b) = 1$, then it can be shown that for each x for which $x+y = ab + m$, $1 \leq x \leq ab$, and x and y both relatively prime to ab, we must have

$$x \equiv x_i \pmod{a} \quad \ldots\ldots(1)$$

where $x_i \in S_1$. For, suppose $x \equiv x_j \pmod{a}$, $1 \leq x_j \leq a$, where $x_j \notin S_1$, then

$$x = x_j + ka$$

and for some y,

$$x_j + ka + y = ab + m \quad \ldots\ldots(2)$$

and for some z,

$$x_j + z = a + m \quad \ldots\ldots(3)$$

where either $(x_j,a) = g_1 > 1$ or $(z,a) = g_2 > 1$, since otherwise x_j would be in S_1.

Now, $(x_j,a) = g_1$

$\Rightarrow$ g_1/x and $g_1/(x,ab) = 1$,

so that g_2 is greater than 1.

But, subtracting (3) from (2), we get

$$g_2 /(y,ab) = 1$$

$\therefore$ $x \not\equiv x_j \pmod{a}$; $x_j \notin S_1$

$\therefore$ (1) is derived

i.e. $x \equiv x_i \pmod{a}$; $x_i \in S_1$

Hence, if $x+y = ab+m$, $1 \leq x \leq ab$ and x and y both relatively prime to ab, then x is of one of the forms

$x_i,\ x_i+a,\ x_i+2a,\ \ldots\ldots,x_i+(b-1)a,\ldots\ldots\ldots(4)$

where $x_i \in S_1$. For each i, the set of numbers given by (4) constitutes a complete residue system (mod b), since (a,b) = 1.

Now, let $S_2 = \{x_1', \ldots\ldots\ldots, x'_{\phi(b,m)}\}$ be the set of all values of x for which x+y = b+m, $1 \leq x \leq b$, and x and y both relatively prime to b. Then repeating the arguments used to derive (1), we observe that only those elements of (4) can satisfy the given conditions i.e. x+y = ab+m, $1 \leq x \leq ab$, (x,ab) = 1, (y,ab) = 1, which are congruent to some element of S_2(mod b). Thus, for each i, there are $\phi(b,m)$ values in the set given by (4) which are easily seen to satisfy all the required conditions so that, since there are $\phi(a,m)$ values of i, we have

$$\phi(ab,m) = \phi(a,m)\phi(b,m)$$

Theorem 7:
$$\phi(n,m) = n \prod_{i=1}^{r} \left(1 - \frac{\epsilon_m(p_i)}{p_i} \right)$$

where $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$ with the p's being primes

and $\epsilon_m(p) = \begin{cases} 2 & \text{if } p \nmid m \\ 1 & \text{if } p/m \end{cases}$

We have already proved the special case of this theorem when m = 0

i.e. $\phi(n) = \phi(n,0) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i} \right)$

Proof: Since $\phi(n,m)$ is multiplicative,

$$\therefore\ \phi(n,m) = \prod_{i=1}^{r} \phi(p_i^{\alpha_i}, m)$$

Let's now first prove

$$\phi(p_i^{\alpha_i},m) = p_i^{\alpha_i}\left(1 - \frac{2}{p_i}\right) \text{ if } p_i \nmid m$$

As x runs through the numbers $1, \ldots\ldots, p_i^{\alpha_i}$, there are $p_i^{\alpha_i-1}$ values of x which are divisible by p_i and consequently have to be subtracted to satisfy the required conditions. Since $x+y = p_i^{\alpha_i} + m$ (definition 10), it is impossible that both x and y are divisible by p_i, as $p_i \nmid m$, and since y runs through a complete residue system $(\text{mod } p_i^{\alpha_i})$, as x runs through the numbers $1, \ldots\ldots, p_i^{\alpha_i}$, there are $p_i^{\alpha_i-1}$ values of y which are divisible by p_i, which occur in ordered pairs $\langle x,y \rangle$ distinct from those for which x is divisible by p_i. We therefore have

$$\begin{aligned}\phi(p_i^{\alpha_i},m) &= p_i^{\alpha_i} - 2p_i^{\alpha_i-1} \\ &= p_i^{\alpha_i}\left(1 - \frac{2}{p_i}\right)\end{aligned}$$

For p/m, we observe that in this case the ordered pairs $\langle x,y \rangle$ for which $x+y = p_i^{\alpha_i} + m$ in which x is divisible by p_i are identical with those for which y is divisible by p_i, so that

$$\begin{aligned}\phi(p_i^{\alpha_i},m) &= p_i^{\alpha_i} - p_i^{\alpha_i-1} \\ &= p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)\end{aligned}$$

Thus, $\phi(n,m) = \prod_{i=1}^{r} \phi(p_i^{\alpha_i},m)$

$$= \begin{cases} \prod_{i=1}^{r} p_i^{\alpha_i}\left(1 - \frac{2}{p_i}\right) & \text{when } p \nmid m \\ \prod_{i=1}^{r} p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right) & \text{when } p/m \end{cases}$$

$$\phi(n,m) = \begin{cases} \prod_{i=1}^{r} p_i^{\alpha_i} \prod_{i=1}^{r} \left(1 - \frac{2}{p_i} \right) & \text{when } p \nmid m \\ \prod_{i=1}^{r} p_i^{\alpha_i} \prod_{i=1}^{r} \left(1 - \frac{1}{p_i} \right) & \text{when } p/m \end{cases}$$

$$= \begin{cases} n \prod_{i=1}^{r} \left(1 - \frac{2}{p_i} \right) & \text{when } p \nmid m \\ n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i} \right) & \text{when } p/m \end{cases}$$

$$\text{or} \quad = n \prod_{i=1}^{r} \left(1 - \frac{\epsilon_m(p_i)}{p_i} \right)$$

$$\text{when } \epsilon_m(p_i) = \begin{cases} 2 & \text{if } p \nmid m \\ 1 & \text{if } p/m \end{cases}$$

II. C.S. Venkataraman[29] gave another generalization of Euler's ϕ - function which bears a certain similarity to the previous one.

Definition 11:

$\phi(m,g)$ is defined as the number of the positive integers which are not greater than m and which have a specified divisor g of m as their g.c.d. (greatest common divisor) with m.

We can see very easily that when $g = 1$,

$$\phi(m,1) = \phi(m)$$

The multiplicativity of $\phi(m,g)$ here is again not as obvious as that of $\phi(n)$.

Theorem 8: $\phi(m,g)$ is a multiplicative function,

i.e. if $(m,n) = 1$ and g' is any divisor of n, then

$$\phi(mn,gg') = \phi(m,g)\phi(n,g')$$

Proof: It follows from lemma 5 that if b is any number of a complete

set of residues (mod mn), then b can be written uniquely in the form of a'm + an (mod mn) where a is a number of a complete set of residues (mod m) and a' is a number of a complete set of residues (mod n).

Suppose now that $(a,m) = g$; $(a',n) = g'$. Then since $(m,n) = 1$, $(g,g') = 1$, and also

$(an,m) = g$; $(a'm,n) = g'$

$\therefore$ $(a'm+an,m) = g$; $(a'm+an,n) = g'$

$\therefore$ $(a'm+an,mn) = gg'$.

Obviously there are $\phi(m,g)\phi(n,g')$ numbers of a'm+an and by lemma 5, they are distinct (mod mn). Hence it follows that there are at least $\phi(m,g)\phi(n,g')$ numbers not greater than mn and having the g.c.d. gg' with mn. There cannot be more, for, if b is one of the $\phi(mn,gg')$ numbers, by lemma 5, (since then b is also a member of a complete set of residues mod (mn)).

$b \equiv a'm + an$ (mod mn) ;

also $(b,mn) = gg'$,

$\therefore$ $(a'm+an,mn) = gg'$.

But, $(m,n) = 1$, and $(g,g') = 1$

$\therefore$ $(a'm+an,m) = g$; $(a'm+an,n) = g'$

$\therefore$ $(an,m) = g$; $(a'm,n) = g'$

$\therefore$ $(a,m) = g$; $(a',n) = g'$.

$\therefore$ There can be only $\phi(m,g)\phi(n,g')$ numbers not greater than mn having the g.c.d. gg' with mn.

Hence $\phi(mn,gg') = \phi(m,g)\phi(n,g')$ if $(m,n) = 1$.

Theorem 9: $\phi(m,g) = \frac{m}{g}\prod\left(1 - \frac{1}{p}\right)$ where p runs through the distinct

set of residues (mod mn), then b can be written uniquely in the form of a'm + an (mod mn) where a is a number of a complete set of residues (mod m) and a' is a number of a complete set of residues (mod n).

Suppose now that $(a,m) = g$; $(a',n) = g'$. Then since $(m,n) = 1$, $(g,g') = 1$, and also

$(an,m) = g$; $(a'm,n) = g'$

$\therefore$ $(a'm+an,m) = g$; $(a'm+an,n) = g'$

$\therefore$ $(a'm+an,mn) = gg'$.

Obviously there are $\phi(m,g)\phi(n,g')$ numbers of a'm+an and by lemma 5, they are distinct (mod mn). Hence it follows that there are at least $\phi(m,g)\phi(n,g')$ numbers not greater than mn and having the g.c.d. gg' with mn. There cannot be more, for, if b is one of the $\phi(mn,gg')$ numbers, by lemma 5, (since then b is also a member of a complete set of residues mod (mn)).

$b \equiv a'm + an \pmod{mn}$;

also $(b,mn) = gg'$,

$\therefore$ $(a'm+an,mn) = gg'$.

But, $(m,n) = 1$, and $(g,g') = 1$

$\therefore$ $(a'm+an,m) = g$; $(a'm+an,n) = g'$

$\therefore$ $(an,m) = g$; $(a'm,n) = g'$

$\therefore$ $(a,m) = g$; $(a',n) = g'$.

$\therefore$ There can be only $\phi(m,g)\phi(n,g')$ numbers not greater than mn having the g.c.d. gg' with mn.

Hence $\phi(mn,gg') = \phi(m,g)\phi(n,g')$ if $(m,n) = 1$.

Theorem 9: $\phi(m,g) = \frac{m}{g}\prod\left(1 - \frac{1}{p}\right)$ where p runs through the distinct

prime factors of $\frac{m}{g}$.

Proof:

By theorem 8, clearly it is sufficient if we prove the result when m is a power of a prime p, i.e. it is sufficient if we prove the theorem for $\phi(p^r, p^\alpha)$ where $\alpha \leq r$.

If $\alpha = r$, obviously $\phi(p^r, p^\alpha) = 1$ .....(1)

Next, suppose $\alpha < r$,

Now, there are $p^{r-\alpha}$ numbers $\not> p^r$ which are multiples of p^α. It is evident that if we exclude from these, the numbers which are multiples of $p^{\alpha+1}$, we will get precisely all and only those numbers ($\not> p^r$) which have the g.c.d. p^α with p^r. The multiples of $p^{\alpha+1}$ ($\not> p^r$) are $p^{r-\alpha-1}$ in number. Hence the number of numbers ($\not> p^r$) which have the g.c.d. p^α with p^r is

$$p^{r-\alpha} - p^{r-\alpha} - p^{r-\alpha-1} = p^{r-\alpha}\left(1 - \frac{1}{p}\right)$$

Therefore

$$\text{if } \alpha < r, \quad \phi(p^r, p^\alpha) = \frac{p^r}{p^\alpha}\left(1 - \frac{1}{p}\right) \quad \text{.....(2)}$$

Combining (1) and (2) we can at once obtain that

$$\text{if } \quad m = \prod_{i=1}^{r} p_i^{r_i}, \qquad g = \prod_{i=1}^{r} p_i^{\alpha_i} \qquad \text{and } \alpha_i \leq r_i,$$

$$\phi(m,g) = \prod_{i=1}^{r} \phi(p_i^{r_i}, p_i^{\alpha_i})$$

$$= \frac{m}{g} \prod\left(1 - \frac{1}{p}\right)$$

where p ranges over the distinct prime factors of $\frac{m}{g}$.

§ Möbius μ - function $\mu(n)$

Möbius function is one of the most important arithmetical functions, which is defined as follows.

Definition 12:

μ - function is defined as follows

$$\begin{cases} (1) & \mu(1) = 1 \\ (2) & \mu(n) = 0 \text{ if } a^2/n, \text{ with } a>1 \\ (3) & \mu(n) = (-1)^k \text{ if } k \text{ is the number of distinct prime factors of } n. \end{cases}$$

It is easy to see that $\mu(n)$ is multiplicative.

For, if $(m,n) = 1$

case (i) if one of m, n is equal to 1, say m

$\mu(mn) = \mu(1n) = \mu(n)$

$\because \mu(m) = \mu(1) = 1$ (by definition)

$\therefore \mu(m)\mu(n) = 1.\mu(n) = \mu(n)$

Hence, $\mu(mn) = \mu(m)\mu(n)$.

case (ii) if one of the m, n has a squared factor, say m; i.e. a^2/m

$\Rightarrow a^2/mn$

$\therefore \mu(mn) = 0$ (by definition)

also, $\mu(m)\mu(n) = 0\,\mu(n) = 0$

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

case (iii) if m has r distinct prime factors and n has s distinct prime factors $\Rightarrow$ mn has r+s distinct prime factors.

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

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

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

Also, from the definition of $\mu(n)$ itself, it can be deduced that

$$\sum_{d/n} \mu(d) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n>1 \end{cases} \qquad \ldots\ldots\ldots(1)$$

For, if we take $Q(n) = \sum_{d/n} \mu(d)$, and since $\mu(n)$ is multiplicative, therefore $Q(n)$ is also multiplicative by lemma 3 of Chapter 1. Since $Q(1) = \mu(1) = 1$ and $Q(p^{\alpha}) = \sum_{e=0}^{\alpha} \mu(p^e) = 1 + (-1) = 0$ we have the desired result.

The following is the so-called Möbius inversion formula, which is one of the most important fundamental blocks in the theory of numbers.

<u>Theorem 10</u>: Let $g(n)$ and $f(n)$ be arithmetical functions. If they satisfy the relation

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

then

$$f(n) = \sum_{d/n} \mu(\tfrac{n}{d})\, g(d)$$

$$= \sum_{d/n} \mu(d)\, g(\tfrac{n}{d})$$

<u>Proof</u>:

$$\sum_{d/n} \mu(d)\, g(\tfrac{n}{d}) = \sum_{d/n} \mu(d) \sum_{\delta/\frac{n}{d}} f(\delta)$$

$$= \sum_{d\delta/n} \mu(d)\, f(\delta)$$

$$= \sum_{\delta/n} f(\delta) \sum_{d/\frac{n}{\delta}} \mu(d)$$

$$= f(n), \quad (\text{ by } (1))$$

It is trivial to see that

$$\sum_{d/n} \mu(\tfrac{n}{d})\, g(d) = \sum_{d/n} \mu(d)\, g(\tfrac{n}{d})$$

therefore, the theorem is proved.

The converse of this theorem is of frequent use in the theory of numbers also.

Theorem 11:

$$f(n) = \sum_{d/n} \mu(\tfrac{n}{d})\, g(d)$$

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

Proof:

$$\sum_{d/n} f(d) = \sum_{d/n} f(\tfrac{n}{d})$$

$$= \sum_{d/n} \sum_{\delta/\frac{n}{d}} \mu(\tfrac{n}{d\delta})\, g(\delta)$$

$$= \sum_{d\delta/n} (\tfrac{n}{d\delta})\, g(\delta)$$

$$= \sum_{\delta/n} g(\delta) \sum_{d/\frac{n}{\delta}} \mu(\tfrac{n}{d\delta})$$

$$= g(n) \quad \text{by (1)}$$

It should be noted that $g(n)$ and $f(n)$ do not necessarily have to be multiplicative; in fact, any arithmetical function will do.

Characteristic properties of $\mu(n)$

I. The equation (1) stated above can be shown as a characteristic property of $\mu(n)$. In other words,

Theorem 12: If (1) is satisfied by another function $\mu^*(n)$, then it

implies that

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

We can use the Möbius inversion formula to prove that it is so.

Proof: Suppose that $\mu^*(n)$ has the property (1)

i.e. $$\sum_{d/n} \mu^*(d) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n>1 \end{cases}$$

Take another function $w(n)$, defined by

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

Then, we have $w(n) = \sum_{d/n} \mu^*(d)$ for all n. Hence by Möbius inversion formula, we get

$$\mu^*(n) = \sum_{d/n} \mu(n)\ w(\tfrac{n}{d})$$

$$= \mu(n)\ w(1) \qquad \text{(by definition of } w(n))$$

$$= \mu(n)$$

Since it is true for all n,

$$\therefore \quad \mu^*(n) \equiv \mu(n)$$

II. U.V.Satyanarayana [24] established in one of his papers that the inversion itself is a characteristic property of the Möbius function.

Namely, in form of a theorem, it will be :

Theorem 13:

Let $f(n)$, $g(n)$ and $\mu^*(n)$ be three arithmetical functions, and

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

$$f(n) = \sum_{d/n} \mu^*(d)\ g(\tfrac{n}{d})$$

$$f(1) \neq 0$$

then, $\mu^*(n)$ coincides with $\mu(n)$.

Before we proceed to the proof of the theorem, we need to discuss one lemma first.

Lemma 7 :

If $\alpha(n)$ and $\beta(n)$ are two arithmetical functions and

$$\begin{cases} \text{(i)} \quad \alpha(n) = \sum_{\delta/n} \alpha(\delta)\ \beta\left(\frac{n}{\delta}\right) \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \ldots\ldots\ldots\ldots (2) \\ \text{(ii)} \quad \alpha(1) \neq 0 \end{cases}$$

then $$\beta(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

Proof:

Take $n = 1$ and $n = 2$ in (2). We get

$$\begin{cases} \alpha(1) = \alpha(1)\ \beta(1) \\ \alpha(1) \neq 0 \end{cases}$$

and

$$\begin{cases} \alpha(2) = \alpha(1)\ \beta(2) + \alpha(2)\ \beta(1) \\ \alpha(1) \neq 0 \end{cases}$$

From the above equations, we have at once

$$\beta(1) = 1$$

$$\beta(2) = 0$$

By mathematical induction, it iseasy to show that $\beta(n) = 0$ for all $n \geq 2$.

Proof of theorem 13:

$$f(n) = \sum_{d/n} \mu^*(d)\ g\left(\frac{n}{d}\right) \qquad \text{(given condition)}$$

$$= \sum_{d/n} \mu^*(d) \sum_{\delta/\frac{n}{d}} f(\delta) \qquad \text{(given co ndition)}$$

$$= \sum_{\delta\, d/n} \mu^*(d)\ f(\delta)$$

$$= \sum_{\delta/n} f(\delta) \sum_{d/\frac{n}{\delta}} \mu^*(d)$$

Let $\beta(n) = \sum_{d/n} \mu^*(d)$

We then have

$$f(n) = \sum_{\delta/n} f(\delta)\ \beta\left(\frac{n}{\delta}\right)$$

$$\Rightarrow \quad \beta(n) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n>1 \end{cases} \qquad \text{(by lemma 7)}$$

Again, by theorem 12, it is proved that $\mu^*(n)$ satisfies the three conditions of $\mu(n)$, thus it is identical to the Möbius μ - function.

Remark:

The condition $f(1) \neq 0$ in theorem 13 proved above can be

Proof of theorem 13:

$$f(n) = \sum_{d/n} \mu^*(d)\ g\left(\frac{n}{d}\right) \qquad \text{(given condition)}$$

$$= \sum_{d/n} \mu^*(d) \sum_{\delta/\frac{n}{d}} f(\delta) \qquad \text{(given co ndition)}$$

$$= \sum_{\delta\, d/n} \mu^*(d)\ f(\delta)$$

$$= \sum_{\delta/n} f(\delta) \sum_{d/\frac{n}{\delta}} \mu^*(d)$$

Let $\beta(n) = \sum_{d/n} \mu^*(d)$

We then have

$$f(n) = \sum_{\delta/n} f(\delta)\ \beta\left(\frac{n}{\delta}\right)$$

$$\Rightarrow \quad \beta(n) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n>1 \end{cases} \qquad \text{(by lemma 7)}$$

Again, by theorem 12, it is proved that $\mu^*(n)$ satisfies the three conditions of $\mu(n)$, thus it is identical to the Möbius μ - function.

Remark:

The condition $f(1) \neq 0$ in theorem 13 proved above can be

replaced by a more general condition $f(n) \neq 0$.

i.e.

Theorem 14:

Let $f(n)$, $g(n)$ and $\mu^*(n)$ be three arithmetical functions with

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

(ii) $f(n) = \sum_{d/n} \mu^*(d)\ g(\frac{n}{d})$

and

(iii) $f(n) \neq 0$

then $\mu^*(n)$ coincides with $\mu(n)$.

We need a few lemmas before we can prove the above theorem.

Lemma 8; If $\alpha(n) \neq 0$ and $\beta(n) \neq 0$,

then

$$\gamma(n) = \sum_{d/n} \alpha(d)\ \beta(\frac{n}{d}) \neq 0$$

Proof: Suppose m_1 and n_1 are the least of the positive integers. m and n to make $\alpha(m) \neq 0$ and $\beta(n) \neq 0$,

Now, $\gamma(m_1 n_1) = \sum_{d/m_1 n_1} \alpha(d)\beta(\frac{m_1 n_1}{d})$

$$= \sum_{\substack{d/m_1 n_1 \\ d>m_1}} \alpha(d)\beta(\frac{m_1 n_1}{d}) + \alpha(m_1)\beta(n_1) + \sum_{\substack{d/m_1 n_1 \\ d<m_1}} \alpha(d)\beta(\frac{m_1 n_1}{d})$$

when $d>m_1$, $\frac{m_1 n_1}{d} < n_1$

$\therefore \beta(\frac{m_1 n_1}{d}) = 0$

when $d<m_1$, $\alpha(d) = 0$

$\therefore \gamma(m_1 n_1) = \alpha(m_1)\beta(n_1) \neq 0$

i.e. $\gamma(n) = \sum_{d/n} \alpha(n)\beta(\frac{n}{d}) \neq 0$

Lemma 9 : If $\alpha(n)$ and $\beta(n)$ are two arithmetical functions and

(1) $\alpha(n) \not\equiv 0$

(2) $\alpha(n) = \sum_{d/n} \alpha(d)\beta(\frac{n}{d})$

then $\beta(n) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n>1 \end{cases}$

Proof: Define a function $\gamma(n) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n>1 \end{cases}$

then it is clear that

$$\alpha(n) = \sum_{d/n} \alpha(d)\gamma(\frac{n}{d})$$

and by hypothesis (2), we have

$$\sum_{d/n} \alpha(d)\beta(\frac{n}{d}) = \sum_{d/n} \alpha(d)\gamma(\frac{n}{d})$$

or $$\sum_{d/n} \alpha(d)\left[\beta(\frac{n}{d}) - \gamma(\frac{n}{d})\right] \equiv 0$$

$\therefore \alpha(n) \not\equiv 0$ (by hypothesis (1))

and by lemma 8, we get

$$\beta(\frac{n}{d}) - \gamma(\frac{n}{d}) \equiv 0$$

or, which is the same thing, if we write it as

$$\beta(n) - \gamma(n) \equiv 0$$

i.e. $\beta(n) = \gamma(n)$

$\therefore \beta(n) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n>1 \end{cases}$

Proof of theorem 14:

From (1) and (2) of the hypothesis, we get

$$f(n) = \sum_{d/n} \mu^*(d) \sum_{\delta/\frac{n}{d}} f(\delta)$$

$$= \sum_{\delta\, d/n} \mu^*(d)\, f(\delta)$$

$$= \sum_{\delta/n} f(\delta) \sum_{d/\frac{n}{\delta}} \mu^*(d)$$

$$= \sum_{\delta/n} f(\delta)\, \beta\left(\frac{n}{\delta}\right)$$

where $\beta\left(\frac{n}{\delta}\right)$ is defined as $\sum_{d/\frac{n}{\delta}} \mu^*(d)$.

Since by (1) of the hypothesis, $f(n) \neq 0$, therefore

$$\beta(n) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n>1 \end{cases} \qquad \text{(by lemma 9)}$$

and by theorem 12,

we have (i) $\mu^*(1) = 1$

(ii) $\mu^*(n) = (-1)^k$ if n has k distinct prime factors.

(iii) $\mu^*(n) = 0$ if a^2/n with $a>0$.

i.e. $\mu^*(n)$ coincides with the Möbius μ- function.

Generalization of $\mu(n)$

In one of his papers, H. Gupta [18] gave a certain generalization of $\mu(n)$ which is defined as follows.

Definition 13: $v_r(n)$ is defined by the relation

$$\sum_{d/n} v_r(d) = \begin{cases} 1 & (r \geq 0) \text{ if } n=a^r, \text{ a being a positive integer,} \\ 0 & (r \geq 0) \text{ if } n \neq a^r, \text{ a being a positive integer,} \end{cases}$$

Evidently $v_r(n)$ is identical with the Möbius function $\mu(n)$ for $r = 0$.

For r=1, the function $v_r(n)$ appears to be of little importance as

$$v_1(n) = \begin{cases} 1 & \text{if } n=1 \\ 0 & \text{if } n\neq 1 \end{cases}$$

Therefore, for convenience's sake, we shall write $v(n)$ in place of $v_r(n)$ with r being an integer ≥ 2. Also, p with or without subscripts will denote a prime ≥ 2.

Theorem 15: $v(n)$ is a multiplicative function

i.e. if $(a,b) = 1$, then

$$v(a,b) = v(a)\, v(b).$$

Proof:

Suppose the theorem is true for every $n \leq (ab - 1)$.

Then

$$\sum_{d/ab} v(d) = \sum_{\substack{d_1/a \\ d_2/b}} v(d_1 d_2)$$

$$= \sum_{d_1/a} v(d_1) \cdot \sum_{d_2/a} v(d_2) + v(ab) - v(a)v(b)$$

Now, two cases arise.

case (i), if a and b are both r^{th} powers of integers > 0, then the left side is equal to 1, and so also is each sum on the right side.

$$\therefore \sum_{d/ab} v(d) = \sum_{d_1/a} v(d_1) \cdot \sum_{d_2/b} v(d_2)$$

case (ii), if at least one of the numbers a and b is not an r^{th} power, the left side is zero and so also is at least one of the sigmas on the right.

$$\therefore \text{ again, } \sum_{d/ab} v(d) = \sum_{d_1/a} v(d_1) \cdot \sum_{d_2/b} v(d_2)$$

Hence $v(ab) = v(a)\, v(b)$ provided $(a,b) = 1$.

The theorem now follows by induction.

In view of the multiplicativity of $v(n)$, we need only to find the value of $v(p^{\alpha})$, $(\alpha \geq 0)$ in order to find the value of $v(n)$.

Now,

$$\sum_{d/p^{\alpha}} v(d) = \sum_{d_1/p^{\alpha-1}} v(d_1) + v(p^{\alpha})$$

If $\alpha \equiv 0 \pmod{r}$, we have $v(p^{\alpha}) = 1$

If $\alpha \equiv 1 \pmod{r}$, we have $v(p^{\alpha}) = -1$

If $\alpha \not\equiv 0$ or $1 \pmod{r}$, we have $v(p^{\alpha}) = 0$

These results hold for the Möbius function.

CHAPTER III

INVERSION

§ Fundamental theorem of the theory of inversion

Arithmetical functions play a very important part in " inversion " which is one of the most interesting topics in number theory. The Möbius inversion formula is usually considered to be the " principle of inversion of arithmetical functions." The Möbius function is rendered indispensable in the whole theory of inversion. In fact, it is on its property

$$\sum_{d/n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n \neq 1 \end{cases} \quad \ldots\ldots\ldots\ldots (1)$$

that the Möbius inversion formula depends.

However, analogous to (1), there holds a property for any numerical function f(n), not for $\mu(n)$ alone, that throws a great deal of light on many inversion formulas. The said property can be given in the form of a theorem.

Theorem I

For any numerical function f(n), it is possible to determine a numerical function f' (n) such that

$$\sum f(d)\ f'(\delta) = \begin{cases} f(1) & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

where the summation $\sum$ refers to all pairs (d, δ) of conjugate divisors $d, \delta > 0$ of n. ($n = d\delta$) The required f'(n), called

the reciprocal of f(n), can be defined by

$$f'(1) = 1 ,$$

$$f'(n) = \sum_{k=1}^{\alpha(n)} (-1)^k \left[f(n) \right]_k \quad \frac{1}{f^k(1)}, \quad n > 1$$

where $\alpha(n)$ is the total number of prime divisors of n and $\left[f(n) \right]_k$ denotes

$$\sum f(d_1)\, f(d_2) \ldots\ldots\ldots\ldots f(d_k)$$

with the summation going through all the distinct resolutions of n into k factors each of which is greater than 1.

The proof of this theorem will be more clearly seen if we here give a numerical example first.

Example:

Let n = 18. Then, the pairs (d, δ) of conjugate divisors of 18 being

$$(d, \delta) = (1,18), (2,9), (3,6), (6,3), (9,2), (18,1),$$

Let us now first calculate f'(18). The distinct resolutions of 18 will be:

1 factor 18;

2 factors 2,9; 3,6; 6,3; 9,2;

3 factors 2,3,3; 3,2,3; 3,3,2;

Hence,

$$f'(18) = (-1)^1 \frac{f(18)}{f(1)} + (-1)^2 \left[\frac{f(2)f(9)+f(3)f(6)+f(6)f(3)+f(9)f(2)}{f^2(1)} \right]$$

$$+ (-1)^3 \left[\frac{f(2)f(3)f(3)+f(3)f(2)f(3)+f(3)f(3)f(2)}{f^3(1)} \right]$$

$$= -\frac{f(18)}{f(1)} + 2\frac{f(2)f(9)}{f^2(1)} + 2\frac{f(3)f(6)}{f^2(1)} - 3\frac{f(2)f^2(3)}{f^3(1)}$$

Similarly, we get

$$f'(9) = (-1)^1 \frac{f(9)}{f(1)} + (-1)^2 \left[\frac{f(3)f(3)}{f^2(1)}\right]$$

$$= -\frac{f(9)}{f(1)} + \frac{f^2(3)}{f^2(1)}$$

$$f'(6) = (-1)^1 \frac{f(6)}{f(1)} + (-1)^2 \left[\frac{f(2)f(3) + f(3)f(2)}{f^2(1)}\right]$$

$$= -\frac{f(6)}{f(1)} + 2\frac{f(2)\,f(3)}{f^2(1)}$$

$$f'(3) = (-1)^1 \frac{f(3)}{f(1)} = -\frac{f(3)}{f(1)}$$

$$f'(2) = -\frac{f(2)}{f(1)}$$

$$f'(1) = 1$$

$$\therefore \sum f(d)\, f'(\delta) = f(1)f'(18) + f(2)f'(9) + f(3)f'(6) + f(6)f'(3)$$
$$+ f(9)f'(2) + f(18)f'(1)$$

$$= f(1)\left[-\frac{f(18)}{f(1)} + 2\frac{f(2)f(9)}{f^2(1)} + 2\frac{f(3)f(6)}{f^2(1)} - 3\frac{f(2)f^2(3)}{f^3(1)}\right]$$

$$+ f(2)\left[-\frac{f(9)}{f(1)} + \frac{f^2(3)}{f^2(1)}\right] + f(3)\left[-\frac{f(6)}{f(1)} + 2\frac{f(2)f(3)}{f^2(1)}\right]$$

$$+ f(6)\left[-\frac{f(3)}{f(1)}\right] + f(9)\left[-\frac{f(2)}{f(1)}\right] + f(18)$$

$$= 0$$

Thus the theorem is verified for n = 18.

Now, we proceed to the proof of the theorem itself.

Proof:

When n = 1, the theorem is trivial. It remains to prove the case when $n > 1$.

Glancing at the example given above, it is seen that to prove

$$\lesssim f(d)\ f'(\delta) = 0 \qquad \text{for } n > 1,$$

it is sufficient to prove that the coefficient of the particular term

$$f(d_1)\ f(d_2)\ f(d_3)\ \ldots\ldots\text{for } (d_k)$$

where the values of $d_1, d_2, d_3, \ldots\ldots d_k$ are fixed except as to order, is zero in the sum

$$\lesssim f(d)\ f'(\delta) \qquad , \quad n > 1 \ \ldots\ldots\ldots (2)$$

k being defined by $1 \leq k \leq \alpha(n)$.

It is evident that the only terms in (2) contributing to the required coefficient will occur only in those of the following products for which the arguments of f are distinct:

$$f(1)\ f'(n), \quad f(d\ )\ f'(\tfrac{n}{d_1}), \ldots\ldots f(d_k)\ f'(\tfrac{n}{d_k})$$

Let $A_k(n)$ denote the total number of distinct resolutions of n into k factors each greater than 1, while each of the resolutions is constructed from the fixed (except as to

order) values $d_1, d_2, \ldots\ldots, d_k$; and similarly let $A_{k-1}(\frac{n}{d_i})$ denote the total number of distinct resolutions of $\frac{n}{d_i}$ into k-1 factors each greater than 1, each resolution being constructed from the same set of values only with d_i omitted. Then it is seen immediately that the required coefficient is

$$\frac{(-1)^k}{f^{k-1}(1)}\left[A_k(n) - \sum{}' A_{k-1}\left(\frac{n}{d_i}\right)\right]$$

where $\sum'$ extends only to those d_i, each counted once only, that occurs among the set of fixed values $d_1, d_2, \ldots\ldots, d_k$. The point here is that $\sum'$ refers only to those of the $d_1, d_2, \ldots\ldots\ldots, d_k$ that are distinct.

It remains to find the value of $A_k(n)$ and $A_{k-1}(\frac{n}{d_i})$. In finding $A_k(n)$, we have to determine only the number of different ways in which the k fixed values $d_1, d_2, \ldots\ldots, d_k$ may be rearranged among themselves.

Let $d_1, d_2, \ldots\ldots\ldots, d_y$ be the distinct factors among the k fixed factors $d_1, d_2, \ldots\ldots\ldots, d_k$ and let

$$k = r\,y + z, \qquad 0 \leq z < y \ldots\ldots\ldots\ldots (3)$$

We may arrange the d's into sets S_i, S_{z+j} ($i = 1,2,\ldots\ldots\ldots,z$; $j = 1,2, \ldots\ldots\ldots, y-z$)

$$d_1 , d_2 , \ldots\ldots\ldots, d_z , \ldots\ldots, d_y ,$$
$$d_{y+1} , d_{y+2} , \ldots\ldots\ldots, d_{y+z} , \ldots\ldots, d_{2y},$$
$$d_{2y+1} , d_{2y+2} , \ldots\ldots\ldots, d_{2y+z} , \ldots\ldots, d_{3y},$$
$$\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots$$
$$d_{(r-1)y+1}, d_{(r-1)y+2}, \ldots\ldots\ldots, d_{(r-1)y+z}, \ldots\ldots d_{ry},$$
$$d_{ry+1} , d_{ry+2} \ldots\ldots\ldots, d_{ry+z},$$

with $S_i \equiv d_{ay+i}$ (a = 0, 1, 2, ..., r)

$S_{z+j} \equiv d_{by+z+j}$ (b = 0, 1, 2, ..., r-1)

such that all the factors in each set S_i are equal ,

i.e. $d_i = d_{y+i} = d_{2y+i} = \ldots\ldots\ldots = d_{(r-1)y+i} = d_{ry+i}$

and all the factors in each set S_{z+j} are equal,

i.e. $d_{z+j} = d_{y+z+j} = d_{2y+z+j} = \ldots\ldots\ldots\ldots = d_{(r-1)y+z+j}$

but no factor in any set is equal to any factor of any other set. Hence, the resolution

$$n = d_1 d_2 d_3 \ldots\ldots\ldots\ldots d_k \qquad \ldots\ldots\ldots (4)$$

is equivalent to

$$n = (d_1 d_2 \ldots\ldots\ldots d_z)^{r+1} (d_{z+1} d_{z+2} \ldots\ldots d_y)^r \ldots\ldots (5)$$

where all $d_1, d_2, \ldots\ldots d_z, d_{z+1}, d_{z+2}, \ldots\ldots\ldots\ldots d_y$ are distinct.

The total number of factors is thus

$$z (r + 1) + (y - z)r = yr + z = k$$

which coincides with our assumption in (3).

Since (4) is equivalent to (5), therefore the number of different arrangements of the d's in (4) is equal to the number of different arrangements of the d's in (5). By definition of $A_k(n)$, we can say

$$A_k(n) = \frac{k\,!}{\left[(r+1)!\right]^z \, (r\,!)^{y-z}}$$

Similarly it follows that

$$A_{k-1}\left(\frac{n}{d_i}\right) = \frac{(k-1)!}{\left[\left[(r+1)!\right]^{z-1} r\,!\right] (r!)^{y-z}} \quad (i=1,2,..,z)$$

$$A_{k-1}\left(\frac{n}{d_j}\right) = \frac{(k-1)!}{\left[(r+1)!\right]^z \left[(r!)^{y-z-1}(r-1)!\right]} \quad (j=z+1, z+2 \ldots, y)$$

or we can write

$$A_{k-1}\left(\frac{n}{d_i}\right) = \frac{r+1}{k} A_k(n)$$

$$A_{k-1}\left(\frac{n}{d_j}\right) = \frac{r}{k} A_k(n)$$

Therefore $A_k(n) - \sum' A_{k-1}\left(\frac{n}{d_i}\right)$

$$= A_k(n) - \sum_{i=1}^{z} A_{k-1}\left(\frac{n}{d_i}\right) - \sum_{j=z+1}^{y} A_{k-1}\left(\frac{n}{d_j}\right)$$

$$= A_k(n) - z\left(\frac{r+1}{k}\right) A_k(n) - (y-z)\left(\frac{r}{k}\right) A_k(n)$$

$$= A_k(n)\left[1 - \frac{z(r+1)}{k} - \frac{(y-z)\,r}{k}\right]$$

$$= A_k(n) \left[\frac{k - zr - yr + zr}{k} \right]$$

$$= A_k(n) \left[\frac{k - (z + yr)}{k} \right]$$

$$= A_k(n) \left[\frac{k - k}{k} \right]$$

$$= 0$$

$$\therefore \quad \frac{(-1)^k}{f^{k-1}(1)} \left[A_k(n) - \sum{}' A_{k-1}\left(\frac{n}{d_i}\right) \right] = 0$$

$$\Longrightarrow \qquad f(d) \quad f'(\delta) = 0$$

Thus the proof is complete.

A special case of the above theorem is also noteworthy. It is the case when the numerical function f(n) is restricted to be multiplicative. In which case, the f'(n) is usually called the inverse of f(n), (same as the $f^{-1}(n)$ defined in Chapter I) which is also a multiplicative function itself. With the multiplicative property of f(n) and f'(n), the proof of the theorem is much simpler. Here we shall give a proof of the above theorem with the restriction that f(n) and f'(n) are multiplicative.

Proof:

Now let $n = p_1^{\alpha} p_2^{\beta} \ldots\ldots\ldots$

with the p's being prime numbers. Since f(n) is multiplicative,

$$\therefore \quad f(n) = f\left(p_1^{\alpha} \right) f\left(p_2^{\beta} \right) \ldots\ldots\ldots$$

Thus from arbitrary values associated with prime-power values of n, we can build up a unique multicative function.

Suppose that we are able to determine numbers $f'(p^{\alpha})$

for every prime p, and every index α, such that

$$\sum_{d/p} f\left(\frac{p^{\alpha}}{d}\right) f'(d) = \begin{cases} f(1) & \text{for } \alpha = 0 \\ 0 & \text{for } \alpha > 0 \end{cases} \quad \ldots\ldots\ldots (6)$$

Let $f'(n)$ be the multiplicative function constructed from the values $f'(p^{\alpha})$, Since f and f' thus defined are both multiplicative, then the composite F is also multiplicative. We recall that the definition of composite F of f_1 and f_2 is given by

$$F(n) = \sum_{d/n} f_1(d) \; f_2\left(\frac{n}{d}\right)$$

Therefore,

$$F(n) = F(p_1^{\alpha}) \; F(p_2^{\beta}) \ldots\ldots\ldots\ldots$$

But from (6), each $F(p^{\alpha}) = f(1)$ or 0, according as α is equal or greater than zero. Also since $f(n)$ is multiplicative, so it implies that $f(1) = 1$.

$\therefore \; f^k(1) = 1^k = f(1)$ for any integer $k > 0$

Hence

$$F(n) = \sum_{d/n} f\left(\frac{n}{d}\right) f'(d)$$

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

Thus the theorem is proved, provided we can determine numbers $f'(p^{\alpha})$, satisfying equations of the type (6). However, the determination of the numbers $f'(p^{\alpha})$ is just a matter of straight-forward solution of linear equations. Thus, for given p, α, the equations (6) are:

$$
\begin{aligned}
&f(p) + f'(p) && = 0\\
&f(p^2) + f(p)\,f'(p) + f'(p^2) && = 0\\
&\quad\vdots \qquad\quad \vdots && \quad\vdots\\
&f(p^{\alpha}) + f(p^{\alpha-1})f'(p) + \ldots + f'(p^{\alpha}) && = 0
\end{aligned}
$$

Solving these, we have:

$$
(-1)^{\alpha} f'(p^{\alpha}) = \begin{vmatrix}
f(p) & 1 & 0 & 0 \ldots\ldots 0\\
f(p^2) & f(p) & 1 & 0 \ldots\ldots 0\\
\vdots & \vdots & & \\
f(p^{\alpha-1}) & f(p^{\alpha-2}) & \ldots\ldots\ldots f(p) & 1\\
f(p^{\alpha}) & f(p^{\alpha-1}) & \ldots\ldots\ldots\ldots & f(p)
\end{vmatrix}
$$

Thus, with these numbers $f'(p^{\alpha})$, our proof is complete.

Before we prove a statement of Liouville to illistrate one use of the theorem stated above, we first note a fact which is of considerable importance. We see that

$$\sum_n \left[f_1(d) \sum_{\delta} f_2(\delta_1)\, f_3(\delta_2) \right]$$

and $$\sum_n f_1(d_1)\, f_2(d_2)\, f_3(d_3)$$

are identical, where the first of which $\sum_n$ refers to all d, δ such that $d\delta = n$ and $\sum_{\delta}$ to all δ_1, δ_2 such that $\delta_1 \delta_2 = \delta$; and in the second, $\sum_n$ refers to all d_1, d_2, d_3 such that $d_1 d_2 d_3 = n$.

Similarly,

$$\sum_n \left[f_1(d) \sum_{\delta} f_2(\delta_1)\, f_3(\delta_2)\, f_4(\delta_3) \right] ,$$

$$n = d\delta, \quad \delta = \delta_1\delta_2\delta_3 ,$$

$$\sum_n \left[\sum_d f_1(d_1)\, f_2(d_2) \sum_{\delta} f_3(\delta_1)\, f_4(\delta_2) \right],$$

$$n = d\delta, \; d = d_1 d_2, \; \delta = \delta_1\delta_2,$$

$$\sum_n f_1(d_1)\, f_2(d_2)\, f_3(d_3)\, f_4(d_4),$$

$$n = d_1 d_2 d_3 d_4.$$

are all equal. This applies to any number of functions, which, moreover, need not be all distinct.

Illustration of the use of Theorem I

Now we shall prove a statement of Liouville, which states that if

$$\sum_n A(d)\ B(\delta) = \sum_n C(d)\ D(\delta) \quad \ldots\ldots\ldots\ldots\ldots\ldots (7)$$

and

$$\sum_n A(d)\ E(\delta) = \sum_n C(d)\ F(\delta) \quad \ldots\ldots\ldots\ldots\ldots\ldots (8)$$

for all positive integral values of n where A, B, C, D, E, F, are all numerical functions of n, then

$$\sum_n F(d)\ B(\delta) = \sum_n E(d)\ D(\delta) \quad \ldots\ldots\ldots\ldots\ldots\ldots (9)$$

for like values of n.

Proof:

Here we shall use multiple summation. Let n be resolved into sets of factors each greater than 1.

(7) then becomes

$$\sum_{\delta} A(\delta_1)\ B(\delta_2) = \sum_{\delta} C(\delta_1)\ D(\delta_2)$$
$$\delta = \delta_1 \delta_2 \ ,$$

since (7) is valid for all n, and hence for the positive integer δ.

Multiplying (10) by C'(d), the reciprocal of C(d) (as defined in Theorem I) and summing the result with respect to all d, we have

$$\sum_n \left[C'(d) \sum_{\delta} C(\delta_1)\ D(\delta_2) \right] = \sum_n \left[C'(d) \sum_{\delta} A(\delta_1)\ B(\delta_2) \right]$$
$$n = d\,\delta \ ,$$

or

$$\sum_n \left[D(d) \sum_{\delta} C'(\delta_1)\ C(\delta_2) \right] = \sum_n \left[A(d_1)\, C'(d_2)\ B(d_3) \right]$$
$$n = d_1\, d_2\, d_3 \ ,$$

By theorem I, we have

$$C(1)\ D(n) = \sum_n A(d_1)\ C'(d_2)\ B(d_3)$$

or we can replace n by δ and get

$$C(1)\ D(\delta) = \sum_{\delta} A(\delta_1')\ C'(\delta_2')\ B(\delta_3') \qquad \delta = \delta_1'\delta_2'\delta_3' \qquad \text{.....(11)}$$

Similarly, we get from (8)

$$A(1)\ E(d) = \sum_d A'(d_1')\ C(d_2')\ F(d_3') \qquad \text{.....(12)}$$

$$d = d_1'\ d_2'\ d_3'$$

Multiplying the corresponding members of (11) and (12) and summing the result over all pairs (d,δ), we have

$$\begin{aligned} A(1)\ C(1) \sum_n E(d)\ D(\delta) &= \sum_n \left[\sum_d A'(d_1')\ C(d_2')\ F(d_3') \sum_{\delta} A(\delta_1')\ C'(\delta_2')\ B(\delta_3')\right] \\ &= \sum_n \left[\sum_{d_1} A'(d_1'')\ A(\delta_1'') \sum_{d_2} C(d_2'')\ C'(\delta_2'') \sum_{d_3} F(d_3'')B(\delta_3'')\right] \\ &\qquad d_1 = d_1''\delta_1'', \quad d_2 = d_2''\delta_2'', \quad d_3 = d_3''\delta_3'' \\ &= A(1)\ C(1) \sum_n F(d)\ B(\delta) \qquad \text{(by Theorem I)} \end{aligned}$$

Dividing out the common factor $A(1)\ C(1)$, we then get

$$\sum_n E(d)\ D(\delta) = \sum_n F(d)\ B(\delta)$$

Here, we can see how Theorem I can be applied to prove Liouville's statement.

Some inversion formulas:

Now, with the fundamental block of inversion being set up, more and more inversion formulas have been established to

embellish the whole theory of inversion.

Here, we shall choose a few most important inversion formulas and discuss them accordingly.

§ I. Baker's inversion formula (1890)

H. F. Baker [3] established an inversion formula which states as follows:

Let $a_1,\ldots\ldots,a_n$ be distinct primes and S any set of positive integers. For $k \leq n$, let $F(a_1,\ldots\ldots,a_k)$ denote the set of all the numbers in S which are divisible by each of the primes $a_{k+1}, a_{k+2},\ldots\ldots, a_n$, so that $F(a_1,\ldots\ldots,a_n) = S$.

For k=0, write F(0) for F, so that F(0) consists of the numbers of S which are divisible by $a_1,\ldots\ldots,a_n$. We now divide $F(a_1,\ldots.a_k)$ into subsets. Those of its numbers which are divisible by no one of $a_1,\ldots\ldots,a_k$ form the subset $f(a_1,\ldots\ldots,a_k)$. Those divisible by a_1, but by no one of $a_2,\ldots.,a_k$, form the subset $f(a_2,a_3,\ldots a_k)$. Those divisible by a_1 and a_2, but by no one of $a_3,a_4,\ldots.,a_k$ form the subset $f(a_3,a_4,\ldots\ldots,a_k)$. Finally, those divisible by $a_1,\ldots$ a_k form the subset f(0). Thus $F(a_1,\ldots\ldots a_k)$ is defined by

$$F(a_1,a_2,\ldots\ldots,a_k) = f(a_1,a_2,\ldots.,a_k) + \sum_1 f(a_2,a_3,\ldots,a_k) + \sum_2 f(a_3,a_4,\ldots,a_k) + \ldots\ldots + \sum_{k-1} f(a_1) + f(0) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

where $\sum_r$ indicates a summation extending to all selections of k-r of the artuments $a_1,a_2,\ldots.,a_k$; the inversion is stated in the form:

$$f(a_1,a_2,\ldots\ldots,a_n) = F(a_1,a_2,\ldots\ldots,a_n) - \sum_1 F(a_2,a_3,\ldots\ldots,a_n) + \sum_2 F(a_3,a_4,\ldots\ldots,a_n) + \ldots\ldots + (-1)^{n-1}\sum_{n-1} F(a_1) + (-1)^n F(0) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

The inversion is proved by counting the number of times that a particular f occurs when each F is replaced by its equivalent as defined by (1). For example, the function $f(0)$ will occur once from $F(a_1,a_2,\ldots\ldots,a_n)$.

$\binom{n}{1} = \dfrac{n!}{1!\,(n-1)!}$ times from $\sum_1 F(a_2, \ldots\ldots, a_n)$

$\binom{n}{2} = \dfrac{n!}{2!\,(n-2)!}$ times from $\sum_2 F(a_3, \ldots\ldots, a_n)$

$\vdots$

$\binom{n}{n-1} = \dfrac{n!}{(n-1)!\,1!}$ times from $\sum_{n-1} F(a_1)$

$\binom{n}{n} = 1$ time from $F(0)$

$\therefore \quad 1 - \binom{n}{1} + \binom{n}{2} - \ldots\ldots + (-1)^{n-1}\binom{n}{n-1} + (+1)^n\binom{n}{n}$

$= (1-1)^n = 0$

$\therefore$ $f(0)$ occurs none at all in (2).

Similarly, $f(a_1)$ is seen to occur, on the whole, $(1-1)^{n-1} = 0$ times in (2).

With the same argument, we can prove that all the functions $f(a_1, a_2, \ldots, a_k)$ (with $k < n$) actually donot occur in (2). Thus only the function $f(a_1, a_2, \ldots, a_n)$ is left and (2) is obvious.

§ II. Cohen's first inversion principle (1959)

E. Cohen [12] established the following inversion principle:

Let $f(n,r)$ be a complex-valued even function of n (mod r). Then if $r = r_1 r_2$, where r_1 and r_2 are positive integers, it follows that

$$f(n, r) = \sum_{d/(n,r)} h(d, \tfrac{r}{d})$$

$$\rightleftharpoons \quad h(r_1, r_2) = \sum_{d/r_1} f(\tfrac{r_1}{d_1}, r)\mu(d)$$

First of all, we shall define what an even function is.

Definition I : A function $f(n,r)$ is called even (mod r) if

$$f(n,r) = f((n,r), r)$$

where $f(n,r)$ denotes a complex-valued arithemetical function of n and r, and n, r are integers with r necessarily positive.

Let us now proceed to the proof of the above inversion principle itself.

Proof:

A. By assumption, $f(n,r)$ is defined by

$$f(n,r) = \sum_{d/(n,r)} h(d, \tfrac{r}{d})$$

Then, using the relation $r = r_1 r_2$, we have

$$\sum_{d/r_1} f(\tfrac{r_1}{d}, r)(d) = \sum_{d/r_1} \sum_{\delta/(\frac{r_1}{d_1}, r)} h(\delta, \tfrac{r}{\delta})\mu(d)$$

$$= \sum_{d/r_1} \mu(d) \sum_{\delta/(\frac{r_1}{d_1}, r)} h(\delta, \tfrac{r}{\delta})$$

$$= \sum_{\delta/r_1} h(\delta, \tfrac{r}{\delta}) \sum_{d/\frac{r_1}{\delta}} \mu(d)$$

$$= h(r_1, r_2)$$

$$\therefore \sum_{d/n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases} \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Thus we have completed the first part of the proof.

B. We assume this time that

$$h(r_1, r_2) = \sum_{d/r_1} f\left(\frac{r_1}{d}, r\right)\mu(d)$$

with $r = r_1 r_2$.

Now, we have

$$\sum_{d/(n,r)} h\left(d, \frac{r}{d}\right) = \sum_{d/(n,r)} \sum_{\delta/d} f\left(\frac{d}{\delta}, r\right)\mu(\delta)$$

$$= \sum_{d/(n,r)} f(\beta, r)\mu(\delta)$$

$$= \sum_{\beta/(n,r)} f(\beta, r) \sum_{\delta/\frac{(n,r)}{\beta}} \mu(\delta)$$

$$= f((n,r), r) \qquad (\text{by } (1))$$

by definition of an even function (mod r)

$$f(n,r) = f((n,r), r)$$

$\therefore$ the converse of A is proved also.

The stated inversion formula leads immediately to a characterization of the class of even functions (mod r), which shows that:

A function $f(n,r)$ is even (mod r) if and only if it has a representation of the form

$$f(n,r) = \sum_{d/(n,r)} h\left(d, \frac{r}{d}\right)$$

and the function $h(r_1, r_2)$ is uniquely determined by

$$h(r_1, r_2) = \sum_{d/r_1} f\left(\frac{r_1}{d}, r\right)\mu(d)$$

for positive values of r_1 and r_2.

We note that the above inversion formula is reduced to the ordinary Möbius inversion formula when $f(n,r)$ is restricted to the subclass of completely even functions (mod r), that is, functions satisfying $f(n,r) = f(n', r')$ for all n, n' and all positive r, r' such that $(n,r) = (n', r')$

In mathematical terms, we get the Möbius inversion formula from the above inversion formula by replacing $h(r_1, r_2)$ by $h(r_1)$ and $f(n,r)$ by $g((n,r))$ and putting $r_2 = 1$

i.e. we have the following statement (2) :

Let $f(n,r)$ be a completely even function (mod r). It follows that

$$f(n,r) = g((n,r)) = \sum_{d/(n,r)} h(d)$$

$$\rightleftharpoons \quad h(r) = \sum_{d/r} f\left(\frac{r}{d}, r\right)\mu(d)$$

$$= \sum_{d/r} g\left(\frac{r}{d}\right)\mu(d)$$

Thus, as in the case of the even functions (mod r) being characterized by Cohen's first inversion principle, the class of completely even functions (mod r) is characterized by (2).

§ Proof of Brauer - Rademacher identity

Now, we shall give a proof of the Brauer-Rademacher identity [13]

$$\phi(r) \sum_{\substack{d/r \\ (d,n)=1}} \frac{d}{\phi(d)}\mu\left(\frac{r}{d}\right) = \mu(r) \sum_{d/(n,r)} d\,\mu\left(\frac{r}{d}\right) \quad \ldots(3)$$

as an illustration of the inversion principle which we just proved above. But before proving the identity itself, it is necessary

to introduce a few definitions and some lemmas on $\phi(r)$ and $\mu(r)$ first.

Lemma I :

$$\phi(n) = \sum_{d/n} \mu(d) \frac{n}{d}$$

Proof:

We know that $\phi(n)$ is the number of positive integers less than or equal to n that are relatively prime to n. Let T denote the set of integers 1,2,....., n, i.e. the set of integers i satisfying $1 \leq i \leq n$. We then separate T into subsets T_d where d/n, by putting i into T_d if $(i,n) = d$. Then each element of T is in exactly one T_d. Moreover, i is in T_d if and only if i is of the form j d with $1 \leq j \leq \frac{n}{d}$, and $(j, \frac{n}{d}) = 1$. Therefore there are exactly $\phi(\frac{n}{d})$ elements in T_d. Since there are n elements in T, we have $n = \sum_{d/n} \phi(\frac{n}{d})$ which is the same as $n = \sum_{d/n} \phi(d)$.

By Möbius inversion formula, we thus have

$$\phi(n) = \sum_{d/n} \mu(d) \frac{n}{d}$$

Lemma 2 :

If q is an integer ≥ 2 and p is a prime, then

$$\phi(p^q) = p\,\phi(p^{q-1})$$

Proof:

Then by lemma 1, we have

$$\phi(p^t) = \mu(1)\,p^t + \mu(p)\,p^{t-1} + \ldots\ldots + \mu(p^t)$$

$$= p^t + (-1)^p\,p^{t-1} + 0$$

$$= p(p^{t-1} - p^{t-2}) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

$\therefore \phi(p^{t-1}) = p^{t-1} - p^{t-2}$

$\therefore$ (4) becomes $\phi(p^t) = p\,\phi(p^{t-1})$

Thus, the lemma follows immediately.

Definition 2:

The core $\gamma(r)$ of r is defined to be 1 if $r = 1$, and to be the product of the distinct prime factors of r if $r > 1$.

Definition 3:

An integer r is called primitive if r contains no square divisors > 1; and called non-primitive if it does.

From the definitions above, we can see that $\mu(r) \neq 0$, if r is primitive and $\mu(r) = 0$ if r is non-primitive.

Lemma 3 ;

If r is primitive, and s is an integer > 1 such that $\gamma(s)/r$, then

$$\sum_{d/r} \frac{d\ \mu(d)}{\phi\ (ds)} = 0$$

Proof:

Let $r = r_1 r_2$; $(r_1, r_2) = 1$, and $s = s_1 s_2 > 1$

Since $\gamma(s)/r$,

$\therefore$ $\gamma(s_1)/r_1$ and $\gamma(s_2)/r_2$

Thus the multiplicative properties of $\phi(r)$ and $\mu(r)$ imply that

$$\sum_{d/r} \frac{d\,\mu(d)}{\phi\,(ds)} = \sum_{d_1/r_1} \frac{d_1\,\mu(d_1)}{\phi\,(d_1 s_1)} \sum_{d_2/r_2} \frac{d_2\,\mu(d_2)}{\phi\,(d_2 s_2)}$$

where d_1 denotes the divisors of r_1 and d_2 denotes the divisors of r_2.

Since either $s_1 > 1$ or $s_2 > 1$, so it suffices to prove

the lemma in case r = p (a prime) and s = p^k, k > 0.

But $$\sum_{d/p} \frac{d\,\mu(d)}{\phi(dp^k)} = \frac{1}{\phi(p^k)} - \frac{p}{\phi(p^{k+1})}$$

which, by lemma 1, is equal to

$$= \frac{1}{p\phi(p^{k-1})} - \frac{p}{p\,\phi(p^k)}$$

$$= \frac{1}{\phi(p^k)} - \frac{1}{\phi(p^k)}$$

$$= 0$$

the lemma is proved.

Lemma 4 :

If r is primitive and d is a divisor of r, then

$$\mu\left(\frac{r}{d}\right) = \mu(r)\mu(d)$$

Proof:

Since r is primitive and by the multiplicativity of $\mu(r)$ we have

$$\mu\left(\frac{r}{d}\right) = \mu\left(\frac{r}{d}\right)\mu^2(d)$$

$$= \mu\left(\frac{r}{d}\,d^2\right)$$

$$= \mu(r)\mu(d)$$

Lemma 5:

$$\sum_{d/r,\ (\frac{r}{d},n)=1,} \mu(d) = \begin{cases} \mu(r) & \text{if } r/n \\ 0 & \text{otherwise} \end{cases}$$

where the summation is over divisors d of r whose conjugate divisors $\frac{r}{d}$ are prime to n.

Proof:

When n = 1, we have

$$\sum_{d/r} \mu(d) = e(r)$$

where $e(r)$ is defined to be $= \begin{cases} 1 & \text{if } r = 1 \\ 0 & \text{otherwise} \end{cases}$

We then have

$$\sum_{\substack{d/r, \\ (\frac{r}{d}, n)=1}} \mu(d) = \sum_{d/r} \mu(d) \; e\left(\left(\tfrac{r}{d}, n\right) \right)$$

$$= \sum_{d/r} \mu(d) \sum_{\delta/(\frac{r}{d}, n)} \mu(\delta)$$

$$= \sum_{\delta/(n,r)} \mu(\delta) \sum_{d/(\frac{r}{\delta})} \mu(d)$$

$$= \sum_{\delta/(n,r)} \mu(\delta) \; e\left(\tfrac{r}{d}\right)$$

Thus by the definition of $e(r)$, we then get

$$\sum_{\substack{d/r \\ (\frac{r}{d}, n) = 1}} \mu(d) = \begin{cases} \mu(r) & \text{if } r/n \\ 0 & \text{otherwise} \end{cases}$$

<u>Proof of the Brauer-Rademacher identity</u>:

Let us denote the left hand side of (3) by $A(n,r)$. Evidently $A(n,r)$ is an even function (mod r), thus we can apply the inversion formula to obtain

$$A(n,r) = \sum_{d/(n,r)} H\left(d, \tfrac{r}{d}\right) \quad \ldots\ldots\ldots\ldots\ldots (5)$$

where $h(r_1, r_2) = \sum_{\substack{\delta/r_1 \\ r = r_1 r_2,}} A\left(\tfrac{r_1}{\delta}, r\right) \mu(\delta)$

Hence, by definition of $A(n,r)$, we have

$$h(r_1, r_2) = \phi(r) \sum_{d/r} \frac{d}{\phi(d)} \mu\left(\tfrac{r}{d}\right) \sum_{\substack{\delta/r_1 \\ (d, \frac{r_1}{\delta}) = 1}} \mu(\delta) \quad \ldots\ldots (6)$$

By lemma 5, $\sum_{\substack{\delta / r_1 \\ (d, \frac{r_1}{\delta})=1}} \mu(\delta)$ is equal to zero unless r_1/d, in which case it has the value $\mu(r_1)$. When r_1/d, we can write

$d = r_1 m$, (6) becomes

$$h(r_1, r_2) = \phi(r)\, r_1 \mu(r_1) \sum_{m/r_2} \frac{m}{\phi(r_1 m)} \mu\left(\frac{r_2}{m}\right)$$

$\because \mu\left(\frac{r_2}{m}\right)$ is zero unless $\frac{r_2}{m} / \gamma(r_2)$

therefore we may put $m = \left[\frac{r_2}{\gamma(r_2)}\right] e$ to obtain

$$h(r_1, r_2) = \frac{\phi(r)\, \mu(r_1)\, r}{\gamma(r_2)} \sum_{e/\gamma(r_2)} \frac{e\, \mu\left[\frac{\gamma(r_2)}{e}\right]}{\phi\left[\frac{re}{\gamma(r_2)}\right]}$$

Now put $\frac{r}{\gamma(r_2)} = R_1 R_2$, where $\gamma(R_2) / r_2$ and $(R_1, r_2) = 1$.

We see at once that R_1/r_1. Then by lemma (4) and the multiplicativity of $\phi(r)$ we have

$$h(r_1, r_2) = \frac{r\, \phi(r)\, \mu(r_1)\, \mu(\gamma(r_2))}{\gamma(r_2)\, \phi(R_1)} \sum_{e/\gamma(r_2)} \frac{e\, \mu(e)}{\phi(R_2 e)} \quad \ldots\ldots(7)$$

By lemma 3, the sum in (7) is zero unless $R_2 = 1$. But $R_2 = 1$

$\Rightarrow r_1 r_2 = r = R_1 \gamma(r_2)$ so that

$$\left(\frac{r_1}{R_1}\right) r_2 = \gamma(r_2)$$

Hence, $h(r_1, r_2) = 0$ unless $r_2 = \gamma(r_2)$ and $R_1 = r_1$, and in particular, unless r_2 is primitive and $(r_1, r_2) = 1$.

We can see that $h(r_1, r_2) = 0$ if r is non-primitive;

i.e. $h(r_1, r_2) = 0$, if $\mu(r) = 0$ .....(8)

Thus in the remainder of the proof, we suppose that r is primitive;

so that $r_2 = \gamma(r_2)$, $R_2 = 1$, $(r_1, r_2) = 1$, $R_1 = r_1$,

Hence (7) becomes

$$h(r_1, r_2) = r_1 \phi(r_2) \mu(r) \sum_{e/r_2} \frac{e\mu(e)}{\phi(e)}$$

$$= r_1 \mu(r) \sum_{e/r_2} e\mu(e) \phi\left(\frac{r_2}{e}\right)$$

By lemma 1 and lemma 4, we have

$$h(r_1, r_2) = r_1 \mu(r_1) \sum_{e/r_2} e\mu(e) \sum_{\delta/\frac{r_2}{e}} \delta\mu(e\delta) \ldots (9)$$

Putting $\delta e = D$ in (9) we get

$$h(r_1, r_2) = r_1 \mu(r_1) \sum_{e/r_2} \mu(e) \sum_{D/r_2, e/D} D\mu(D)$$

$$= r_1 \mu(r_1) \sum_{D/r_2} D\mu(D) \sum_{e/D} \mu(e)$$

$\because$ $\sum_{d/r} \mu(d) = \begin{cases} 1 & \text{if } r = 1 \\ 0 & \text{if } r > 1 \end{cases}$

$\therefore$ $h(r_1, r_2) = r_1 \mu(r_1)$ if $\mu(r) \neq 0$ .....(10)

Combining (8) and (10) into a single formula thus we have, for all r,

$$h(r_1, r_2) = \mu(r)\, r_1 \mu(r_2) \ldots\ldots\ldots\ldots\ldots\ldots\ldots (11)$$

Substituting (11) in (5), we finally get

$$A(n,r) = \sum_{d/(n,r)} \mu(r)\, d\mu\left(\frac{r}{d}\right)$$

$$= \mu(r) \sum_{d/(n,r)} d\mu\left(\frac{r}{d}\right)$$

Thus the Brauer-Rademacher identity is proved.

§ III Cohen's Second Inversion Principle:

Along with the inversion principle relating to the class of all even functions (mod r), which we discussed above, E. Cohen developed also another inversion principle limited to

the primitive functions (mod r) only this time.

Definition 4:

A complex-valued arithmetical function $f(n,r)$ is called primitive (mod r) if $f(n,r) = f(\gamma(n,r), r)$ for all n while $\gamma(n,r) = \gamma((n,r))$ and $\gamma((n,r))$ is the core of (n,r).

Definition 5:

A completely primitive function $f(n,r)$ (mod r) is defined as one satisfying $f(n,r) = f(n',r')$ for all n, n' and all positive r, r' such that

$$\frac{\gamma(r)}{\gamma(n,r)} = \frac{\gamma(r')}{\gamma(n', r')}$$

Definition 6:

$\chi(n,r)$ is defined by

$$\chi(n,r) = \sum_{d/(n,r)} d\mu\left(\frac{r}{d}\right)$$

Before introducing the inversion principle itself, we have to go through a few lemmas which are needed in the proof of the inversion principle. Nevertheless, the proofs of the following lemmas are quite obvious, mainly based on the multiplicative properties of $\mu(r)$ and $\chi(n,r)$, while r is taken as the power of a prime, so we shall just state them without going into the proofs.

Lemma 6:

If $r = r_1 r_2$, r_1 is primitive, and $\delta / \gamma(r)$, then

$$\sum_{\substack{d/\frac{r\, r_1}{\gamma(r)} \\ (\delta, \frac{r}{d}) = 1}} \chi(r_2, d) = \begin{cases} \frac{r\ \mu(r_1)}{\gamma(r)} & \text{if } \delta = r_1 \\ 0 & \text{if } \delta \neq r_1 \end{cases}$$

Lemma 7:

If $r = r_1 r_2$, then

$$\sum_{\substack{d\delta = r \\ (\delta, r_2) = 1}} \chi(r_1, d) = r_1 \mu(r_2)$$

Lemma 8:

If r is primitive, r_2 / r, and r_1 / r_2, then

$$\sum_{\substack{d\rho = r \\ (d,n)=1 \\ \rho / r_1,\ d / r_2}} \mu(d) = \begin{cases} \mu\left[\frac{r}{(n,r)}\right] & \text{if } r_1 = (n,r),\ r_2 = r; \\ 0 & \text{otherwise,} \end{cases}$$

Theorem 2: (the inversion principle for the primitive functions)

Let r_1, r_2 be positive integers, and r_1 primitive. If $H(r_1, r_2)$ is a function of r_1, r_2 and $f(n,r)$ is a primitive function (mod r) and $r = r_1 r_2$, then it follows that

$$f(n,r) = \sum_{\substack{d / \gamma(r) \\ (d,n)=1}} H\left(d, \frac{r}{d}\right) \equiv \sum_{d / \frac{\gamma(r)}{\gamma(n,r)}} H\left(d, \frac{r}{d}\right) \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

$$\rightleftharpoons H(r_1, r_2) = \frac{\gamma(r)\,\mu(r_1)}{r} \sum_{d / \frac{r\,r}{\gamma(r)}1} f\left(\frac{r}{d}, r\right) \chi(r_2, d) \ldots (2)$$

Proof:

A. By applying our assumption that

$$f(n,r) = \sum_{\substack{d / \gamma(r) \\ (d,n) = 1}} H\left(d, \frac{r}{d}\right)$$

the right side of (2) becomes

$$\frac{\gamma(r)\,\mu(r_1)}{r} \sum_{d / \frac{r\,r}{\gamma(r)}1} f\left(\frac{r}{d}, r\right) \chi(r_2, d)$$

$$= \frac{\gamma(r)\mu(r_1)}{r} \sum_{d/\frac{r\,r_1}{\gamma(r)}} \left[\sum_{\substack{\delta/\gamma(r) \\ (\delta, \frac{r}{d})=1}} H(\delta, \tfrac{r}{\delta}) \right] \chi(r_2, d)$$

$$= \frac{\gamma(r)\ \mu(r_1)}{r} \sum_{\delta/\gamma(r)} H(\delta, \tfrac{r}{\delta}) \sum_{\substack{d/\frac{r\,r_1}{\gamma(r)} \\ (\delta, \frac{r}{d})=1}} \chi(r_2, d)$$

$$= \frac{\gamma(r)\ \mu(r_1)}{r} H(r_1, r_2) \frac{r\,\mu(r_1)}{\gamma(r)} \quad \text{by lemma (6)}$$

$$= \mu^2(r_1)\ H(r_1, r_2)$$

$= H(r_1, r_2)$, as r_1 is primitive.

B. We assume now

$$H(r_1, r_2) = \frac{\gamma(r)\mu(r_1)}{r} \sum_{d/\frac{r\,r_1}{\gamma(r)}} f(\tfrac{r}{d}, r)\chi(r_2, d)$$

Then

$$\sum_{\substack{d/\gamma(r) \\ (d,n)=1}} H(d, \tfrac{r}{d}) = \frac{\gamma(r)}{r} \sum_{\substack{d/\gamma(r) \\ (d,n)=1}} \mu(d) \sum_{\delta/\frac{dr}{\gamma(r)}} f(\tfrac{r}{\delta}, r)\chi(\tfrac{r}{d}, \delta)$$

$$= \frac{\gamma(r)}{r} \sum_{\delta/r} f(\tfrac{r}{\delta}, r) \sum_{\substack{d/\gamma(r) \\ (d,n)=1 \\ \frac{\gamma(r)}{d}/\frac{r}{\delta}}} \mu(d) \sum_{c/(\frac{r}{d}, \delta)} c\mu(\tfrac{\delta}{c})$$

$$= \frac{\gamma(r)}{r} \sum_{\delta/r} f(\tfrac{r}{\delta}, r) \sum_{c/\delta} c\,\mu(\tfrac{\delta}{c}) \sum_{\substack{d\rho = \gamma(r) \\ (d,n)=1 \\ d/\frac{r}{c},\ \rho/\frac{r}{\delta}}} \mu(d)$$

.....(3)

∵ by lemma (8),

$$\sum_{\substack{d\rho = \gamma(r) \\ (d,n)=1 \\ d/\frac{r}{c}, \rho/\frac{r}{\delta}}} \mu(d)$$ is equal to zero unless $\gamma(\tfrac{r}{\delta}) = \gamma(n, r)$,

$\gamma(\frac{r}{c}) = \gamma(r)$ and in which case, it has the value $\mu\left[\frac{\gamma(r)}{\gamma(n,r)}\right]$. Also,

since $f(n,r)$ is primitive (mod r), $\therefore$ we have

$$f(\tfrac{r}{\delta}, r) = f(\gamma(\tfrac{r}{\delta}), r) = f(\gamma(n,r), r)$$
$$= f(n,r)$$

$\therefore$ (3) becomes

$$\frac{\gamma(r)\mu\left[\frac{\gamma(r)}{\gamma(n,r)}\right] f(n,r)}{r} \sum_{\substack{\delta/r \\ \gamma(\frac{r}{\delta})=\gamma(n,r)}} \sum_{\substack{c/\delta \\ \gamma(\frac{r}{c})=\gamma(r)}} c\mu(\tfrac{\delta}{c}) \quad \ldots.(4)$$

We note that the conditions δ/r, $\gamma(\frac{r}{\delta})=\gamma(n,r)$ are equivalent to the conditions $\delta/\frac{r}{\gamma(n,r)}$, $(\frac{r}{\delta}, \gamma(r)) = \gamma(n,r)$. Similarly $\gamma(\frac{r}{c})=\gamma(r)$ is equivalent to $c/\frac{r}{\gamma(r)}$ for a divisor c of r.

Therefore, by definition of $\chi(n,r)$, (4) becomes

$$\frac{\gamma(r)\mu\left[\frac{\gamma(r)}{\gamma(n,r)}\right] f(n,r)}{r} \sum_{\substack{\delta\rho=\frac{r}{\gamma(n,r)} \\ (\rho, \frac{\gamma(r)}{\gamma(n,r)})=1}} \chi(\tfrac{r}{\gamma(r)}, \delta)$$

$$= \frac{\gamma(r)\mu\left[\frac{\gamma(r)}{\gamma(n,r)}\right] f(n,r)}{r} \cdot \frac{r\mu\left[\frac{\gamma(r)}{\gamma(n,r)}\right]}{\gamma(r)} \quad \text{(by lemma 7)}$$

$$= \mu^2\left[\frac{\gamma(r)}{\gamma(n,r)}\right] f(n,r)$$

$$= f(n,r)$$

Thus the proof is complete.

Again, as a consequence of the above inversion principle we can characterize the class of primitive functions (mod r) as follows:

A function $f(n,r)$ is primitive if and only if it can be represented in the form

$$f(n,r) = \sum_{\substack{d/\gamma(r) \\ (d,n)=1}} H(d, \tfrac{r}{d})$$

and the function $H(r_1, r_2)$ is uniquely determined by

$$H(r_1, r_2) = \frac{\gamma(r)\mu(r_1)}{r} \sum_{d/\frac{rr_1}{\gamma(r)}} f\left(\frac{r}{d}, r\right) \chi(r_2, d)$$

$$r = r_1 r_2,$$

with r_1, r_2 being positive and r_1 primitive.

We note also that this inversion principle can be reduced to the Möbius inversion formula if we restrict this to the subclass of completely primitive functions (mod r); for if we put $r = r_1$, $r_2 = 1$ and $f(n,r) = j(m)$ where m denotes $\frac{\gamma(r)}{\gamma(n,r)}$, the inversion principle becomes

$$f(n,r) = \sum_{\substack{d/\gamma(r) \\ (d,n)=1}} H(d)$$

$$\rightleftharpoons \quad H(r_1) = \sum_{d/r_1} f\left(\frac{r_1}{d}, r_1\right) \mu\left(\frac{r_1}{d}\right) \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (5)$$

Since $\chi(1,d) = \mu(d)$,

we can rewrite (5) as follows,

$$j(m) = \sum_{d/m} H(d)$$

$$\rightleftharpoons \quad H(r_1) = \sum_{d/r_1} j(d)\mu\left(\frac{r_1}{d}\right)$$

which is the ordinary Möbius inversion formula.

§ Proofs of the generalized Landau and Hölder identities

To illustrate the use of Cohen's inversion principles, now we shall prove two well-known identities of number theory whose proofs are based on these inversion formulas. A few preliminary lemmas are needed before we start proving the identities.

Definition 7:

A function f(n) is said to be completely multiplicative if $f(1) = 1$, $f(mn) = f(m)\,f(n)$ for all m,n. We note that a completely

multiplicative function is the same as a linear function. (see pg.2)

Definition 8:

A divisor d of r is called a canonical divisor of r if $(d, \frac{r}{d}) = 1$.

Let us here introduce a notation that

$$f(n,r) = \sum_{d/(n,r)} y(d)\ x(\tfrac{r}{d})\ \mu(\tfrac{r}{d})$$

and $F(r) = f(0,r)$

with $x(r)$ and $y(r)$ being functions of r.

Lemma 9: If $y(r)$ is completely multiplicative, then

$$F(r) = y\left(\frac{r}{\gamma(r)}\right)\ F(\gamma(r))$$

Proof:

By the complete multiplicativity of $y(r)$ and the definition of $f(n,r)$, we have

$$\begin{aligned} F(r) = f(0,r) &= \sum_{d/r} y(d)\ x(\tfrac{r}{d})\ \mu(\tfrac{r}{d}) \\ &= \sum_{\substack{d\delta = r \\ \delta / \gamma(r)}} y(\tfrac{r}{\delta})\ x(\delta)\mu(\delta) \\ &= y\left(\frac{r}{\gamma(r)}\right) \sum_{\delta/\gamma(r)} y\left(\frac{\gamma(r)}{\delta}\right)\ x(\delta)\mu(\delta) \\ &= y\left(\frac{r}{\gamma(r)}\right)\ F(\gamma(r)) \end{aligned}$$

Lemma 10: If $x(r)$ is multiplicative, $y(r)$ is completely multiplicative, and for all primes p, $y(p) \neq 0$, $y(p) \neq x(p)$, then $F(r) \neq 0$ for all r.

Proof:

Since $F(1) = f(0,1) = 1 \neq 0$, we have to prove the lemma here only for $r > 1$.

Since $x(r)$, $y(r)$ and $\mu(r)$ are multiplicative,

$\therefore$ $F(r)$ is also.

Now let p^{λ} range over the canonical prime power divisors of r $(\lambda > 0)$ and, by the multiplicativity of $F(r)$, we have

$$F(r) = \prod_{p^{\lambda}/r} \left[\sum_{d/p^{\lambda}} y(d)\, x\left(\frac{r}{d}\right) \mu\left(\frac{r}{d}\right) \right]$$

$$= \prod_{p^{\lambda}/r} \left[y(p^{\lambda}) - y(p^{\lambda-1})\, x(p) \right]$$

$$= \prod_{p^{\lambda}/r} \left[y^{\lambda}(p) - y^{\lambda-1}(p)\, x(p) \right]$$

$$= \prod_{p^{\lambda}/r} \left[y^{\lambda-1}(p) \left(y(p) - x(p) \right) \right] \quad \ldots\ldots\ldots (6)$$

$$\neq 0$$

Lemma 11 : Under the conditions of lemma 10, if a and b are positive integers, then

$$F(a,b) = \frac{F(a)\, F(b)\, y((a,b))}{F((a,b))}$$

Proof:

Since $F(r)$ and $y(r)$ are multiplicative, so it suffices to prove the lemma in case $a = p^{t}$, $b = p^{s}$, p prime, and $t \geq s > 0$. Since $y(r)$ is completely multiplicative, it follows from (6) that for $q > 0$.

$$F(p^{q}) = y^{q-1}(p) \left[y(p) - x(p) \right]$$

By lemma 9, and lemma 10, we then have

$$\frac{F(a)\, F(b)\, y((a,b))}{F((a,b))} = \frac{F(p^{t})\, F(p^{s})\, y(p^{s})}{F(p^{s})}$$

$$= F(p^{t})\, y^{s}(p)$$

$$= y\left[\frac{p^{t}}{\gamma(p^{t})}\right] F(\gamma(p^{t}))\, y^{s}(p)$$

$$= y(p^{t-1})\, F(p)\, y^{s}(p)$$

$$= y^{t-1+s}(p)\, F(p)$$

$$= F\ (p^{s+t})$$

$$= F(a,b)$$

By multiplicativity, the lemma follows for arbitrary values of a and b.

Theorem 3: (Generalization of Landau Identity)

If $x(r)$ is multiplicative, $y(r)$ is completely multiplicative, and for ali primes p, $y(p) \neq 0$, $y(p) \neq x(p)$, then

$$\sum_{\substack{d/r \\ (d,n)=1}} \frac{x(d)}{F(d)}\, \mu^2(d) = \frac{y(r)\ \ F(\ (n,r)\ )}{F(r)\ \ y(\ (n,r)\ )} \qquad \ldots\ldots(7)$$

Proof: Since $\mu(r)$, $x(r)$ and $y(r)$ are all multiplicative, $\therefore F(r)$ is also multiplicative.

Denote the right side of (7) by $I(n,r)$. By lemma 9, we have

$$I(n,r) = \frac{y(r)\ \ y\left[\frac{(n,r)}{\gamma(n,r)}\right] F\ (\gamma(n,r)\ )}{y(\frac{r}{\gamma(r)})\ F(\gamma(r))\ y(\ (n,r)\ )}$$

$$= \frac{y\left[\frac{\gamma(r)}{\gamma(n,r)}\right]}{F\left[\frac{\gamma(r)}{\gamma(n,r)}\right]} \qquad \begin{array}{l}(\text{ by the multiplicativity of} \\ \quad y(r) \text{ and } F(r)\ )\end{array}$$

$$= \frac{y(m)}{F(m)} \qquad \left(\ m = \frac{\gamma(r)}{\gamma(n,r)}\ \right)$$

Hence $I(n,r)$ is completely primitive (mod r). By applying (5) we have

$$I(n,r) = \sum_{\substack{d/\gamma(r) \\ (d,n)=1}} H(d) \qquad \ldots\ldots(8)$$

where, assuming r_1 primitive,

$$H(r_1) = \sum_{d/r_1} I\left(\frac{r_1}{d}, r_1\right)\mu\left(\frac{r_1}{d}\right)$$

$$= \sum_{d/r_1} \frac{y(d)}{F(d)}\mu\left(\frac{r_1}{d}\right)$$

By the multiplicativity of $\mu(r)$ and $F(r)$ and by lemma 5 and lemma 4 of last section,

$$H(r_1) = \frac{\mu(r_1)}{F(r_1)} \sum_{d/r_1} y(d)\mu(d)\, F\left(\frac{r_1}{d}\right)$$

$$= \frac{\mu(r_1)}{F(r_1)} \sum_{d/r_1} y(d)\mu(d) \sum_{ce=\frac{r_1}{d}} y(c)\, x(e)\mu(e)$$

Since $y(r)$ is completely multiplicative,

$$\therefore \quad H(r_1) = \frac{\mu(r_1)}{F(r_1)} \sum_{D/r_1} y(D)\, x\left(\frac{r_1}{D}\right)\mu\left(\frac{r_1}{D}\right) \sum_{d/D} \mu(d)$$

with $c\,d = D$

$$\therefore \quad \sum_{d/r} \mu(d) = \begin{cases} 1 & \text{if } r = 1 \\ 0 & \text{if } r > 1 \end{cases}$$

$$\therefore \quad H(r_1) = \frac{\mu^2(r_1)\; x(r_1)}{F(r_1)} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (9)$$

Combining (8) and (9) we thus have

$$I(n,r) = \sum_{\substack{d/\gamma(r) \\ (d,n)=1}} H(d)$$

$$= \sum_{\substack{d/r \\ (d,n)=1}} \left[\frac{x(d)}{F(d)}\right] \mu^2(d)$$

Theorem 4: (Generalization of Hölder's Identity)

If $x(r)$ and $y(r)$ satisfy the conditions of lemma 10, then

$$f(n,r) = \frac{F(r)\; x(e)\,\mu(e)}{F(e)} \qquad \left(e = \frac{r}{(n,r)}\right)$$

where $f(n,r)$ is defined as before,

i.e. $$f(n,r) = \sum_{d/(n,r)} y(d)\ x(\tfrac{r}{d})\mu(\tfrac{r}{d})$$

Proof: Denote $\dfrac{F(r)\ x(e)\mu(e)}{F(e)}$ by $J(n,r)$.

Evidently $J(n,r)$ is even (mod r). Hence by Cohen's first inversion principle,

$$J(n,r) = \sum_{d/(n,r)} h(d, \tfrac{r}{d})$$

where, with $r = r_1\ r_2$,

$$h(r_1,r_2) = \sum_{d/r_1} J(\tfrac{r_1}{d}, r)\,\mu(d)$$

$$= \sum_{d/r_1} \frac{F(r)\ x(\frac{rd}{r_1})\ (\frac{rd}{r_1})}{F(\frac{rd}{r_1})}\mu(d)$$

$$= F(r) \sum_{d/r_1} \frac{x(r_2 d)\ (r_2 d)\mu(d)}{F(r_2\ d)}$$

$$= \frac{F(r)\ x(r_2)\mu(r_2)}{F(r_2)} \sum_{\substack{d/r_1 \\ (d,r_2)=1}} \left[\frac{x(d)}{F(d)}\right]\mu^2(d)$$

(by multiplicativity of $F(r)$, $x(r)$ and $\mu(r)$)

$$= \frac{F(r)\ x(r_2)\mu(r_2)}{F(r_2)} \cdot \frac{y(r_1)\ F((r_1,r_2))}{F(r_1)\ y((r_1,r_2))}$$

(by theorem 3.)

$$= F(r)\ x(r_2)\mu(r_2)\ y(r_1)\ \frac{1}{F(r_1 r_2)}$$ (by lemma 11.)

$$= x(r_2)\mu(r_2)\ y(r_1)$$

$$\therefore\ f(n,r) = \sum_{d/(n,r)} y(d)\ x(\tfrac{r}{d})\mu(\tfrac{r}{d})$$

$$\therefore \quad J(n,r) = \sum_{d/(n,r)} h\left(d, \frac{r}{d}\right)$$

$$= \sum_{d/(n,r)} x\left(\frac{r}{d}\right)\mu\left(\frac{r}{d}\right)\, y(d)$$

$$= f(n,r)$$

This completes the proof.

Thus, in viewing the inversion formulas given above, we can see the importance played by the Möbius μ - function in the theory of inversion, hence in the theory of numbers as a whole.

Bibliography

1. Alder, H.L. A generalization of the Euler ϕ - function. Amer. Math. Monthly, Vol. 65, 1958. pg 690 - 692.
2. Apostel, T.M. A characteristic property of the Möbius function. Amer. Math. Monthly, Vol. 72, 1965, pg 279 - 282.
3. Baker. H.F. On Euler's ϕ - function. Proceedings of London Math. Soc. Vol. 21 (1889 - 1890). pg 30 - 32.
4. Bell. E.T. An arithmetical theory of certain numerical functions. University of Washington Publications in Math. and Phy. Sciences. Vol. 1, No.1, 1915. pg 1 - 44.
5. Bell.E.T. Inversion principle. Duke Math. Jour. 15, 1948. pg 79 - 85.
6. Bell.E.T. Outline of a theory of arithmetical functions in their algebraic aspects. Indian Math. Journal. Vol. 17 (1927 -28). pg 249 - 260.
7. Bell.E.T. Note on an inversion formula. Amer. Math. Monthly, Vol. 43 (1936). pg 464 - 465.
8. Bell.E.T. On a certain inversion in the theory of numbers. Tokoku Math. Jour. Vol. 17 (1920). pg 221 - 231.
9. Bell.E.T. Extension of Dirichlet multiplication and Dedekind inversion . Bull. of the A. M. S. Vol. 28 (1922). pg 111 - 122.
10. Beumer, M.G. The arithmetical function $\tau_k(n)$. Amer. Math.Monthly, Vol. 69, 1962. pg 777 - 781.
11. Cohen, E. A class of arithmetic function. Proceeding of Nat. Acad. of Sciences. 41 (1955). pg 939 - 944.
12. Cohen, E. Arithmetical inversion formula. Canadian Jour. of Math. 12 (1960). pg 399 - 409.

13.Cohen, E. The Brauer - Rademacher identity. Amer. Math. Monthly. Vol. 67, 1960. pg 30 - 33.

14.Cohen, E. Representations of even functions (mod r), I. Arithmetical identities. Duke Math. Jour. Vol. 25 (1958). pg 401 - 421.

15.Dedekind, R. Abrifs einer Theorie der höhern Congruenzen in Bezug auf einen reellen Primzahl - Modulus. Jour. für Math. 54, 1857. pg 1 - 27.

16.Dickson, L.E. History of the theory of Numbers. Vol. 1. Chelsea publishing Co, N.Y. 1952.

17.Erdos,P. Some remarks on Euler's ϕ function.Acta. Arith. 4 (1958) pg 10 - 19.

18.Gupta, H. A generalization of the Möbius function. Scripta Math.Vol. 19 1953. pg 121 - 126.

19.Hardy and Wright An introduction to the theory of numbers. Third ed. Oxford at the Clarendon Press 1954.

20.Makowski, A. On some equations involving functions $\phi(n)$ and $\sigma(n)$. Amer. Math. Monthly, Vol. 67, 1960. pg 668 - 670.

21.Niven, I. and Zuckerman, H.S. An introduction to the theory of Numbers. Second Edition. Wiley and Sons Inc. 1966.

22.Rademacher, H. Lectures on Elementary Number Theory. Blaisdell publishing company 1964.

23.Satyanarayana, U.V. On the inversion property of the Möbius μ - function I. Math. Gazette. 1963. No. 359. pg 38 - 42.

24.Satyanarayana, U.V. On the inversion property of the Möbius μ - function I. Math, Gazette. 1965. No.368. pg 171 - 178.

25.Scholomiti, N.C. A property of the τ- function. Amer. Math. Monthly. Vol. 72, 1965. pg 745 - 747.

26.Swetharanyam, S. A note on the Möbius function. Math. Gazette. 1961, No.351. pg 43 - 47.

27.Vaidyanathaswamy, R. The theory of multiplicative Arithmetic functions. Amer. Math. Soc. Transaction. Vol. 33, 1931. pg 579 - 662.

28.Vaidyanathaswamy, R. On the inversion of multiplicative arithmetical functions. Indian Math. Soc. Journal. 1927. pg 69 - 73.

29.Venkataraman, C.S. A generalization of Euler's ϕ function. Mathematics Student 17 (1949). pg 34 - 36.