Analytic Number Theory

Notes

Basu Dev Karki

IMPORTANT

These notes are based on my personal study of Introduction to Analytic Number Theory by Tom M. Apostol, a foundational text in number theory. While the theorems and concepts covered here follow standard results from Apostol and other classic sources, all proofs, explanations, and commentary are my own and written in my own words. I have expanded on many of the original proofs by adding more context, detailed intermediate steps, and clarifying remarks to make the material more approachable for other learners.

These notes are intended purely for educational and non-commercial purposes. They are not a substitute for the original book. I strongly recommend readers refer to Apostol's text for full rigor.

Any errors or informal explanations here are entirely my responsibility. Constructive feedback and suggestions for improvement are always welcome.

Content

Arithmetical Functions and Dirichlet Multiplication 3

1.1 Introduction 3

1.2 Möbius Function $\mu(n)$ 3

1.3 Euler Toitent Function $\varphi(n)$ 4

1.4 Relation between φ and μ 4

1.5 A product formula for $\varphi(n)$ 5

1.6 Dirichlet Product of Arithmetical Functions 7

1.7 Dirichlet Inverses and Möbius Inversion Formula 8

1.8 The Mangoldt Function $\Lambda(n)$ 10

1.9 Multiplicative functions 11

1.10 Multiplicative Functions and Dirichlet Convolution 12

1.11 The inverse of completely multiplicative function 13

1.12 Liouville's Function 14

1.13 The divisor function $\sigma_\alpha(n)$ 15

1.14 Generalized Convolution 15

1.15 Formal Power Series 17

1.16 The Bell Series of an Arithmetic Function 18

1.17 Bell Series and Dirichlet Product 18

1.18 Derivative of Arithmetical Function 18

1.19 The Selberg Identity 19

Arithmetical Functions and Dirichlet Multiplication

1.1 Introduction

A real or complex valued function defined on the integers is called an arithmetical function or a number-theoretic function. We'll focus on two things first, the Möbius function $\mu(n)$ and Euler Toitent function $\varphi(n)$.

1.2 Möbius Function $\mu(n)$

Definition 1.1. The Möbius function is defined as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^m & \text{if } n \text{ is squarefree and has } m \text{ primes} \\ 0 & \text{if } n \text{ not squarefree} \end{cases}$$

Here is some short table values for $\mu(n)$:

n	1	2	3	4	5	6	7	8	9
$\mu(n)$	1	-1	-1	0	1	-1	-1	0	0

This is a great function and will come in handy later on. For now, let's explore this remarkable formula,

Theorem 1.1. *If $n \geq 1$ then*

$$\sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1 & \textit{if } n = 1 \\ 0 & \textit{if } n > 1 \end{cases}$$

Proof. For $n = 1$ it's obvious so assume $n > 1$. Notice that, from the definition of μ, we have $\mu(n) = 0$ if there exists a prime p such that $p^2 \mid n$.That implies that any non-squarefree divisor does not contribute to the sum. Thus,

$$\begin{aligned}\sum_{d|n} \mu(d) &= \mu(1) + \mu(p_1) + \cdots + \mu(p_m) + \mu(p_1p_2) + \cdots + \mu(p_1p_k) \\ &+ \cdots + \mu(p_1p_2\cdots p_k) \\ &= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k \\ &= (1-1)^k \\ &= 0\end{aligned}$$

□

1.3 Euler Toitent Function $\varphi(n)$

The Euler Toitent function, $\varphi(n)$, counts how many numbers less than n are there, such that they share no common factor.

n	1	2	3	4	5	6	7	8	9
$\varphi(n)$	1	1	2	2	1	2	6	4	6

Theorem 1.2. *If $n \geq 1$ then*

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

Proof. We'll first introduce a new set,

$$A_d = \{k : \gcd(k, n) = d, 1 \leq k \leq n\}$$

Now, one can see that

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

These sets are disjoint and thus,

$$\sum_{d|n} |A_d| = n$$

Now, we form another set,

$$\psi = \{z : \gcd(z, n/d) = 1, 1 \leq z \leq n/d\}$$

Now, we can see there is a bijection between A_d and ψ. For a k, we can write $k = dz$ as $k \leq n$. Since there is a bijection, we can say,

$$|A_d| = |\psi| = \varphi(n/d)$$

Thus,

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

□

1.4 Relation between φ and μ

The function μ and φ are connected by the following relation:

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

Proof. We can write $\varphi(n)$ as a sum,

$$\varphi(n) = \sum_{k=1}^{n} \left\lfloor \frac{1}{\gcd(n, k)} \right\rfloor$$

Now, from Theorem 1.1 we can reinterpret this,

$$\varphi(n) = \sum_{k=1}^{n} \sum_{d|\gcd(n,k)} \mu(d)$$

Here, we are finding each d for a given k and then summing it. However, we can flip it and find each k for a given d and then sum it. Since we already know d must divide n, we just need to find k for which it is a multiple of d. Thus,

$$\varphi(n) = \sum_{d|n} \varphi(n) \sum_{d|k} 1 = \sum_{d|n} \varphi(n) \frac{n}{d}$$

□

1.5 A product formula for $\varphi(n)$

Since we have explored the connection between φ and μ, we now are ready to explore the product formula for $\varphi(n)$.

Theorem 1.3.

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

where p is prime.

Proof. Suppose n has r distinct prime divisors. We can expand the product on the left side of the equation,

$$\prod_{p|n} \left(1 - \frac{1}{p}\right) = 1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \sum \frac{1}{p_i p_j p_k} + \cdots + \sum \frac{(-1)^r}{p_i p_j + \cdots p_r}$$

Each product of prime in the denominator is a divisor of n. And since $\mu(d) = 0$ for non-square free d, we can replace ± 1 in the numerator with $\mu(d)$. Thus,

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

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

□

Now we can establish some identities using this product formula.

Theorem 1.4. *The following properties are true:*

a. $\varphi(mn) = \varphi(m)\varphi(n)(d/\varphi(d))$, *where* $\gcd(m, n) = d$.

b. $a \mid b \implies \varphi(a) \mid \varphi(b)$.

c. If n *has* r *distinct odd primes then* $2^r \mid \varphi(n)$.

Proof. For a. we can $m = d\alpha$ and $n = d\beta$. Then, we can explicitly write it in its prime form,

$$d = r_1^{c_1} \cdots r_x^{c_x}$$

$$\alpha = p_1^{a_1} \cdots p_m^{a_m}$$
$$\beta = q_1^{b_1} \cdots q_n^{b_n}$$

Here, r_i, p_i, q_i all are primes.

$$\varphi(mn) = (d\alpha)(d\beta)\left(1 - \frac{1}{r_1}\right)\cdots\left(1 - \frac{1}{r_x}\right)\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_m}\right)$$
$$\left(1 - \frac{1}{q_1}\right)\cdots\left(1 - \frac{1}{p_n}\right)$$

$$\implies \varphi(mn) = \varphi(m)(d\beta)\left(1 - \frac{1}{q_1}\right)\cdots\left(1 - \frac{1}{p_n}\right)$$

$$\implies \varphi(mn) = \frac{\varphi(m)(d\beta)\left(1 - \frac{1}{q_1}\right)\cdots\left(1 - \frac{1}{p_n}\right)\left(1 - \frac{1}{r_1}\right)\cdots\left(1 - \frac{1}{r_x}\right)}{\left(1 - \frac{1}{r_1}\right)\cdots\left(1 - \frac{1}{r_x}\right)}$$

$$\implies \varphi(mn) = \frac{\varphi(m)\varphi(n)}{\left(1 - \frac{1}{r_1}\right)\cdots\left(1 - \frac{1}{r_x}\right)}$$

$$\implies \varphi(mn) = \frac{\varphi(m)\varphi(n)d}{\varphi(d)}$$

For part b., we can write a and b in their prime form,

$$b = p_1^{a_1} \cdots p_m^{a_m} q_1^{b_1} \cdots q_n^{b_n}$$

$$a = p_1^{r_1} \cdots p_m^{r_m}$$

where $a_i, b_i, r_i \geq 1$. Now,

$$\varphi(b) = p_1^{a_1} \cdots p_m^{a_m}\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_m}\right) q_1^{b_1} \cdots q_n^{b_n}\left(1 - \frac{1}{q_1}\right)\cdots\left(1 - \frac{1}{q_n}\right)$$

$$\varphi(b) = \varphi(a) \cdot N$$

Thus, $\varphi(b)$ is a multiple of $\varphi(a)$.

For $c.$, let

$$n = 2^x \cdot p_1^{a_1} \cdots p_z^{a_r}$$

$$\varphi(n) = p_1^{a_1 - 1} \cdots p_r^{a_r - 1} \cdots (p_1 - 1) \cdots (p_z - 1)$$

Each $p_i - 1$ has a factor of 2, since there are r of them 2^r must divide $\varphi(n)$. □

1.6 Dirichlet Product of Arithmetical Functions

The sum with the form

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

where f and g are arithmetical functions, occur frequently in number theory. We'll explore more about these sums.

Definition 1.2. If f and g are arithmetical functions, then we define the Dirichlet convolution, $h(n)$ by

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

Here, we'll write $(f * g)$ instead of $h(n)$ for better notation and convenience.

Definition 1.3. We define another arithmetic function N such that $N(n) = n$.

Theorem 1.5. *Dirichlet convolution is commutative and associative. That is, for arithmetical functions f, g and h the following is true,*

$$f * g = g * h \qquad \text{(Commutative Law)}$$

$$(f * g) * h = f * (g * h) \qquad \text{(Associative Law)}$$

Proof. From the definition of $f * g$ we know,

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

We can rewrite the sum in a new way,

$$\begin{aligned} f * g &= \sum_{a \cdot b = n} f(a) g(b) \\ &= \sum_{a \cdot b = n} g(b) f(a) \\ &= g * f \end{aligned}$$

Here, a and b vary over the divisors of n. This proves the commutative law.

For the associative law, we define $f * g = A$,

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

$$\begin{aligned}\implies A * h &= \sum_{a\cdot d=n} A(d)h(a) \\ &= \sum_{a\cdot d=n} \left[\sum_{b\cdot c=d} f(b)g(c) \right] h(a) \\ &= \sum_{a\cdot b\cdot c=n} f(b)g(c)h(a)\end{aligned}$$

We can now perform similar operation to $f * (g * h)$ to arrive at the same sum, which will prove associativity of the convolution. □

Definition 1.4. The identity arithmetical function is given by

$$I(n) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1 \end{cases}$$

Theorem 1.6. *For all arithmetical functions f we have $f * I = I * f = I$.*

Proof. From the definition of $f * g$,

$$\begin{aligned} f * I &= \sum_{d|n} f(d) I\left(\frac{n}{d}\right) \\ &= f(n) + \sum_{\substack{d|n \\ d<n}} f(d) I\left(\frac{n}{d}\right) \\ &= f(n) \end{aligned}$$

Since, $\frac{n}{d} > 1$ for $d < n$.

$$\begin{aligned} I * f &= \sum_{d|n} I(d) f\left(\frac{n}{d}\right) \\ &= f(n) + \sum_{\substack{d|n \\ d>1}} I(d) f\left(\frac{n}{d}\right) \\ &= f(n) \end{aligned}$$

Since, $I(1) = 1$. □

1.7 Dirichlet Inverses and Möbius Inversion Formula

Theorem 1.7. *For an arithmetical function f with $f(1) \neq 0$, there exists a unique function f^{-1} known as the Dirichlet inverse, such that*

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

The function is given by,

$$f^{-1}(1) = \frac{1}{f(1)}, \qquad f^{-1}(n) = -\frac{1}{f(1)} \sum_{d|n} f\left(\frac{n}{d}\right) f^{-1}(d) \quad \textit{for } n > 1$$

Proof. Let's first deal with when $n = 1$.

$$(f * f^{-1})(1) = I(1) = 1$$
$$f(1) \cdot f^{-1}(1) = 1$$

Since, $f(1) \neq 0$ so there is only one function which satisfies the equation, namely $f^{-1}(1) = \frac{1}{f(1)}$.

Now suppose we can uniquely determine $f^{-1}(k)$ for $k < n$ then

$$\begin{aligned}(f * f^{-1})(n) &= \sum_{d|n} f\left(\frac{n}{d}\right) f^{-1}(d) \\ &= f^{-1}(n) f(1) + \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d)\end{aligned}$$

Since, $(f * f^{-1})(n) = I(n) = 0$ for $n > 1$. Thus,

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

This function is unique as, $f(n)$ depends on previously known values ($f^{-1}(k)$'s), more precisely on $f(1)$ which is fixed and non-zero. □

Remark. The set of arithmetical functions for which $f(1) \neq 0$ forms an abelian group with binary operation as the convolution. The identity of course being $I(n)$. As a consequence,

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

Definition 1.5. We define the unit function to be an arithmetic function such that $u(n) = 1$ for all n.

From Theorem 1.1 we know that,

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

From our definition of convolution and unit function, Theorem 1.1 can be represented as

$$\mu * u = I$$

Thus, u is the Dirichlet inverse of μ and vice versa; that is

$$u = \mu^{-1} \quad \text{and} \quad \mu = u^{-1}$$

Theorem 1.8. *Möbius Inversion Formula. Let f, g be arithmetic functions. Then,*

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

Proof. Given $f = g * u$, we can now perform left multiplication by μ,

$$f * \mu = (g * u) * \mu = g * (u * \mu) = g * I = g$$

Now, given $g = f * \mu \implies g * u = f * (\mu * u) = f$. □

An example of the Möbius inversion formula has already been presented in Theorem 1.2 and section 1.4, i.e

$$N(n) = \sum_{d|n} \varphi(n) \Longleftrightarrow \varphi(n) = \sum_{d|n} N\left(\frac{n}{d}\right) \mu(d)$$

1.8 The Mangoldt Function $\Lambda(n)$

Definition 1.6. For $n \geq 1$ we define

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

The Mangoldt function helps us understand how the primes are distributed.

Theorem 1.9. *If $n \geq 1$ then we have*

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

Proof. The theorem is obviously true for $n = 1$. Assume, $n > 1$ and write

$$n = \prod_{k=1}^{r} p_k^{a_k}$$

Taking $\log$ on both sides,

$$\log n = \sum_{k=1}^{r} a_k \log p_k$$

Now, consider the sum,

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

We know that $\Lambda(d) = 0$ for $d \neq p^m$ for some prime p and $m \geq 1$ from the definition. Thus, we can just focus on divisors of form p^m.

$$\sum_{d|n} \Lambda(n) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \Lambda(p_k^m) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \log p_k = \sum_{k=1}^{r} a_k \log p_k = \log n$$

□

Theorem 1.10. *If $n \geq 1$ then*

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

Proof. The first equality just uses Theorem 1.8. For the second equality,

$$\begin{aligned} \sum_{d|n} \mu(d) \log \frac{n}{d} &= \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d \\ &= I(n) \log n - \sum_{d|n} \mu(d) \log d \\ &= -\sum_{d|n} \mu(d) \log d \end{aligned}$$

Since, $I(n) \log n = 0$ for $n \geq 1$. □

1.9 Multiplicative functions

We discussed that the collection of functions such that $f(1) \neq 0$ under Dirichlet multiplication forms an abelian group. We'll discuss an important subgroup of that, known as multiplicative functions.

Definition 1.7. An arithmetical function f is called multiplicative if $f(n) \neq 0$ for all n and if

$$f(mn) = f(m)f(n) \quad \text{if } \gcd(m,n) = 1.$$

It is called completely multiplicative if we have

$$f(mn) = f(m)f(n) \quad \text{for all } m, n.$$

Example 1. $f_\alpha(n) = n^\alpha$ where $\alpha \in \mathbb{C}$. This function is completely multiplicative. We denote f_α by N^α and call it a power function.

Example 2. The identity function $I(n)$ is completely multiplicative.

Example 3. The Möbius and Euler Toitent functions are multiplicative but not completely.

Theorem 1.11. *If f is multiplicative, then $f(1) = 1$.*

Proof. We have $f(1 \cdot n) = f(1)f(n)$. Choose a n such that $f(n) \neq 0$ then

$$f(n)(1 - f(n)) = 0 \implies f(1) = 1$$

□

Remark. Since, $\Lambda(1) = 0$, the Mangoldt function is not multiplicative.

Theorem 1.12. *Given f with $f(1) = 1$. Then*

a. f is multiplicative if and only if,

$$f(p_1^{a_1} \cdots p_m^{a_m}) = f(p_1^{a_1}) \cdots f(p_m^{a_m})$$

for all primes p_i and all integers $a_i \geq 1$.

b. If f is multiplicative, then f is completely multiplicative if and only if,

$$f(p^n) = f(p)^n$$

for all primes p and all integers $n \geq 1$.

Proof. For a. and b. we can just use Definition 1.7. If f is multiplicative then by definition,

$$\begin{aligned} f(p_1^{a_1} \cdots p_m^{a_m}) &= f(p_1^{a_1})f(p_2^{a_2} \cdots p_m^{a_m}) \\ &= f(p_1^{a_1})f(p_2^{a_2})f(p_3^{a_3} \cdots p_m^{a_m}) \\ &= \quad \vdots \\ &= f(p_1^{a_1}) \cdots f(p_m^{a_m}) \end{aligned}$$

For b. we again use the definition,

$$\begin{aligned} f(p^n) = f(p^{n-1} \cdot p) &= f(p^{n-1})f(p) \\ &= f(p^{n-2})f(p)^2 \\ &= \vdots \\ &= f(p)^n \end{aligned}$$

□

1.10 Multiplicative Functions and Dirichlet Convolution

Theorem 1.13. *If f and g are multiplicative arithmetic functions, then so is their Dirichlet product $f * g$.*

Proof. Let $h = f * g$ and let m, n be coprime integers then,

$$h(mn) = \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right)$$

Now, let $d = ab$ where $a \mid m$, $b \mid n$ and $\gcd(a, b) = 1$, which implies $\gcd(m/a, n/b) = 1$. Thus,

$$h(mn) = \sum_{\substack{a|m \\ b|n}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right)$$

Now, we fix a and then run b over the divisors of n.

$$h(mn) = \sum_{a|m} f(a)g\left(\frac{m}{a}\right)\sum_{b|n} f(b)g\left(\frac{n}{b}\right)$$

$$h(mn) = h(m)h(n)$$

□

Remark. Dirichlet product of two completely multiplicative functions doesn't necessarily need to be completely multiplicative.

Theorem 1.14. *If g and $f * g$ are both multiplicative, then so is f.*

Proof. We proceed with a contrary statement. Suppose f is not multiplicative. Let m, n be two coprime integers, then there exist coprime integers m, n such that

$$f(mn) \neq f(m)f(n)$$

Now, we choose m, n such that the product is as small as possible. If $mn = 1$ then

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

$$\implies h(1) = f(1)g(1) = f(1) \neq 1 \qquad \text{(Theorem 1.11)}$$

This proves h is not multiplicative.

Suppose now $mn > 1$ then for all integers a, b such that $ab < mn$,

$$f(ab) = f(a)f(b)$$

Now taking a look at the sum,

$$\begin{aligned} h(mn) &= \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) \\ &= \sum_{\substack{a'|m \\ b'|n}} f(a'b')g\left(\frac{mn}{a'b'}\right) \\ &= \sum_{\substack{a'|m \\ b'|n \\ a'b'<mn}} f(a')f(b')g\left(\frac{m}{a'}\right)g\left(\frac{n}{b'}\right) + f(mn) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{\substack{a'|m\\ b'|n}} f(a')f(b')g\left(\frac{m}{a'}\right)g\left(\frac{n}{b'}\right) - f(m)f(n) + f(mn)\\
&= \sum_{a'|m} f(a')g\left(\frac{m}{a'}\right)\sum_{b'|n} f(b')g\left(\frac{n}{b'}\right) - f(m)f(n) + f(mn)\\
&= h(m)h(n) - f(m)f(n) + f(mn)
\end{aligned}
$$

Since, $f(mn) \neq f(m)f(n)$ so $h(mn) \neq h(m)h(n)$. Contradiction. □

Theorem 1.15. *If f is multiplicative, then so is f^{-1}.*

Proof. We know f and $f * f^{-1} = I$ both are multiplicative. Thus from Theorem 1.14, f^{-1} is multiplicative as well. □

Remark. Theorem 1.14 and Theorem 1.15 together show us that the set of arithmetic multiplicative functions is a subgroup of the group of all arithmetic functions with $f(1) \neq 0$.

1.11 The inverse of completely multiplicative function

Theorem 1.16. *Let f be a multiplicative function, then the f is completely multiplicative if and only if,*

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

Proof. Let $g = \mu(n)f(n)$. If f is completely multiplicative, then we have,

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

$$\implies (g * f)(n) = f(n)\sum_{d|n}\mu(d) = f(n)I(n) = I(n)$$

Thus, $g = f^{-1}$.

If $f^{-1}(n) = \mu(n)f(n)$ then,

$$I(n) = (f^{-1} * f)(n) = \sum_{d|n} f^{-1}(d)f\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right)$$

Now, taking $n = p^a$,

$$\mu(1)f(1)f(p^a) + \mu(p)f(p)f(p^{a-1}) = 0$$

$$\implies f(p^a) = f(p)f(p^{a-1})$$

The above implies f is completely multiplicative. □

Example. The inverse of φ. Since $\varphi = \mu * N$, we have $\varphi = N^{-1} * \mu^{-1} =$. But $N^{-1} = \mu N$ from the above theorem. Thus,

$$\varphi = (\mu N) * \mu^{-1} = \mu N * u = \sum_{d|n} \mu(d)d$$

Theorem 1.17. *If f is multiplicative, then*

$$\sum_{d|n} \mu(d)f(d) = \prod_{p|n}(1 - f(p))$$

Proof. Let

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

One can verify that g is multiplicative. So, we just need to play with p^a.

$$g(p^a) = \sum_{d|p^a} \mu(d)f(d) = \mu(1)f(1) + \mu(p)f(p) = 1 - f(p)$$

$$\implies g(n) = \prod_{p|n} g(p^a) = \prod_{p|n}(1 - f(p))$$

□

Remark. We can prove Theorem 1.3 alternatively with the help of this. We know,

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = n\sum_{d|n} \mu(d)\frac{1}{d}$$

Let $\Omega(n) = \frac{1}{n}$ then we know it is multiplicative.

$$\varphi(n) = n\sum_{d|n} \mu(d)\Omega\left(d\right)$$

Then using our theorem, we get

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

1.12 Liouville's Function

This function is an important example of a completely multiplicative function.

Definition 1.8. We define Liouville's function by,

$$\lambda(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^{a_1 + \cdots a_m} & \text{if } n = p_1^{a_1} \cdots p_m^{a_m} \end{cases}$$

The definition shows at once that λ is completely multiplicative.

Theorem 1.18. *For every $n \geq 1$ we have*

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

Proof. Let

$$g(n) = \lambda * u = \sum_{d|n} \lambda(d)$$

Thus, $g(n)$ is multiplicative due to theorem Theorem 1.13. Thus we can draw our attention to $g(p^a)$.

$$\begin{aligned} g(p^a) &= \sum_{d|p^a} \lambda(d) = \lambda(1) + \lambda(p) + \cdots + \lambda(p^a) \\ &= 1 - 1 + 1 - 1 + \cdots = \begin{cases} 1 & \text{if } a \text{ is even} \\ 0 & \text{if } a \text{ is odd} \end{cases} \end{aligned}$$

Thus, if all the exponents of n are even, then $g(n) = 1$ else $g(n) = 0$. This proves the theorem. □

1.13 The divisor function $\sigma_\alpha(n)$

Definition 1.9. Let $a \in \mathbb{C}$ and $n \geq 1$ be an integer then we define the sum of the αth powers of the divisors of n by,

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha$$

The function $\sigma_\alpha(n)$ is multiplicative as $\sigma_\alpha = u * N^\alpha$. One can verify that

$$\sigma_\alpha(n) = \begin{cases} \frac{p^{\alpha(a+1)}-1}{p^\alpha - 1} & \text{if } \alpha \neq 0 \\ a+1 & \text{if } \alpha = 0 \end{cases}$$

Theorem 1.19. *For $n \geq 1$ the inverse of the divisor function is given by,*

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

Proof. Since $\sigma_\alpha = u * N^\alpha$ and N^α is completely multiplicative we can use Theorem 1.16

$$\sigma_\alpha^{-1} = \mu * (\mu N^\alpha)$$

□

1.14 Generalized Convolution

Let $F : (0, +\infty) \longrightarrow \mathbb{C}$ be a function such that $F(x) = 0$ for all $0 < x < 1$.

Definition 1.10. Let α be a arithmetic function. Then, we define Generalized convolution by

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

If $F(x) = 0$ for all nonintegral x then we can see it's an arithmetic function. Thus,

$$(\alpha \circ F)(n) = (\alpha * F)(n)$$

The following theorem sort of serves as a substitution for associative law as $\circ$ is neither associative nor commutative.

Theorem 1.20. *For any arithmetic functions α and β, we have*

$$a \circ (\beta \circ F) = (\alpha * \beta) \circ F$$

Proof. For $x > 0$ we have

$$(\alpha \circ (\beta \circ F)) = \sum_{n \le x} \alpha(n) \sum_{m \le x/n} \beta(m) F\left(\frac{x}{mn}\right)$$

Now we can fix a certain n then go through all m, which is the same as the following

$$(\alpha \circ (\beta \circ F) = \sum_{mn \le x} \alpha(n)\beta(m) F\left(\frac{x}{mn}\right)$$

Now, we can fix an integer $k \le n$ and suppose $k = mn$, we consider all combinations of the pair (m, n). Thus,

$$\begin{aligned}(\alpha \circ (\beta \circ F) &= \sum_{k \le x} \left\{ \sum_{i \mid k} \alpha(i) \beta\left(\frac{k}{i}\right) \right\} F\left(\frac{x}{k}\right) \\ &= \sum_{k \le x} (\alpha * \beta)(k) F\left(\frac{x}{k}\right) \\ &= ((\alpha * \beta) \circ F)\end{aligned}$$

□

Also, note that the identity function for convolution is also an identity for generalized convolution, i.e.

$$(I \circ F)(x) = F(x)$$

Theorem 1.21. *Inversion formula for generalized convolution. Let α be a arithmetical function such that α^{-1} exists*

$$G(x) = \sum_{n \le x} \alpha(n) F\left(\frac{x}{n}\right) \iff F(x) = \sum_{n \le x} \alpha^{-1}(x) G\left(\frac{x}{n}\right)$$

Proof. If $G = \alpha \circ F$ then consider

$$\alpha^{-1} \circ G = \alpha^{-1} \circ (\alpha \circ F) = (\alpha^{-1} * \alpha) \circ F = I \circ F = F$$

If $F = \alpha^{-1} \circ G$ then consider

$$\alpha \circ G = (\alpha * \alpha^{-1}) \circ G = G$$

□

Theorem 1.22. *Inversion formula for generalized convolution. Let α be a arithmetical function such that it's completely multiplicative, then we have*

$$G(x) = \sum_{n \le x} \alpha(n) F\left(\frac{x}{n}\right) \iff F(x) = \sum_{n \le x} \mu(n)\alpha(n) G\left(\frac{x}{n}\right)$$

Proof. Use Theorem 1.16 and Theorem 1.20. □

1.15 Formal Power Series

A Formal Power series is an infinite sum of the form

$$\sum_{n=0}^{\infty} a(n)x^n$$

But here we don't talk about convergence or divergence, instead we draw our interest to the sequence of coefficients.

$$(a(0), a(1), \cdots, a(n), \cdots)$$

Let $A(x)$ and $B(x)$ be two formal power series. We define the following operations on formal power series,

1. $A(x) = B(x) \iff a(n) = b(n) \quad \forall n \geq 0$
2. $A(x) + B(x) = \sum_{n=0}^{\infty}(a(n) + b(n))x^n$
3. $A(x)B(x) = \sum_{n=0}^{\infty} c(n)x^n$ where

$$c(n) = \sum_{k=0}^{n} a(n)b(n-k)$$

The sequence $\{c(n)\}$ is known as *Cauchy product* of sequences $\{a(n)\}$ and $\{b(n)\}$.
For each formal power series $A(x)$, with $a(0) \neq 0$ there is a uniquely determined formula power series $B(x)$ such that $A(x)B(x) = 1$. If we write,

$$A(x) = \sum_{n=0}^{\infty} a(n)x^n \qquad B(x) = \sum_{n=0}^{\infty} b(n)x^n$$

Then the coefficient of $B(x)$ can be determined by solving the following infinite system of equations,

$$a(0)b(0) = 1$$
$$a(0)b(1) + a(1)b(0) = 0$$
$$a(0)b(2) + a(1)b(1) + a(2)b(0) = 0$$
$$\vdots$$

The formal power series,

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

has an inverse, given by

$$B(x) = 1 - ax$$
$$\implies \frac{1}{1-ax} = 1 + \sum_{n=1}^{\infty} a^n x^n$$

One can use induction to prove that, $b(n) = 0$ for all $n \geq 2$ for this series.

1.16 The Bell Series of an Arithmetic Function

Definition 1.11. Let f be an arithmetic function and p be a prime. Then,

$$f_p(x) = \sum_{n=0}^{\infty} f(p^n)x^n$$

is the formal power series of f modulo p and we call it the Bell series.

Theorem 1.23. *Let f and g be multiplicative arithmetic functions. Then, $f = g$ if and only if,*

$$f_p(x) = g_p(x)$$

Proof. If $f = g$ then $f(p^n) = g(p^n)$ thus $f_p(x) = g_p(x)$. If $f_p(x) = g_p(x)$ then by definition $f(p^n) = g(p^n) \implies f = g$. □

1.17 Bell Series and Dirichlet Product

The following theorem relates Bell series with Dirichlet product.

Theorem 1.24. *Let f and g be two arithmetic functions. Let $h = f * g$ be their Dirichlet product. Then for every prime we have,*

$$h_p(x) = f_p(x)g_p(x)$$

Proof. We have,

$$h(p^n) = \sum_{d|p^n} f(d)g\left(\frac{p^n}{d}\right) = \sum_{k=0}^{n} f(p^k)g(p^{n-k})$$

The right hand side is the *Cauchy Product* of $\{f(p^n)\}$ and $\{g(p^n)\}$. This proves the theorem. □

1.18 Derivative of Arithmetical Function

Definition 1.12. For any arithmetical function f, we define its derivative f' to be arithmetic function given by

$$f'(n) = f(n)\log n$$

Example. Since, $I(n)\log n = 0$ for all n we have $I' = 0$. Also, $u' = \log n$.Hence the formula $\sum_{d|n} \Lambda(n) = \log n$ can be rewritten as

$$\Lambda * u = u'$$

The arithmetical derivative shares a lot of common properties with the usual derivative we know.

Theorem 1.25. *If f and g are arithmetic functions then we have*

a. $(f + g)' = f' + g'$

b. $(f * g)' = f' * g + f * g'$

c. $(f^{-1})' = -f * (f * f)^{-1}$, *provided that* $f(1) \neq 0$

Proof. $a.$ is immediate. For $b.$ we can use the property of $\log$.

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

$$(f*g)' = f'*g + f*g'$$

For $c.$ we use the fact that $I' = 0$,

$$\begin{aligned} &(f*f^{-1})' = 0 \\ \implies\ & f'*f^{-1} + f*(f^{-1})' = 0 \\ \implies\ & f*(f^{-1})' = -f'*f^{-1} \\ \implies\ & (f^{-1})' = -f'*(f*f)^{-1} \end{aligned}$$

As $f^{-1}*f^{-1} = (f*f)^{-1}$. □

1.19 The Selberg Identity

Using the concept of derivative we can derive an identity sometimes useful.

Theorem 1.26. *For* $n \geq 1$ *we have*

$$\Lambda(n)\log n + \sum_{d|n}\Lambda(d)\Lambda\left(\frac{n}{d}\right) = \sum_{d|n}\mu(d)\log^2\frac{n}{d}$$

Proof. We know that,

$$\Lambda * u = u'$$

Now,

$$\begin{aligned} &\Lambda*u' + \Lambda'*u = u'' \\ \implies\ & \Lambda*(\Lambda*u) + \Lambda'*u = u'' \end{aligned}$$

Multiplying by u^{-1} on both side

$$\Lambda*\Lambda + \Lambda' = u''*\mu$$

□