Contents

1 The Fundamental Theorem of Arithmetic **3**
1.1 The series of reciprocals of the primes 3

2 Arithmetical Functions and Dirichlet Multiplication **5**
2.1 Mobius function 5
2.2 The Euler totient function 5
2.3 The Dirichlet product 6
2.4 The Mangoldt function Λ 7
2.5 Multiplicative functions 7
2.6 Liouville's function λ 8
2.7 The divisor function σ_α 8
2.8 Generalized convolution 8
2.9 Formal power series 9
2.10 The Selberg theorem 9

3 Averages of Arithmetical Functions **11**
3.1 Asymptotic equality of function 11

Chapter 1

The Fundamental Theorem of Arithmetic

induction, well-ordering principle, divisibility, gcd is commutative,associative, and distributive, relatively prime, primes, fundamental theorem of arithmetic.

1.1 The series of reciprocals of the primes

Theorem 1.1. *The infinite series* $\sum \frac{1}{p_n}$ *diverges.*

Proof. Suppose it does not, let $Q = p_1 \dots p_k$. Then, for all $r \geq 1$,

$$\sum_{n=1}^{r} \frac{1}{1+nQ} \leq \sum_{t=1}^{\infty} \left(\sum_{m=k+1}^{\infty} \frac{1}{p_m} \right)^t$$

■

Euclidean algorithm, division algorithm, gcd algorithm. **Exercises**

1. 1,2,$(a, c) = 1 \implies (a, bc) = (a, b)$,18,28,29,30

Chapter 2

Arithmetical Functions and Dirichlet Multiplication

Definition: A function $f : \mathbb{N} \to \mathbb{C}$ is an arithmetical function.

2.1 Mobius function

The Mobius function μ, is defined as $\mu(1) = 1$ and for $n > 1$ if $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$

$$\mu(n) = \begin{cases} (-1)^k & \alpha_1 = \dots = \alpha_k = 1 \\ 0 & \text{otherwise} \end{cases}$$

Theorem 2.1. *If* $n \geq 1$,

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

2.2 The Euler totient function

The Euler totient function ϕ is defined as

$$\phi(n) = \sum_{k=1}^{n}{}' \, 1 = \left| \left\{ 1 \leq k \leq n \,\middle|\, (k, n) = 1 \right\} \right|$$

Theorem 2.2. *If* $n \geq 1$,

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

Theorem 2.3. *If* $n \geq 1$,

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

2.2.1 The product formular for $\phi(n)$

Theorem 2.4. *For any* $n \geq 1$,

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

Corollary 2.5.

1. $\phi(p^\alpha) = (p-1)p^{\alpha-1}$.
2. $\phi(mn) = \phi(m)\phi(n)\frac{d}{\phi(d)}$ *where* $d = (m, n)$.
3. *If* $a \mid b$, *then* $\phi(a) \mid \phi(b)$.
4. $\phi(n)$ *is even for* $n \geq 3$. *Moreover, if* n *has* r *distinct odd prime factos, then* $2^r \mid \phi(n)$.

2.3 The Dirichlet product

Definition: Let f and g be two arithmetical functions, their **Dirichlet product** is defined as

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

Then, we can write $\phi = \mu * N$ where $N(n) = n$.

Theorem 2.6.

1. $f * g = g * f$.
2. $(f * g) * k = f * (g * k)$.

Definition: The identity function, $I(n) = \left\lfloor \frac{1}{n} \right\rfloor$.

Theorem 2.7. *For any arithmetical function* f, $I * f = f * I = f$.

Theorem 2.8. *If* f *is an arithmetical function with* $f(1) \neq 0$, *there is a unique arithmetical function* f^{-1}, *called the Dirichlet inverse of* f *such that*

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

Moreover, f^{-1} *is given by* $f^{-1}(1) = \frac{1}{f(1)}$ *and for* $n > 1$

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

Remark 1. The set of all arithmetical functions f with $f(1) \neq 0$ is an Abelian group under Dirichlet multiplication.

Proposition 2.9. $(f * g)^{-1} = f^{-1} * g^{-1}$.

Definition: The unit function $u(n) = 1$ for all n. Since $\sum_{d|n} \mu(d) = I(n)$, then $\mu * u = I$ and thus by uniqueness of inverse $\mu^{-1} = u$.

Theorem 2.10 (Mobius inversion formula). *If*

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

then,

$$g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right) \tag{2.1}$$

Proof. Since $f = g * u$, then $g = f * u^{-1} = f * \mu$. ∎

2.4 The Mangoldt function Λ

Definition: For every integer $n \geq 1$, we define

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

Theorem 2.11. *For $n \geq 1$,*

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

and

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

2.5 Multiplicative functions

Definition: An arithmetical function f is **multiplicative** if $f \not\equiv 0$ and

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

whenver $(m, n) = 1$. The function f is said to be **completely multiplicative** if for all m, n

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

Remark 2. Multiplicative functions for a subgroup under $*$.

Proposition 2.12. *If f is multiplicative, then $f(1) = 1$.*

Theorem 2.13. *Given an arithmetical function f with $f(1) = 1$*

1. *f is multiplicative if and only if $f(\prod p_i^{\alpha_i}) = \prod f(p_i^{\alpha_i})$*
2. *If f is multiplicative, then f is completely multiplicative if $f(p^\alpha) = (f(p))^\alpha$.*

Theorem 2.14. *If f and g are both multiplicative, then $f * g$ is multiplicative. If g and $f * g$ are both multiplicative, then f is multiplicative.*

2.5.1 Inverse of completely multiplicative functions

Theorem 2.15. *Let f be a multiplicative function. Then, f is completely multiplicative if and only if*

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

Remark 3. Note that $N = \phi * u$ and $\phi = N * \mu$ therefore, $\phi^{-1} = \mu^{-1} * N^{-1} = u * N^{-1}$. Since N is completely multiplicative, $\phi^{-1} = u * \mu N$. That is,

$$\phi^{-1}(n) = \sum_{d|n} d\mu(d)$$

Theorem 2.16. *If f is multiplicative,*

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

2.6 Liouville's function λ

Definition: The Liouville function λ is defined as $\lambda(1) = 1$ and if $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, then

$$\lambda(n) = (-1)^{\alpha_1 + \dots + \alpha_k}$$

and also $\lambda^{-1}(n) = |\mu(n)|$.

2.7 The divisor function σ_α

Definition: For all $\alpha \in \mathbb{C}$, $\sigma_\alpha(n) = \sum_{d|n} d^\alpha = u \times N^\alpha$

Proposition 2.17. *The divisor function σ_α is multiplicative. Therefore,*

$$\sigma_\alpha\big(p^k\big) = 1 + p^\alpha + \dots + p^{k\alpha} = \begin{cases} \dfrac{p^{(k+1)\alpha} - 1}{p^\alpha - 1} & \alpha \neq 0 \\ k+1 & \alpha = 0 \end{cases}$$

Theorem 2.18. *For $n \geq 1$, we have*

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

2.8 Generalized convolution

Let $F :]0, \infty[\to \mathbb{C}$ such that $F(x) = 0$ for $0 < x < 1$. Let f be an arithmetical function

$$f \circ F(x) = \sum_{n \leq x} f(n) F\Big(\frac{x}{n}\Big)$$

is a function such that $f \circ F(x) = 0$ for $0 < x < 1$ and defined on $]0, \infty[$.

Remark 4. In general, $\circ$ is not commutative nor associative.

Theorem 2.19. *Let f and g be two arithmetical functions*

$$f \circ (g \circ F) = (f * g) \circ F$$

Theorem 2.20 (Inverse formula). *Let f have inverse f^{-1}, then the equation*

$$G(x) = \sum_{n \leq x} f(x) F\Big(\frac{x}{n}\Big)$$

implies

$$F(x) = \sum_{n \leq x} f^{-1}(x) G\Big(\frac{x}{n}\Big)$$

Theorem 2.21 (Generalized Mobius inversion). *Let f be a completely multiplicative function*

$$G(x) = \sum_{n \leq x} f(n) F\Big(\frac{x}{n}\Big) \iff F(x) = \sum_{n \leq x} \mu(n) f(n) G\Big(\frac{x}{n}\Big)$$

2.9 Formal power series

Definiton of formal power series as usual with equality, sum, and multiplication. Therefore, formal power series form a ring with 0 and 1. If the leading coefficient is non-zero, then the formal power series is invertible.

Definition: Let f be an arithmetical function and p be a prime

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

is the **Bell series of f modulo** p.

Theorem 2.22. *If f and g are multiplicative, then $f = g$ if and only if $f_p = g_p$ for all p.*

Example 2.1.

$$\mu_p(x) = 1 - x \qquad I_p(x) = 1 \qquad \lambda_p(x) = \frac{1}{1+x}$$
$$\phi_p(x) = \frac{1-x}{1-px} \qquad u_p(x) = \frac{1}{1-x} \qquad N_p^{\alpha}(x) = \frac{1}{1-p^{\alpha}x}$$

Theorem 2.23. *Let f and g be two arithmetical functions and $h = f * g$, then $h_p = f_p g_p$ for all p.*

As a result,

$$(\sigma_\alpha)_p(x) = N_p^{\alpha}(x)u_p(x) = \frac{1}{1-p^{\alpha}x}\frac{1}{1-x} = \frac{1}{1-(p^{\alpha}+1)x+p^{\alpha}x^2} = \frac{1}{1-\sigma_\alpha(p)+p^{\alpha}x^2}$$

Definition: The derivative arithmetical function f is defined by

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

Theorem 2.24.

1. $(f+g)' = f' + g'$.
2. $(f * g)' = f' * g + f * g'$.
3. $(f^{-1})' = -f' * (f * f)^{-1}$ *provided that* $f(1) \neq 0$.

2.10 The Selberg theorem

Theorem 2.25. *For $n \geq 1$,*

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

Chapter 3

Averages of Arithmetical Functions

Arithmetical functions fluctuate a lot, by taking averages we can determine their behaviour

$$\tilde{f}(n) = \frac{1}{n} \sum_{k=1}^{n} f(k)$$

3.1 Asymptotic equality of function

$f(x) \in O(g(x))$ if there exists $M > 0$ and a such that for all $x \geq a$, $|f(x)| \leq M|g(x)|$. Usually, g is taken to be positive.

Definition: If $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$, then f is asymptotic to g as $x \to \infty$ and we write $f(x) \sim g(x)$ as $x \to \infty$.