Contents

Part I

Elementary Number Theory

Chapter 1

Preliminary

Theory of numbers is about the study of natural numbers, denoted by $\mathbb{N} = \{0, 1, 2, \ldots\}$. Formally, the set of natural numbers is defined as non-empty set with $0 \in \mathbb{N}$ with a successor function $S : \mathbb{N} \to \mathbb{N}$ such that

$$\forall x, S(x) \neq 0 \tag{1.1}$$
$$\forall x, y, S(x) = S(y) \implies x = y \tag{1.2}$$
$$\forall x, x + 0 = 0 + x = x \tag{1.3}$$
$$\forall x, x \cdot 0 = 0 \cdot x = 0 \tag{1.4}$$
$$\forall x, y, S(x + y) = x + S(y) \tag{1.5}$$
$$\forall x, y, S(x \cdot y) = x \cdot y + x \tag{1.6}$$
$$\forall \phi, \Big(\phi(0) \wedge (\forall x, \phi(x) \implies \phi(S(x)))\Big) \implies \forall x, \phi(x) \tag{1.7}$$

The last axiom is called the principle of induction. It says that if for some predicate ϕ, $\phi(0)$ and ϕ is such that if ϕ is true for x then it is also true for $S(x)$, then ϕ is true for all natural numbers.

Algebraically, the natural numbers form a commutative monoid under addition and positive natural numbers form a commutative monoid under multiplication.

Definition (Well-ordering principle): Any non-empty subset of natural numbers has a smallest element.

Theorem 1.1. *The well-ordering principle and principle of induction are equaivalent.*

Part II

Analytical Number Theory

Chapter 2

The Fundamental Theorem of Arithmetic

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

2.1 The series of reciprocals of the primes

Theorem 2.1. *The infinite series* $\sum \frac{1}{p_n}$ *diverges.*

Proof. Suppose the sum converges instead and let k be such that

$$\sum_{n=k+1}^{\infty} \frac{1}{p_n} \leq \frac{1}{2}$$

Let $Q = p_1 \ldots p_k$, then for all $r \geq 1$,

$$\begin{aligned}\sum_{n=1}^{r} \frac{1}{1+nQ} &\leq \sum_{t=1}^{\infty} \left(\sum_{m=k+1}^{\infty} \frac{1}{p_m} \right)^t \\ &\leq \sum_{t=1}^{\infty} \left(\frac{1}{2} \right)^t \\ &= 1\end{aligned}$$

By allowing $r \to \infty$, we get

$$\sum_{n=1}^{\infty} \frac{1}{1+nQ} \leq 1$$

However, this is a constradiction as the sum diverges as

$$\sum_{n=1}^{\infty} \frac{1}{1+nQ} \leq \sum_{n=1}^{\infty} \frac{1}{Q+nQ} \leq \frac{1}{Q} \sum_{n=2}^{\infty} \frac{1}{n}$$

Therefore, $\sum \frac{1}{p_n}$ must diverge. ∎

Euclidean algorithm, division algorithm, gcd algorithm.

Exercises

1. If $(a, b) = 1$ and if $c \mid a$ and $d \mid b$, then $(c, d) = 1$.

   Solution. Let $e = (c, d)$, since $e \mid c$, then $e \mid a$ and similarly, $e \mid b$. Therefore, $e \mid (a, b)$ which means $e = 1$. ▷

2. If $(a, b) = (a, c) = 1$, then $(a, bc) = 1$.

   Solution. Let $d = (a, bc)$ and $e = (b, d)$. Then, $e \mid d$ and hence $e \mid a$, as a result $e \mid (a, b)$ which means $e = 1$. Note that, $d \mid bc$ but $(b, d) = 1$ thus, $d \mid c$. Since $d \mid a$, then $d \mid (a, c)$ and hence $d = 1$. ▷

3. If $(a, c) = 1$, then $(a, bc) = (a, b)$.

   Solution. Let $d = (a, bc)$ and $e = (c, d)$. Then, $e \mid d$ and hence $e \mid a$, as a result $e \mid (a, c)$ which means $e = 1$. Note that, $d \mid bc$ but $(c, d) = 1$ thus, $d \mid b$. Since $d \mid a$, then $d \mid (a, b)$. Moreover, $(a, b) \mid d$ since $(a, b) \mid a$ and $(a, b) \mid bc$. Therefore, $d = (a, b)$. ▷

4. If $m \neq n$ compute the $\gcd\big(a^{2^m} + 1, a^{2^n} + 1\big)$ in terms of a.

   Solution. WLOG assume $n < m$ and note that

   $$a^{2^m} - 1 = a^{2^{m-n} \cdot 2^n} - 1 = \big(a^{2^n} - 1\big)\big(a^{2^n} + 1\big)\big(a^{2 \cdot 2^n} + 1\big) \dots \Big(a^{2^{m-n-1} \cdot 2^n} + 1\Big)$$

   and hence

   $$a^{2^n} + 1 \mid a^{2^m} - 1$$

   Therfore,

   $$\big(a^{2^n} + 1, a^{2^m} + 1\big) = \big(2, a^{2^n} + 1\big) = \begin{cases} 1 & a \text{ is even} \\ 2 & a \text{ is odd} \end{cases}$$ ▷

5. If $a > 1$, then $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

   Solution. If $m = n$, then the result hold obviously. Suppose $n < m$ and note that

   $$a^m - 1 = (a^{m-n})(a^n - 1) + (a^{m-n} - 1)$$

   and therefore, $(a^m - 1, a^n - 1) = (a^{m-n} - 1, a^n)$. By applying the Euclidean algorithm we arrive at the conclusion. ▷

6. Given $n > 0$, let S be a set whose elements are positive integers $\leq 2n$ such that if a and b are in S and $a \neq b$, then $a \nmid b$. What is the maximum number of integers that S can contain?

   Solution. Note that S can not have more than n elements. To see this, consider the sets $\big\{m2^k \,\big|\, k \geq 0,\ m2^k \leq 2n\big\}$ for $m = 1, 3, \dots, 2n - 1$. There are $n - 1$ such sets and they partition the set $\{1, 2, \dots, 2n\}$. No two elements of S can come from the same set, and as a result $|S| \leq n - 1$ by pigeonhole principle. However, note that $S = \{n + 1, n + 2, \dots, 2n\}$ satisfies the conditions and has exactly $n - 1$ elements. Therefore, the maximum of $n - 1$ elements is attainable for all $n > 0$. ▷

7. If $n > 1$ prove that the sum $\sum_{k=1}^{n} \frac{1}{k}$ is not an integer. Also show that for any signing of the sum $\sum_{k=1}^{n}(-1)^{a_k}\frac{1}{k}$ is not an integer.

   Solution. Let p be the largest prime less than or equal to n. Let $r, s \in \mathbb{Z}$ be such that $s \neq 0$ and $(r, s) = 1$.

$$\frac{r}{s} = \sum_{\substack{k=1 \\ k\neq p}}^{n} (-1)^{a_k} \frac{1}{k}$$

   We claims that $p \nmid s$. For the sake of contradiction suppose there is an integer q such that $s = pq$. Then,

$$\begin{aligned} r &= s\left(\sum_{\substack{k=1 \\ k\neq p}}^{n} (-1)^{a_k} \frac{1}{k}\right) \\ &= \sum_{\substack{k=1 \\ k\neq p}}^{n} (-1)^{a_k} \frac{pq}{k} \end{aligned}$$

   Since $(p, k) = 1$ for all $k \leq n$ and $k \neq p$, then it must be the case that the sum

$$\sum_{\substack{k=1 \\ k\neq p}}^{n} (-1)^{a_k} \frac{q}{k}$$

   is an integer. Therefore, we have shown that there is integer t such that $r = pt$, which contradicts our assumption that $(r, s) = 1$. Thus, p does not divide s. To conclude, consider the sum

$$\frac{r}{s} + \frac{(-1)^{a_p}}{p} = \frac{pr + (-1)^{a_p} s}{ps}$$

   which can not be integer as $p \nmid s$. ▷

Chapter 3

Arithmetical Functions and Dirichlet Multiplication

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

3.1 Mobius function

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

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

Theorem 3.1. *If* $n \geq 1$,

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

Proof. Suppose $n > 1$ and $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, then

$$\sum_{d|n} \mu(d) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} = (1-1)^k = 0$$

If $n = 1$, then $\sum_{d|n} \mu(d) = \mu(1) = 1$. ∎

3.2 The Euler totient function

The Euler totient function ϕ is defined as

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

Theorem 3.2. *If* $n \geq 1$,

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

Proof. Define the equivalence relation $i \sim j$ whenever $(n,i) = (n,j)$ on the numbers $\leq n$. The divisors of n can be taken as class representatives. We claim that the size of the class d is equal to $\phi\left(\frac{n}{d}\right)$. Note that, if $(n,i) = d$, then $(n/d, i/d) = 1$ and vice versa. That is, there is a bijection between elements of the class d and numbers that are coprime to n/d less than n/d. Therefore,

$$n = \sum_{d|n} |\text{class}_d| = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d)$$ ∎

Theorem 3.3. *If* $n \geq 1$*,*

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

Proof. The statement is clearly true for $n = 1$. Suppose $n > 1$ and $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Let A_i denote the set of all numbers k less than or equal to n such that $p_i \mid (n,k)$. Then,

$$\begin{aligned}
\phi(n) &= \left| \left(\bigcup_{i=1}^{k} A_i \right)^c \right| \\
&= n - \left| \bigcup_{i=1}^{k} A_i \right| \\
&= n - \sum_{j=1}^{n} (-1)^{j-1} \sum_{i_1 < i_2 < \dots < i_j} \left| A_{i_1} \cap \dots \cap A_{i_j} \right| \\
&= n + \sum_{j=1}^{n} \sum_{i_1 < i_2 < \dots < i_j} (-1)^j \frac{n}{p_{i_1} \dots p_{i_j}} \\
&= n + \sum_{j=1}^{n} \sum_{i_1 < i_2 < \dots < i_j} \mu\left(p_{i_1} \dots p_{i_j}\right) \frac{n}{p_{i_1} \dots p_{i_j}} \\
&= \sum_{d|n} \mu(d) \frac{n}{d}
\end{aligned}$$ ∎

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

Theorem 3.4. *For any* $n \geq 1$*,*

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

Proof. If $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ let $m = p_1 \dots p_k$.

$$\begin{aligned}
\phi(n) &= \sum_{d|n} \mu(d) \frac{n}{d} \\
&= n \sum_{d|m} \frac{\mu(d)}{d}
\end{aligned}$$

$$
\begin{aligned}
&= n\left(\sum_{\substack{d|m\\p_1|d}} \frac{\mu(d)}{d} + \sum_{\substack{d|m\\p_1\nmid d}} \frac{\mu(d)}{d}\right)\\
&= n\left(\sum_{\substack{d|m\\p_1\nmid d}} \frac{\mu(p_1 d)}{p_1 d} + \sum_{\substack{d|m\\p_1\nmid d}} \frac{\mu(d)}{d}\right)\\
&= n\left(\left(1-\frac{1}{p_1}\right)\sum_{\substack{d|m\\p_1\nmid d}} \frac{\mu(d)}{d}\right)\\
&= n\prod_{p|n}\left(1-\frac{1}{p}\right)
\end{aligned}
$$

■

Corollary 3.5.

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 factors, then $2^r \mid \phi(n)$.*

Proof.

1. $\phi(p^\alpha) = p^\alpha\left(\frac{p-1}{p}\right) = (p-1)p^{\alpha-1}$.
2. $$
\begin{aligned}
\phi(mn) &= mn\prod_{p|mn}\left(1-\frac{1}{p}\right)\\
&= mn\prod_{\substack{p|n\\p\nmid m}}\left(1-\frac{1}{p}\right)\prod_{\substack{p|m\\p\nmid n}}\left(1-\frac{1}{p}\right)\prod_{p|n,m}\left(1-\frac{1}{p}\right)\\
&= mn\frac{\prod_{p|n}\left(1-\frac{1}{p}\right)}{\prod_{p|n,m}\left(1-\frac{1}{p}\right)}\frac{\prod_{p|m}\left(1-\frac{1}{p}\right)}{\prod_{p|n,m}\left(1-\frac{1}{p}\right)}\prod_{p|n,m}\left(1-\frac{1}{p}\right)\\
&= \phi(m)\phi(n)\frac{1}{\prod_{p|n,m}\left(1-\frac{1}{p}\right)}\\
&= \phi(m)\phi(n)\frac{d}{\phi(d)}
\end{aligned}
$$
3. Note that if $p \mid a$, then $p \mid b$.

4. If n has an odd prime factor, then $\phi(n)$ is even. If n is power of 2 greater than 4, then $\phi(n)$ is also even. If n has r distinct odd prime factors, each contribute at least one factor of 2 in $\phi(n)$ and thus $2^r \mid \phi(n)$. ■

3.3 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 3.6.

1. $f * g = g * f$.

2. $(f * g) * h = f * (g * h)$.

Proof.

1.

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

2.

$$\begin{aligned}
((f * g) * h)(n) &= \sum_{d|n} (f * g)(d)h\left(\frac{n}{d}\right) \\
&= \sum_{d|n} \sum_{k|d} f(k)g\left(\frac{d}{k}\right)h\left(\frac{n}{d}\right) \\
&= \sum_{k|n} \sum_{k|d,d|n} f(k)g\left(\frac{d}{k}\right)h\left(\frac{n}{d}\right) \\
&= \sum_{k|n} \sum_{d|n/k} f(k)g\left(\frac{kd}{k}\right)h\left(\frac{n}{kd}\right) \\
&= \sum_{k|n} \sum_{d|n/k} f(k)g(d)h\left(\frac{n}{kd}\right) \\
&= \sum_{k|n} \sum_{d|n/k} f(k)(g * h)\left(\frac{n}{k}\right) \\
&= (f * (g * h))(n)
\end{aligned}$$

■

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

Theorem 3.7. *For any arithmetical function f, $I * f = f * I = f$.*

Proof. Trivial. ■

Theorem 3.8. *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 $n > 1$

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

Proof. It can be easily shown that the given function is a Dirichlet inverse of f. That is,

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

Suppose g is also a Dirichlet inverse of f. Then,

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

Therefore, $g = f^{-1}$ and f^{-1} is unique. ∎

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

Proposition 3.9. *Suppose f and g are invertible arithmetical functions, then $(f * g)^{-1} = f^{-1} * g^{-1}$.*

Proof. We can readily deduct this from the fact that invertible functions form an Abelian group under Dirichlet multiplication. ∎

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

Theorem 3.10 (Mobius inversion formula). *If*

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

then,

$$g(n) = \sum_{d|n} f(d) \mu\left(\frac{n}{d}\right) \tag{3.1}$$

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

3.4 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 3.11. *For $n \geq 1$,*

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

and

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

Proof. For the first identity we have

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

Hence, $\log = \Lambda * u$. Therfore, $\Lambda = \log * u^{-1} = \log * \mu$. ■

3.5 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 from a subgroup under $*$. The ordinary multiplication and division of two (completely) multiplicative functions are (completely) multiplicative.

Proposition 3.12. *If f is multiplicative, then $f(1) = 1$.*

Proof. Since f is multiplicative, $f(1) = f(1)f(1)$ thus, $f(1) = 0, 1$. If $f(1) = 0$, then $f \equiv 0$ which contradicts our assumption hence $f(1)$ must be 1. ■

Theorem 3.13. *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 and only if $f(p^\alpha) = (f(p))^\alpha$.*

Proof.

1. If f is multiplicative, then the formula is obviously true. Suppose the formula holds and the integers m, n are relatively prime. Let $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ and $n = q_1^{\beta_1} \dots q_r^{\beta_r}$ with no p equal to a q.

$$f(mn) = f\left(\prod p_i^{\alpha_i} \prod q_i^{\beta_i}\right) = \prod_{i,j} f(p_i^{\alpha_i}) f\left(q_j^{\beta_j}\right) = \prod_i f(p_i^{\alpha_i}) \prod_j f\left(q_j^{\beta_j}\right) = f(m)f(n)$$

Therefore, f is multiplicative.

2. If f is completely multiplicative, then the formula holds trivially. Suppose the formula holds and m, n are integers with prime decomposition $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ and $n = p_1^{\gamma_1} \dots p_k^{\gamma_k} q_1^{\beta_1} \dots q_r^{\beta_r}$ with no p equal to a q.

$$\begin{aligned}
f(mn) &= f\Big(\prod p_i^{\alpha_i+\gamma_i} \prod q_i^{\beta_i}\Big) \\
&= \prod_{i,j} f\big(p_i^{\alpha_i+\gamma_i}\big) f\Big(q_j^{\beta_j}\Big) \\
&= \prod_i (f(p_i))^{\alpha_i+\gamma_i} \prod_j f\Big(q_j^{\beta_j}\Big) \\
&= \prod_i (f(p_i))^{\alpha_i} \prod_i (f(p_i))^{\gamma_i} \prod_j f\Big(q_j^{\beta_j}\Big) \\
&= \prod_i f(p_i^{\alpha_i}) \prod_i f(p_i^{\gamma_i}) \prod_j f\Big(q_j^{\beta_j}\Big) \\
&= f(m)f(n)
\end{aligned}$$

■

Theorem 3.14. *If f and g are both multiplicative, then $f * g$ is multiplicative. If g and $f * g$ are both multiplicative, then f is multiplicative.*

Proof. Suppose f and g are two multiplicative functions and m, n are two relatively prime integers. Then,

$$\begin{aligned}
f * g(mn) &= \sum_{d|mn} f(d) g\Big(\frac{mn}{d}\Big) \\
&= \sum_{\substack{d_m|m \\ d_n|n}} f(d_m d_n) g\Big(\frac{m}{d_m}\frac{n}{d_n}\Big) \\
&= \sum_{d_m|m} \sum_{d_n|n} f(d_m) f(d_n) g\Big(\frac{m}{d_m}\Big) g\Big(\frac{n}{d_n}\Big) \\
&= f * g(m) f * g(n)
\end{aligned}$$

Let g be a multiplicative function. We show that g^{-1} is multiplicative as well. Since $g(1) = 1$, then $g^{-1}(1) = 1$. Note that if p is a prime for $k \geq 1$ we have,

$$g^{-1}\big(p^k\big) = -\sum_{i=0}^{k-1} g\big(p^{k-i}\big) g^{-1}\big(p^i\big)$$

Let h be the multiplicative function that agrees with g^{-1} on prime powers. Consider the Dirichlet multiplication $g * h$ for $p_1^{\alpha_1} \dots p_k^{\alpha_k}$ with $\alpha_i \geq 1$.

$$\begin{aligned}
g * h(p_1^{\alpha_1} \dots p_k^{\alpha_k}) &= \sum_{0 \leq i_j \leq \alpha_j} h\big(p_1^{i_1} \dots p_k^{i_k}\big) g\big(p_1^{\alpha_1 - i_1} \dots p_k^{\alpha_k - i_k}\big) \\
&= \sum_{0 \leq i_j \leq \alpha_j} h\big(p_1^{i_1}\big) \dots h\big(p_k^{i_k}\big) g\big(p_1^{\alpha_1 - i_1}\big) \dots g\big(p_k^{\alpha_k - i_k}\big) \\
&= \prod_j \sum_{0 \leq i_j \leq \alpha_j} h\Big(p_j^{i_j}\Big) g\Big(p_j^{\alpha_j - i_j}\Big)
\end{aligned}$$

$$
\begin{aligned}
&= \prod_j \sum_{0 \le i_j \le \alpha_j} g^{-1}\left(p_j^{i_j}\right) g\left(p_j^{\alpha_j - i_j}\right) \\
&= \prod_j \left(\sum_{0 \le i_j < \alpha_j} g^{-1}\left(p_j^{i_j}\right) g\left(p_j^{\alpha_j - i_j}\right) + g^{-1}\left(p_j^{\alpha_j}\right) \right) \\
&= \prod_j \left(\sum_{0 \le i_j < \alpha_j} -g^{-1}\left(p_j^{\alpha_j}\right) + g^{-1}\left(p_j^{\alpha_j}\right) \right) \\
&= 0
\end{aligned}
$$

Also, $g * h(1) = g(1)h(1) = 1$. That is, $g * h = I$ and since Dirichlet inverse is unique it must be that $g^{-1} = h$. ∎

3.5.1 Inverse of completely multiplicative functions

Theorem 3.15. *Let f be a multiplicative function. Then, f is completely multiplicative if and only if*

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

Proof. Suppose f is completely multiplicative and $g(n) = \mu(n) f(n)$

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

Thus, $f^{-1} = g$. Suppose f is a multiplicative function such that $f^{-1} = \mu f$. Let p be prime and $\alpha \ge 1$ be such that $f(p^\alpha) = (f(p))^\alpha$. Then, note

$$f\left(p^{\alpha+1}\right) = -\sum_{i=0}^{\alpha} f\left(p^i\right) f^{-1}\left(p^{\alpha+1-i}\right) = -f(p^\alpha) f^{-1}(p) = (f(p))^\alpha f(p) = (f(p))^{\alpha+1}$$ ∎

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 3.16. *If f is multiplicative,*

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

Proof. Let $g(n) = \sum_{d|n} \mu(d) f(d)$. Note that $g = \mu f * u$ and thus it is multiplicative. Then, to determine g we need to evaluate $g(p^\alpha)$ for prime p and $\alpha \ge 1$.

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

As a result,

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

3.6 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

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

Theorem 3.17. *For $n \geq 1$,*

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

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

Proof. Note that $g = \lambda * u$ is multiplicative since λ is completely multiplicative. Hence, for a prime p and $\alpha \geq 1$ we have

$$g(p^\alpha) = \sum_{i=0}^{\alpha} \lambda(p^i) = \sum_{i=0}^{\alpha} (-1)^i = \frac{1 - (-1)^{\alpha+1}}{1 - (-1)} = \frac{1 + (-1)^\alpha}{2} = \begin{cases} 1 & \alpha \text{ is even} \\ 0 & \alpha \text{ is odd} \end{cases}$$

Therefore,

$$g(n) = \prod_{p^\alpha || n} g(p^\alpha) = \begin{cases} 1 & n \text{ is a perfect square} \\ 0 & \text{otherwise} \end{cases}$$

Since λ is completely multiplicative, $\lambda^{-1} = \mu\lambda$. If there is a prime p such that $p^2 \mid n$, then $\mu(n) = 0$ and $\mu(n)\lambda(n) = |\mu(n)|$. If $n = p_1 \dots p_k$, then $\lambda(n) = \mu(n)$ and thus $\lambda(n)\mu(n) = (\mu(n))^2 = |\mu(n)|$. ∎

3.7 The divisor function σ_α

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

Proposition 3.18. *The divisor function σ_α is multiplicative and*

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

Proof. Trivial. ∎

Theorem 3.19. *For $n \geq 1$, we have*

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

Proof. Since N^α is completely multiplicative we have

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

3.8 Generalized convolution

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

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

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 3.20. *Let f and g be two arithmetical functions*

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

Theorem 3.21 (Inverse formula). *Let f have inverse f^{-1}, then the equation*

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

implies

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

Proof.

$$\begin{aligned}
f \circ (g \circ F)(x) &= \sum_{n \leq x} f(n) g \circ F\left(\frac{x}{n}\right) \\
&= \sum_{n \leq x} f(n) \sum_{k \leq x/n} g(k) F\left(\frac{x}{nk}\right) \\
&= \sum_{n \leq x} \sum_{nk \leq x} f(n) g(k) F\left(\frac{x}{nk}\right) \\
&= \sum_{nk \leq x} f(n) g(k) F\left(\frac{x}{nk}\right) \\
&= \sum_{m \leq x} \sum_{d \mid m} f(d) g\left(\frac{m}{d}\right) F\left(\frac{x}{m}\right) \\
&= \sum_{m \leq x} f * g(m) F\left(\frac{x}{m}\right) \\
&= (f * g) \circ F(x)
\end{aligned}$$

■

Theorem 3.22 (Generalized Mobius inversion). *Let f be completely multiplicative*

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

Proof. We have

$$\mu f \circ G = f^{-1} \circ G = f^{-1} \circ (f \circ F) = (f^{-1} * f) \circ F = F$$

■

3.9 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 3.23. *If f and g are multiplicative, then $f = g$ if and only if $f_p = g_p$ for all p.*

Proof. Trivial. ■

Example 3.1.

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

Theorem 3.24. *Let f and g be two arithmetical functions and $h = f * g$, then $h_p = f_p g_p$ for all p.*

Proof. We have,

$$\begin{aligned} h_p(x) &= \sum_{n=0}^{\infty} h(p^n)x^n \\ &= \sum_{n=0}^{\infty}\sum_{i=0}^{n} f\left(p^i\right)g\left(p^{n-i}\right)x^n \\ &= \sum_{i=0}^{\infty}\sum_{n=i}^{\infty} f\left(p^i\right)g\left(p^{n-i}\right)x^n \\ &= \sum_{i=0}^{\infty} f\left(p^i\right)x^i \sum_{n=i}^{\infty} g\left(p^{n-i}\right)x^{n-i} \\ &= \sum_{i=0}^{\infty} f\left(p^i\right)x^i \sum_{n=0}^{\infty} g(p^n)x^n \\ &= f_p(x)g_p(x) \end{aligned}$$

■

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 3.25.

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

Proof.

1. $(f+g)' = (f+g)\log = f\log + g\log$.
2. $$\begin{aligned}(f * g)'(n) &= f * g(n)\log n \\ &= \sum_{d|n} f(d) g\Big(\frac{n}{d}\Big) \log n \\ &= \sum_{d|n} f(d) g\Big(\frac{n}{d}\Big)\Big(\log d + \log\frac{n}{d}\Big) \\ &= \sum_{d|n} f(d)\log d g\Big(\frac{n}{d}\Big) + \sum_{d|n} f(d) g\Big(\frac{n}{d}\Big)\log\frac{n}{d} \\ &= f' * g(n) + f * g'(n)\end{aligned}$$
3. Note that, $(f * f^{-1})' = I' = I\log \equiv 0$. From the previous part we have $$(f * f^{-1})' = f' * f^{-1} + f * (f^{-1})' = 0 \implies (f^{-1})' = -f^{-1} * f' * f^{-1} = -f' * (f * f)^{-1}$$ ■

3.10 The Selberg theorem

Theorem 3.26. *For* $n \geq 1$,

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

Proof. Recall that $\Lambda = \mu * \log$ and $\Lambda' = \Lambda\log$ by definition.

$$\begin{aligned}\Lambda\log + \Lambda * \Lambda &= \Lambda' + (\mu * \log) * \Lambda \\ &= (\mu * \log)' + (\mu * u') * \Lambda \\ &= \mu' * \log + \mu * \log' + [(\mu * u)' - \mu' * u] * \Lambda \\ &= \mu\log * \log + \mu * \log^2 - \mu\log * u * \Lambda \\ &= \mu\log * \log + \mu * \log^2 - \mu\log * \log \\ &= \mu * \log^2\end{aligned}$$

■

Exercises

1. Prove that
$$\frac{n}{\phi(n)} = \sum_{d|n} \frac{\mu^2(d)}{\phi(d)}$$

Solution. Note that, both the left hand side N/ϕ and the right hand side $\mu^2/\phi * u$ are multiplicative therefore, it suffices to show that they are equal on prime powers.

$$\begin{aligned} LHS &= \frac{p^\alpha}{\phi(p^\alpha)} = \frac{p^\alpha}{p^{\alpha-1}(p-1)} = \frac{p}{p-1} \\ RHS &= \sum_{d|p^\alpha} \frac{\mu^2(d)}{\phi(d)} = \frac{1}{\phi(1)} + \frac{1}{\phi(p)} = \frac{p}{p-1} \\ \implies & LHS = RHS \end{aligned}$$ ▷

2. Let $\nu(n)$ be the number of distinct prime factors of n with $\nu(1) = 1$. Let $f = \mu * \nu$ and prove that $f(n)$ is either 0 or 1.

Solution. Let m, k be an integer with $m, k \geq 1$ and p a prime such that $(m, p) = 1$. Then,

$$\begin{aligned} \mu * \nu\big(p^k m\big) &= \sum_{d|p^k m} \mu(d)\nu\left(\frac{p^k m}{d}\right) \\ &= \sum_{d|m}\sum_{l|p^k} \mu(ld)\nu\left(\frac{p^k m}{ld}\right) \\ &= \sum_{d|m} \mu(d)\nu\left(\frac{p^k m}{d}\right) + \mu(pd)\nu\left(\frac{p^{k-1}m}{d}\right) \\ &= \sum_{d|m} \mu(d)\Big(1+\nu\Big(\frac{m}{d}\Big)\Big) - \mu(d)\Big((1-I(k)) + \nu\Big(\frac{m}{d}\Big)\Big) \\ &= I(k)\sum_{d|m}\mu(d) \\ &= I(k)I(m) \end{aligned}$$

Therefore, the value of the function is either 0 or 1. Moreover, it is only 1 for prime numbers. ▷

3. Prove that
$$\sum_{d^k|n} \mu(d) = \begin{cases} 0 & \text{if } m^k \mid n \text{ for some } m > 1 \\ 1 & \text{otherwise} \end{cases}$$

Solution. Let $n = m^k r$ with $m \geq 1$ and r is k_{th} power free. That is, there is no integer whose k_{th} power divides r. Therefore,

$$\sum_{d^k|n} \mu(d) = \sum_{d^k|m^k} \mu(d) = \sum_{d|m} \mu(d) = I(m)$$ ▷

4. Prove that
$$\sum_{d|n} \mu(d) \log^m(d) = 0$$
if $m \geq 1$ and n has more than m distinct prime factors.

Solution. Let $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ has k distinct prime factors.
$$\begin{aligned}
\sum_{d|n} \mu(d) \log^m(d) &= \sum_{d|p_1 \dots p_k} \mu(d) \log^m(d) \\
&= \sum_{d|p_1 \dots p_{k-1}} \mu(d) \log^m(d) + \mu(dp_k) \log^m(dp_k) \\
&= \sum_{d|p_1 \dots p_{k-1}} \mu(d) \log^m(d) - \mu(d)(\log d + \log p_k)^m \\
&= -\sum_{d|p_1 \dots p_{k-1}} \sum_{j=0}^{m-1} \binom{m}{j} \mu(d) \log^j(d) \log^{m-j}(p_k) \\
&= -\sum_{j=0}^{m-1} \binom{m}{j} \log^{m-j}(p_k) \sum_{d|p_1 \dots p_{k-1}} \mu(d) \log^j(d)
\end{aligned}$$
Assuming that the induction base is true and $k > m$, then we are done by induction. The base case is when $m = 1$. Let $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ and $k \geq 2$,
$$\begin{aligned}
\sum_{d|n} \mu(d) \log d &= -\log(p_k) \sum_{d|p_1 \dots p_{k-1}} \mu(d) \\
&= -\log p_k I(p_1 \dots p_{k-1}) = 0
\end{aligned}$$
▷

5. Let $f(x)$ be defined for all rational x in $0 \leq x \leq 1$ and let
$$F(n) = \sum_{k=1}^{n} f\left(\frac{k}{n}\right) \qquad F^*(n) = \sum_{\substack{k=1 \\ (k,n)=1}} f\left(\frac{k}{n}\right)$$
(a) Show that $F^* = F * \mu$.
(b) Show that
$$\mu(n) = \sum_{\substack{k=1 \\ (k,n)=1}} e^{2\pi ik/n}$$

Solution. (a) We have,
$$\begin{aligned}
F^*(n) &= \sum_{k=1}^{n} I((n,k)) f\left(\frac{k}{n}\right) \\
&= \sum_{k=1}^{n} \sum_{d|(n,k)} \mu(d) f\left(\frac{k}{n}\right) \\
&= \sum_{d|n} \sum_{k=1}^{n/d} \mu(d) f\left(\frac{dk}{n}\right)
\end{aligned}$$

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

(b) Let $f(x) = e^{2\pi i x}$, then

$$F(n) = \sum_{k=1}^{n} e^{2\pi i k/n} = I(n)$$

and thus

$$\mu * F = \mu = F^* = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} e^{2\pi i k/n}$$ ▷

6. Prove that,

$$\sigma_1(n) = \sum_{d|n} \phi(d) \sigma_0\left(\frac{n}{d}\right)$$

And try to generalize it for σ_α

Solution. For integer $\alpha \geq 1$

$$\begin{aligned}
\sigma_\alpha &= N^\alpha * u = (N^{\alpha-1} N) * u \\
&= (N^{\alpha-1} N) * (N^{\alpha-1} \mu) * (N^{\alpha-1} \mu)^{-1} * u \\
&= (N^{\alpha-1} \phi) * N^{\alpha-1} * u \\
&= (N^{\alpha-1} \phi) * \sigma_{\alpha-1}
\end{aligned}$$ ▷

7.

Chapter 4

Averages of Arithmetical Functions

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

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

4.1 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 $x \to \infty$.

4.2 Euler's summation formula

Theorem 4.1. *If f has a continuous derivative f' on the interval $[y, x]$, where $0 < y < x$, then*

$$\begin{aligned}\sum_{y<n\leq x} f(n) = \int_y^x f(t)\,\mathrm{d}t + \int_y^x (t - \lfloor t \rfloor) f'(t)\,\mathrm{d}t \\ + f(x)(\lfloor x \rfloor - x) - f(y)(\lfloor y \rfloor - y)\end{aligned}$$

4.3 Some elementary asymptotic formula

Definition: The Euler-Mascheroni constant is defined as

$$\gamma = \lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k} - \log n\right)$$

Definition: The Riemann zeta function is defined as

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

where $s \in \mathbb{C}$ is a complex variable.

Theorem 4.2. *If $x \geq 1$ we have*

$$\sum_{n\leq x} \frac{1}{n} = \log n + \gamma + O\left(\frac{1}{x}\right) \tag{4.1}$$

$$\sum_{n\leq x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O\big(x^{-s}\big) \qquad s > 0 \wedge s \neq 1 \tag{4.2}$$

$$\sum_{n>x} \frac{1}{n^s} = O\big(x^{1-s}\big) \qquad s > 1 \tag{4.3}$$

$$\sum_{n\leq x} n^\alpha = \frac{x^{\alpha+1}}{\alpha+1} + O(x^\alpha) \qquad \alpha \geq 0 \tag{4.4}$$

4.4 The average order of $d(n)$

Theorem 4.3. *For all $x \geq 1$,*

$$\sum_{n\leq x} d(n) = x \log x + (2\gamma - 1)x + O\big(\sqrt{x}\big)$$

The error term can be improved to $O\big(x^{12/37+\epsilon}\big)$ for all $\epsilon > 0$.

4.5 The average order of $\sigma_\alpha(n)$

Theorem 4.4. *For all $x \geq 1$*

$$\sum_{n\leq x} \sigma_1(x) = \frac{1}{2}\zeta(2)x^2 + O(x \log x)$$

$$\sum_{n\leq x} \sigma_{-1}(x) = \zeta(2)x + O(\log x)$$

If $\alpha > 0$ and $\alpha \neq 1$, then

$$\sum_{n\leq x} \sigma_\alpha(x) = \frac{1}{\alpha+1}\zeta(\alpha+1)x^{\alpha+1} + O\big(x^\beta\big)$$

$$\sum_{n\leq x} \sigma_{-\alpha}(x) = \zeta(\alpha+1)x + O\big(x^\delta\big)$$

where $\beta = \max\{1, \alpha\}$ and $\delta = \max\{0, 1-\alpha\}$.

4.6 The average order $\phi(n)$

Theorem 4.5. *For $x > 1$ we have*

$$\sum_{n\leq x} \phi(n) = \frac{3}{\pi^2}x^2 + O(x \log x)$$

4.7 An application

Definition: Two lattice point P and Q are mutually visible if the line segment connecting them contains no other lattice point.

Theorem 4.6. *Two lattice point (a, b) and (c, d) are mutually visible if and only if $(a-c, b-d) = 1$.*

Consider the square $C(r) = \{(x, y) \mid |x|, |y| \le r\}$, let $N(r) = \#C(r)$ and let $N'(r)$ be the number of visible points from the origin in $C(r)$.

Theorem 4.7. *The set of lattice points visible from the origin has density $\frac{6}{\pi^2}$. That is,*

$$\lim_{n\to\infty} \frac{N'(r)}{N(r)} = \frac{6}{\pi^2}$$

4.8 The average order of $\mu(n)$ and $\Lambda(n)$

Theorem 4.8. *We have*

$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\le x} \mu(n) = 0$$
$$\lim_{x\to\infty} \frac{1}{x} \sum_{n\le x} \Lambda(n) = 1$$

Both are equivalent to prime number theorem.

4.9 The partial sums of Dirichlet product

Theorem 4.9. *If $h = f * g$, let*

$$H(x) = \sum_{n\le x} h(n) \qquad F(x) = \sum_{n\le x} f(n) \qquad G(x) = \sum_{n\le x} g(n)$$

then we have

$$H(x) = \sum_{n\le x} f(n) G\left(\frac{x}{n}\right) = \sum_{n\le x} g(n) F\left(\frac{x}{n}\right)$$

Theorem 4.10. *If $F(x) = \sum_{n\le x} f(n)$ we have*

$$\sum_{n\le x} \sum_{d\mid n} f(d) = \sum_{n\le x} f(x) \left\lfloor \frac{x}{n} \right\rfloor = \sum_{n\le x} F\left(\frac{x}{n}\right)$$

4.10 Applications to $\mu(n)$ and $\Lambda(n)$

Theorem 4.11. *For $x \geq 1$ we have*

$$\sum_{n \leq x} \mu(x) \left(\frac{x}{n} \right) = 1$$
$$\sum_{n \leq x} \Lambda(x) \left(\frac{x}{n} \right) = \log(\lfloor x \rfloor !)$$

Theorem 4.12. *For all $x \geq 1$ we have*

$$\left| \sum_{n \leq x} \frac{\mu(n)}{n} \right| \leq 1$$

with equality hodling if $x < 2$.

Theorem 4.13 (Legendre's Identity). *For all $x \geq 1$*

$$\lfloor x \rfloor ! = \prod_{p \leq x} p^{\alpha(p)}$$

where $\alpha(p) = \sum_{m=1}^{\infty} \left\lfloor \frac{x}{p^m} \right\rfloor$.

Theorem 4.14. *If $x \geq 2$*

$$\log(\lfloor x \rfloor !) = x \log x - x + O(\log x)$$

and hence

$$\sum_{n \leq x} \Lambda(n) \lfloor (x) n \rfloor = x \log x - x + O(\log x)$$

Theorem 4.15. *For $x \geq 2$*

$$\sum_{p \leq x} \lfloor (x) p \rfloor \log p = x \log x + O(x)$$

4.11 Another Identity for the partial sums of a Dirichlet product

Theorem 4.16. *If $h = f * g$, let*

$$H(x) = \sum_{n \leq x} h(n) \qquad F(x) = \sum_{n \leq x} f(n) \qquad G(x) = \sum_{n \leq x} g(n)$$

then we have

$$H(x) = \sum_{n \leq x} \sum_{d | n} f(d) g\left(\frac{n}{d} \right) = \sum_{qd \leq x} f(d) g(q)$$

Theorem 4.17. *If a, b are positive real numbers such that $ab = x$, then*

$$\sum_{qd \leq x} f(d) g(q) = \sum_{n \leq a} f(n) G\left(\frac{x}{n} \right) + \sum_{n \leq b} g(x) G\left(\frac{x}{n} \right) - F(a) G(b)$$

Chapter 5

Elementary Theorems on the Distribution of Prime Numbers

5.1 Chebyshev's functions $\psi(x), \theta(x)$

Definition: For $x > 0$,

$$\psi(x) = \sum_{n \leq x} \Lambda(n) = \sum_{m=1}^{\infty} \sum_{p^m \leq x} \Lambda(p^m) = \sum_{m=1}^{\infty} \sum_{p^m \leq x} \log(p)$$

Moreover, since there are no primes less than 2, if $x^{1/m} < 2$, then the inner sum would be zero. That is,

$$\psi(x) = \sum_{m \leq \lg x} \sum_{p \leq x^{1/m}} \log p$$

Definition: For $x > 0$,

$$\theta(x) = \sum_{p \leq x} \log p$$

Therefore,

$$\psi(x) = \sum_{m \leq \lg x} \theta(\sqrt[m]{x})$$

Theorem 5.1. *For $x > 0$,*

$$0 \leq \frac{\psi(x) - \theta(x)}{x} \leq \frac{(\log x)^2}{2\sqrt{x}\log 2}$$

Proof.

From this theorem, we are able to conclude that if $\lim \frac{\psi(x)}{x}$ exists, then $\lim \frac{\theta(x)}{x}$ exists and they are equal.

5.2 Relations connecting $\theta(x)$ and $\pi(x)$

Theorem 5.2 (Abel's identity). *Let $a(n)$ be arithmetical and let $A(n) = \sum_{n \leq x} a(n)$, with $A(x) = 0$ for $x < 1$. Assume f has a continuous derivative on interval $[y, x]$. Then, we have*

$$\sum_{y \leq n \leq x} a(n)f(x) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)\,\mathrm{d}t$$

The Euler's summation formula can be easily deduced from Abel's.

Theorem 5.3. *For* $x \geq 2$

$$\theta(x) = \pi(x)\log x - \int_2^x \frac{\pi(t)}{t}\,\mathrm{d}t$$

and

$$\pi(x) = \frac{\theta(x)}{\log x} + \int_2^x \frac{\theta(t)}{t\log^2 t}\,\mathrm{d}t$$

5.3 Equivalent forms of Prime Number Theorem

Theorem 5.4. *The following relations are equivalent.*

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1 \tag{5.1}$$

$$\lim_{x\to\infty} \frac{\theta(x)}{x} = 1 \tag{5.2}$$

$$\lim_{x\to\infty} \frac{\psi(x)}{x} = 1 \tag{5.3}$$

Theorem 5.5. *Let* p_n *be the* n_{th} *prime, the following relations are equivalent.*

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

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

$$\lim_{n\to\infty} \frac{p_n}{n\log n} = 1$$

5.4 Inequalities for $\pi(x)$ and p_n

Theorem 5.6. *For every integer* $n \geq 2$

$$\frac{1}{6}\frac{n}{\log n} \leq \pi(n) \leq 6\frac{n}{\log n}$$

and for $n \geq 1$,

$$\frac{1}{6} n\log n < p_n < 12\left(n\log n + n\log\left(\frac{12}{e}\right)\right)$$

Chapter 6

Congrueneces

6.1 Definitions and Properties

Theorem 6.1. *For $c > 0$, $a \equiv b \mod m$ if and only if $ac \equiv bc \mod mc$.*

Theorem 6.2 (Cancellation law). *If $ac \equiv bc \mod m$ and $(c, m) = d$, thesection*

$$a \equiv b \mod m/d$$

6.2 Residue classes

Definition: A set of m representatives, one from each residue classes $\hat{1}, \hat{2}, \ldots, \hat{m}$ is called a complete residue system modulo m.

Theorem 6.3. *If $(k, m) = 1$ and $\{a_1, \ldots, a_m\}$ is a complete residue system, then the set $\{ka_1, \ldots, ka_m\}$ is a complete residue system.*

Theorem 6.4. *If $(a, m) = 1$, then the linear congruence $ax \equiv b \mod m$ has exactly one solution.*

Theorem 6.5. *If $(a, m) = d$ then $ax \equiv b \mod m$ has a solution if and only if $d \mid b$. Moreover, there exactly d solutions, if any exists.*

Theorem 6.6. *If $(a, b) = d$, then there exists $x, y \in \mathbb{Z}$ such that*

$$ax + by = d$$

6.3 Reduced residue classes

Definition: A reduced residue system modulo m is a set of incongruent number modulo m that are relatively prime to m.

Theorem 6.7. *If $(k, m) = 1$ and $\left\{a_1, \ldots, a_{\phi(m)}\right\}$ is a reduced residue system, then the set $\left\{ka_1, \ldots, ka_{\phi(m)}\right\}$ is a reduced residue system.*

Theorem 6.8 (Euler-Fermat theorem). *Assume $(a, m) = 1$, then we have*

$$a^{\phi(m)} \equiv 1 \mod m$$

Theorem 6.9 (Fermat's little theorem). *For all $a \in \mathbb{Z}$ and primes p, $a^p \equiv a \mod p$*

Corollary 6.10. *If $(a, m) = 1$, then*

$$ax \equiv b \mod m \implies x \equiv ba^{\phi(m)-1} \mod m$$

6.4 Polynomial congruence modulo primes

Theorem 6.11 (Lagrange's theorem). *Let p be a prime and $f(x) = c_0 + \cdots + c_n x^n$ be a polynomial with integer coefficient of degree n such that $c_n \not\equiv 0 \mod p$. Then, $f(n) \equiv 0 \mod p$ has at most n solutions.*

6.4.1 Applications of Lagrange's theorem

Theorem 6.12. *If $f(x) = c_0 + c_1 x + \cdots + c_n x^n$ is a polynomial of degreee n with integer coefficients and if the congruence $f(x) \equiv 0 \mod p$ has more than n solutions modulo p, when p is a prime, then every coefficient of f is divisible by p.*

Corollary 6.13. *For all primes p, all the coefficients of the following polynomial are divisible by p.*

$$f(x) = (x-1)(x-2)\dots(x-(p-1)) - x^{p-1} + 1$$

Corollary 6.14 (Wilson's theorem). *$(n-1)! \equiv -1 \mod n$ if and only if n is a prime.*

Corollary 6.15 (Wolstenholmes' theorem). *For any prime $p \geq 5$*

$$\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \mod p$$

6.5 Simultaneous linear congruence

Theorem 6.16 (Chinese remainder theorem). *Assume $m_1, \dots, m_k$ are positive integers that are pairwise relatively prime, $(m_i, m_j) = 1$ for $i \neq j$. Let $b_1, \dots, b_k$ be arbitrary integers. Then, the system of congrueneces*

$$\begin{cases} x & \equiv b_1 \mod m_1 \\ x & \equiv b_2 \mod m_2 \\ & \vdots \\ x & \equiv b_k \mod m_k \end{cases}$$

has exactly one solution modulo $M = m_1 \dots m_k = \prod m_i$.