NUMBER THEORY

[MTH1C05]

STUDY MATERIAL

I SEMESTER
CORE COURSE

M.Sc. Mathematics

(2019 Admission onwards)

UNIVERSITY OF CALICUT
SCHOOL OF DISTANCE EDUCATION
CALICUT UNIVERSITY- P.O
MALAPPURAM- 673635, KERALA

190555

SCHOOL OF DISTANCE EDUCATION

UNIVERSITY OF CALICUT

STUDY MATERIAL FIRST SEMESTER

M.Sc. Mathematics (2019 ADMISSION ONWARDS) CORE

COURSE:

MTH1C05-NUMBER THEORY

Prepared by:

Dr. Anil Kumar V
Professor
Department of Mathematics
University of Calicut

Scrutinized By:

Dr. Preethi Kuttipulackal
Associate Professor & Head
Department of Mathematics
University of Calicut

Number Theory

School of Distance Education

University of Calicut

Anil Kumar V

Contents

Module 1

Arithmetical Functions and its Averages

This module consists of two sections. *Let $\mathbb{N}$ be the set of natural numbers. Then $f : \mathbb{N} \to \mathbb{C}$ is called a sequence. In number theory such functions are called arithmetical functions. In the first section introduces several arithmetical functions. The Dirichlet product of two arithmetical functions are included. Moreover we will prove that the set of all arithmetical functions which do not vanish at 1 form an abelian group under Dirichlet multiplication. Furthermore, Möbius inversion is included. This section also includes generalized convolutions and gives relation between associative property of Dirichlet multiplication and convolution. Generalized inversion formula is also included. The second section is devoted to averages of Arithmetical functions. The well known Euler's summation formula is derived. Several asymptotic formulas are also derived.*

1.1 Arithmetical functions

Definition 1.1.1. *A complex valued function defined on the set of natural numbers is called an* arithmetical function *or a* number theoretic function. *That is, a function $f : \mathbb{N} \to \mathbb{C}$ is called an arithmetical function .*

1.1.1 The Möbius function $\mu(n)$

Definition 1.1.2. *The Mobius function μ is defined as:*

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

From the definition of μ it clear that $\mu(n) = 0$ if and only if n has a square

factor > 1.Obviously,

$$\mu(1) = 1, \mu(2) = -1, \mu(3) = -1, \mu(4) = 0, \mu(5) = -1, \mu(6) = 1, \mu(8) = 0$$

and so on.

Theorem 1.1.1. *If $n \geq 1$ we have*

$$\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

Proof. We consider two cases.
Case 1: Suppose $n = 1$.
In this case

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

Case 2: Suppose $n > 1$.
Then by fundamental theorem of arithmetic, n can be expressed in the following form:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

where p_i's are distinct primes and $\alpha_1, \alpha_2, \ldots, \alpha_k$ are integers greater than or equal to 1. Now consider

$$\sum_{d|n} \mu(d) = \sum_{d|p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}} \mu(d).$$

Note that $\mu(d) = 0$ if and only if d has a square factor. Therefore $\mu(d) \neq 0$ if and only if

$$d = 1; \underbrace{p_1, p_2, \ldots, p_k}_{\binom{k}{1}}; \underbrace{p_1p_2, \ldots, p_{k-1}p_k}_{\binom{k}{2}}; \underbrace{p_1p_2p_3, \ldots p_{k-2}p_{k-1}p_k}_{\binom{k}{3}}; \cdots, \underbrace{p_1p_2 \cdots p_k}_{\binom{k}{k}}.$$

Hence

$$\begin{aligned}
\sum_{d|n} \mu(d) &= \mu(1) + [\mu(p_1) + \mu(p_2) + \cdots + \mu(p_k)] + [\mu(p_1p_2) + \cdots + \mu(p_{k-1}p_k)] + \\
&\qquad [\mu(p_1p_2p_3) + \cdots + \mu(p_{k-2}p_{k-1}p_k)] + [\mu(p_1p_2 \cdots p_k)] \\
&= 1 + \underbrace{[(-1) + (-1) + \cdots + (-1)]}_{\binom{k}{1}} + \underbrace{[(-1)^2 + (-1)^2 + \cdots + (-1)^2]}_{\binom{k}{2}} + \\
&\qquad \underbrace{[(-1)^3 + (-1)^3 + \cdots + (-1)^3]}_{\binom{k}{3}} + \cdots + \underbrace{(-1)^k}_{\binom{k}{k}} \\
&= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \binom{k}{3}(-1)^3 + \cdots + \binom{k}{k}(-1)^k \\
&= (1-1)^n = 0.
\end{aligned}$$

This completes the proof. □

1.1.2 Euler totient function $\varphi(n)$

Definition 1.1.3. *If $n \geq 1$ the Euler totient function $\varphi(n)$ is defined as*

$$\varphi(n) := \#\{a \in \mathbb{N} : a \leq n, (a,n) = 1\}.$$

Thus

$$\varphi(n) = \sum_{k=1}^{n}{}' 1,$$

where dash denotes the sum is taken over those k which are relatively prime to n. That is

$$\varphi(n) = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} 1 = \sum_{k=1}^{n} \left[\frac{1}{(n,k)}\right].$$

Theorem 1.1.2. *If $n \geq 1$ we have*

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

Proof. Let

$$S = \{1, 2, 3, \ldots, n\}$$

We partition the set S into mutually disjoint subsets as follows:
For each divisor d of n, let

$$A(d) := \{k : (k,n) = d, 1 \leq k \leq n\}.$$

Claim 1: If d_1 and d_2 are distinct divisors of n, then $A(d_1) \cap A(d_2) = \emptyset$.

$$\begin{aligned} x \in A(d_1) \cap A(d_2) &\Rightarrow x \in A(d_1) \text{ and } x \in A(d_2) \\ &\Rightarrow (x,n) = d_1 \text{ and } (x,n) = d_2 \\ &\Rightarrow d_1 = d_2, \text{contradiction.} \end{aligned}$$

Claim 2: $\{1, 2, \ldots, n\} = \cup_{d|n} A(d)$.
Obviously

$$\cup_{d|n} A(d) \subseteq S. \tag{1.1}$$

Now

$$\begin{aligned} x \in S &\Rightarrow (x,n) = d \text{ for some } d, 1 \leq d \leq n \\ &\Rightarrow x \in A(d) \\ &\Rightarrow x \in \cup_{d|n} A(d) \text{ for some } d|n. \end{aligned}$$

Thus

$$S \subseteq \cup_{d|n} A(d). \tag{1.2}$$

From equations (1.1) and (1.2) it follows that

$$S = \cup_{d|n} A(d).$$

Therefore

$$\#(S) = \sum_{d|n} \#(A(d)).$$

This implies that

$$n = \sum_{d|n} \#(A(d)). \tag{1.3}$$

Claim : $\#(A(d)) = \varphi(d)$.
Now

$$\begin{aligned} k \in A(d) &\Leftrightarrow (k,n) = d \\ &\Leftrightarrow (k/d, n/d) = 1, 0 < k/d \leq n/d \\ &\Leftrightarrow (q, n/d) = 1, 0 < q \leq n/d \\ &\Leftrightarrow q \in \underbrace{\{k : (k, n/d) = 1, 0 < k \leq n/d\}}_{B} \\ &\Leftrightarrow q \in B \end{aligned}$$

This implies that there is a one to one correspondence between the elements of $A(d)$ and B. Hence

$$\#A(d) = \#(B) = \varphi(n/d).$$

Hence equation (1.3) becomes:

$$n = \sum_{d|n} \varphi(n/d) \tag{1.4}$$

Observe that if d is a divisor of n, then n/d is also a divisor of n. The divisors d and n/d are called conjugate divisors of n. Hence

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

Hence equation (1.4) can be written as

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

This completes the proof of the theorem. □

1.1.3 A relation connecting φ and μ.

Theorem 1.1.3. *If $n \geq 1$ we have*

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

Proof. By the definition of φ, we have

$$\begin{aligned}\varphi(n) &= \sum_{k=1}^{n}\left[\frac{1}{(n,k)}\right] \\ &= \sum_{k=1}^{n}\sum_{d|(n,k)}\mu(d) \text{ (by theorem 1.1.1)} \\ &= \sum_{k=1}^{n}\sum_{d|n\&d|k}\mu(d) \\ &= \sum_{d|n}\left[\sum_{k=1}^{n}\sum_{d|k}\mu(d)\right] \end{aligned} \tag{1.5}$$

Note that for a fixed d, $\sum_{k=1}^{n}\sum_{d|k}\mu(d)$ denotes the summation over all those k in the set $\{1,2,\ldots,n\}$ which are multiples of d.
Question: How many multiples of d are there in the set $\{1,2,3,\ldots,n\}$?
Suppose $1 \le k \le n$ and $k = qd$. Now

$$\begin{aligned} 1 \le k \le n &\Leftrightarrow 0 < k \le n \\ &\Leftrightarrow 0 < \frac{k}{d} \le \frac{n}{d} \\ &\Leftrightarrow 1 \le \frac{k}{d} \le \frac{n}{d} \\ &\Leftrightarrow 1 \le q \le \frac{n}{d} \end{aligned}$$

This implies that in the set $\{1,2,\ldots,n\}$ there are n/d numbers which are multiples of d. These multiples of d are

$$\{d, 2d, \ldots, (n/d)d\}$$

Hence equation (1.5) can be written as:

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

This completes the proof of the theorem. □

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

Theorem 1.1.4. *For $n \ge 1$ we have*

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

where p is a prime divisor of n.

Proof. Here we consider two cases.
Case 1: Suppose $n = 1$.
Note that when $n = 1$, $\varphi(n) = \varphi(1) = 1$. Also when $n = 1$,

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

Since there are no prime divide 1, we define

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

Hence the theorem is true for $n = 1$.
Case 2: Suppose $n > 1$.
In this case n can be expressed in the form:

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

where p_i's are distinct primes and $\alpha_1, \alpha_2, \ldots, \alpha_r$ are integers ≥ 1. Consider

$$\begin{aligned}
\prod_{p|n}\left(1-\frac{1}{p}\right) &= \prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)\\
&= \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)\\
&= 1-\left(\frac{1}{p_1}+\frac{1}{p_2}+\cdots+\frac{1}{p_r}\right)+\left(\frac{1}{p_1p_2}+\frac{1}{p_1p_3}+\cdots+\frac{1}{p_{r-1}p_r}\right)-\\
&\quad\left(\frac{1}{p_1p_2p_3}+\cdots+\frac{1}{p_{r-2}p_{r-1}p_r}\right)+\cdots+\frac{(-1)^r}{p_1p_2\cdots p_r}\\
&= 1+\sum_{i=1}^{r}\frac{(-1)}{p_i}+\sum_{\substack{i,j=1\\ i\neq j}}^{r}\frac{(-1)^2}{p_ip_j}+\sum_{\substack{i,j,k=1\\ i\neq j\neq k}}^{r}\frac{(-1)^3}{p_ip_jp_k}+\cdots+\frac{(-1)^r}{p_1p_2\cdots p_r}\\
&= 1+\sum_{i=1}^{r}\frac{\mu(p_i)}{p_i}+\sum_{\substack{i,j=1\\ i\neq j}}^{r}\frac{\mu(p_ip_j)}{p_ip_j}+\sum_{\substack{i,j,k=1\\ i\neq j\neq k}}^{r}\frac{\mu(p_ip_jp_k)}{p_ip_jp_k}+\cdots+\frac{\mu(p_1p_2\cdots p_r)}{p_1p_2\cdots p_r}\\
&= \sum_{d|n}\frac{\mu(d)}{d}.
\end{aligned}$$

Hence

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

$$= \varphi(n) \text{ (by theorem 1.1.3)}$$

This completes the proof of the theorem. □

Theorem 1.1.5. *Euler's totient has the following properties:*

(a) $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, *for prime* p *and* $\alpha \geq 1$.

(b) $\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$, *where* $d = (m, n)$

(c) $\varphi(mn) = \varphi(m)\varphi(n)$ *if* $(m, n) = 1$.

(d) $a|b$ *implies* $\varphi(a)|\varphi(b)$.

(e) $\varphi(n)$ *is even for* $n \geq 3$. *Moreover, if* n *has distinct* r *odd prime factors then* $2^r|\varphi(n)$.

Proof.
(a) We have

$$\varphi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right) \text{ (theorem 1.1.24)} \tag{1.6}$$

Putting $n = p^\alpha$ in equation (1.6), we obtain:

$$\varphi(p^\alpha)n\prod_{p|p^\alpha}\left(1 - \frac{1}{p}\right) \tag{1.7}$$

$$= p^\alpha\left(1 - \frac{1}{p}\right) \text{ (since } p \text{ is the only prime divisor of } p^\alpha) \tag{1.8}$$

$$= p^\alpha - p^{\alpha-1} \tag{1.9}$$

(b)We have

$$\varphi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right) \text{ (theorem 1.1.24)}$$

Therefore

$$\frac{\varphi(n)}{n} = \prod_{p|n}\left(1 - \frac{1}{p}\right). \tag{1.10}$$

The above equation is true for all natural numbers n. Hence it is true for mn. Hence

$$\frac{\varphi(mn)}{mn} = \prod_{p|mn}\left(1 - \frac{1}{p}\right). \tag{1.11}$$

Note that each prime divisor of mn is either a prime divisor of m or of n, and those prime which divide both m and n also divide $d = (m, n)$. Hence

$$\begin{aligned}\frac{\varphi(mn)}{mn} &= \prod_{p|mn}\left(1-\frac{1}{p}\right)\\ &= \frac{\prod_{p|m}\left(1-\frac{1}{p}\right)\prod_{p|n}\left(1-\frac{1}{p}\right)}{\prod_{p|d}\left(1-\frac{1}{p}\right)}\\ &= \frac{\frac{\varphi(m)}{m}\frac{\varphi(n)}{n}}{\frac{\varphi(d)}{d}} \text{ (by theorem 1.1.24)}\\ &= \varphi(m)\varphi(n)\left(\frac{d}{\varphi(d)}\right).\end{aligned}$$

(c)By part (b) we have

$$\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}, \quad \text{where } d = (m, n).$$

Putting $d = 1$ in the above equation, we obtain

$$\begin{aligned}\varphi(mn) &= \varphi(m)\varphi(n)\frac{1}{\varphi(1)}\\ &= \varphi(m)\varphi(n) \text{ (since } \varphi(1) = 1).\end{aligned}$$

(d)Given that $a|b$.

$$a|b \Rightarrow b = ac,\ 1 \le c \le b.$$

Here we consider 3 cases. **Case 1:** Suppose $b = 1$.
Since $b = 1$ and $1 \le c \le b$, it follows that $c = 1$. This implies that $a = 1$. So $\varphi(a) = \varphi(b) = 1$. Hence $\varphi(a)|\varphi(b)$.
Case 2: Suppose $b > 1$, $c = b$.
In this case $a = 1$. This implies that $\varphi(a) = 1$. Note that 1 divides every integer. In particular $1|\varphi(b)$. Hence $\varphi(a)|\varphi(b)$.
Case 3: $b > 1$, $c < b$.
Now proof is by induction on b.

Step 1: $b = 2$.
Since $1 \le c < b$ and $b = 2$, it follows that $c = 1$. Hence $a = 2$. Therefore $\varphi(a)|\varphi(b)$.

Step 3: Assume that the result is true for all positive integers less than b(That is, whenever $\lambda|\mu$, $\mu < b$, then $\varphi(\lambda)|\varphi(\mu)$).

Step 2: Now to show that the result is true for b.
Let $d = (a, c)$. Then $d|c$. Since $c < b$, by induction hypothesis, we have

$$\varphi(d)|\varphi(c) \Rightarrow \frac{\varphi(c)}{\varphi(d)} \in \mathbb{N}.$$

But now

$$\begin{aligned}\varphi(b) &= \varphi(ac)\\ &= \varphi(a)\varphi(c)\frac{d}{\varphi(d)}\\ &= \varphi(a)d\left[\frac{\varphi(c)}{\varphi(d)}\right]\end{aligned}$$

Since $\varphi(c)/\varphi(d)$ is a natural number, it follows that $\varphi(a)|\varphi(b)$.
(e)Let $n \geq 3$. Then

$$n = 2^k m, \quad \text{for some odd number} m.$$

If $m = 1$, then $n = 2^k$, where $k \geq 2$(since $n \geq 3$). Therefore

$$\begin{aligned}\varphi(n) = \varphi(2^k) &= 2^k - 2^{k-1}\\ &= 2(2^{k-1} - 2^{k-2}) = \text{an even number.}\end{aligned}$$

Assume that m is an odd number greater than 1. Then m has an odd prime divisor say p.
Now

$$\begin{aligned}p|m &\Rightarrow \varphi(p)|\varphi(n)(\because n = 2^k m)\\ &\Rightarrow \varphi(p)|\varphi(n)\\ &\Rightarrow (p-1)|\varphi(n)\\ &\Rightarrow 2|\varphi(n)\ (p \text{ is an odd prime})\\ &\Rightarrow \varphi(n) \text{ is even.}\end{aligned}$$

Next assume that

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

where $p_1, p_2, \ldots, p_r \in \{2, 3, 5, 7, \ldots\}$. Then

$$\begin{aligned}\varphi(n) &= n\prod_{p|n}\left(1 - \frac{1}{p}\right)\\ &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)\\ &= p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1)(p_2 - 1)\cdots(p_n - 1)\end{aligned}$$

Since each p_i is odd it follows that each $(p_i - 1)$ is even. This implies 2^r divides $\varphi(n)$. This completes the proof. □

1.1.5 Dirichlet product of arithmetical functions

Definition 1.1.4. *Let f and g be arithmetical functions. Then the* Dirichlet product *of f and g is denoted by $f * g$ and is defined as*

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

$$= \sum_{ab=n} f(a)f(b), \tag{1.12}$$

where the sum on the right-hand side of (1.12) runs over all ordered pairs (a, b) of positive integers satisfying $ab = n$.

Definition 1.1.5. *If α is a complex number, the power function N^α is an arithmetical function is defined as*

$$N^\alpha(n) = n^\alpha, \forall n \in \mathbb{N}.$$

Definition 1.1.6. *The unit function u is defined as*

$$u(n) = 1 \quad \forall n \in \mathbb{N}.$$

Definition 1.1.7. *The identity function I is defined as*

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

Remark 1. *Theorem 1.1.1 can be stated in the form $\varphi = \mu * u$.*

We have

$$\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right]$$

Now

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{d|n} \mu(d) u\left(\frac{n}{d}\right) \\ &= (\mu * u)(n) \end{aligned}$$

Remark 2. *Theorem 1.1.3 can be sated in the form $\mu * N = \varphi$.*

We have

$$\begin{aligned} \varphi(n) &= \sum_{d|n} \mu(d) \frac{n}{d} \\ &= \sum_{d|n} \mu(d) N\left(\frac{n}{d}\right) \\ &= (\mu * N)(n). \end{aligned}$$

Theorem 1.1.6. *Dirichlet multiplication is commutative and associative. That is, for any multiplicative functions f, g, h we have*

$$f * g = g * f (\textit{Commutative law})$$
$$f * (g * h) = (f * g) * h (\textit{Associative law})$$

Proof. Let f and g be two arithmetical functions. Then

$$\begin{aligned}(f*g)(n) &= \sum_{d|n} f(n)g\left(\frac{n}{d}\right)\\ &= \sum_{ab=n} f(a)g(b)\\ &= \sum_{ba=n} g(b)f(a)\\ &= (g*f)(n).\end{aligned}$$

Hence the Dirichlet product is commutative. That is $f*g = g*f$. Next, we prove that Dirichlet multiplication is associative.
Let $k = g*h$ and $\ell = f*g$. Then

$$\begin{aligned}(f*(g*h))(n) &= (f*k)(n)\\ &= \sum_{ad=n} f(a)k(d)\\ &= \sum_{ad=n} f(a)(g*h)(d)\\ &= \sum_{ad=n} f(a)\sum_{bc=d} g(b)h(c)\\ &= \sum_{abc=n} f(a)g(b)h(c).\end{aligned}$$

$$\begin{aligned}((f*g)*h)(n) &= (\ell*h)(n)\\ &= \sum_{dc=n} \ell(d)h(c)\\ &= \sum_{dc=n} (f*g)(d)f(c)\\ &= \sum_{dc=n}\sum_{ab=d} f(a)g(b)h(c)\\ &= \sum_{abc=n} f(a)g(b)h(c).\end{aligned}$$

Hence $(f*g)*h = f*(g*h)$. □

Theorem 1.1.7. *For any arithmetical function f we have*

$$f*I = I*f = f,$$

where I is the identity function.

Proof. By the definition of Dirichlet product, we have

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

$$
\begin{aligned}
&= I(1)f(n) + \sum_{\substack{d|n \\ d>1}} I(d) f\left(\frac{n}{d}\right) \\
&= f(n) + \sum_{\substack{d|n \\ d>1}} \left[\frac{1}{d}\right] f\left(\frac{n}{d}\right) \\
&= f(n) + 0 \ (\because I(1) = 1I(d) = 0 \text{ if } d > 1.) \\
&= f(n).
\end{aligned}
$$

Hence

$$I * f = f.$$

Since Dirichlet product is commutative, we have $f * I = f$. □

1.1.6 Dirichlet inverses and Mobius inversion formula

Theorem 1.1.8. *If f is an arithmetical function with $f(1) \neq 0$, then there is a unique inverse f^{-1} of f called Dirichlet inverse of f such that*

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

Moreover f^{-1} is given by

$$f^{-1}(n) = \begin{cases} \frac{1}{f(1)} & \text{if } n = 1, \\ -\frac{1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) & \text{if } n > 1. \end{cases}$$

Proof. The proof is by induction on n. Given that $f(1) \neq 0$. Then

$$\frac{1}{f(1)} \in \mathbb{C}.$$

Take $f^{-1}(1) := \frac{1}{f(1)}$. Then $f^{-1}(1)$ is unique. Also

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

Hence the result is true for $n = 1$.
Next assume that the result is true for all natural numbers less than n. That is $f^{-1}(r)$ is uniquely determined for all $r < n$, $f * f^{-1}(r) = I$ for all $r < n$ and

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

We will prove that $(f * f^{-1})(n) = I(n)$ and

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

Define

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

Consider

$$\begin{aligned}
(f * f^{-1})(n) &= \sum_{d|n} f\left(\frac{n}{d}\right) f^{-1}(d), \\
&= f\left(\frac{n}{n}\right) f^{-1}(n) + \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) \\
&= f(1) f^{-1}(n) + \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) \\
&= f(1) \left[-\frac{1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) \right] + \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) \\
&= -\sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) + \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) = 0.
\end{aligned}$$

This implies that the result is true for n. Hence by mathematical induction the result is true for all natural numbers. □

Theorem 1.1.9. *Let*

$$\mathscr{A} := \{f : f \text{ is arithmetical and } f(1) \neq 0\}$$

Then $\mathscr{A}$ is an abelian group under Dirichlet product.

Proof.

Closure property: Let $f, g \in \mathscr{A}$. Then $f(1) \neq 0$ and $g(1) \neq 0$. Also note that $f * g$ is an arithmetical function. Also

$$(f * g)(1) = f(1)g(1) \neq= 0.$$

Hence $f * g \in \mathscr{A}$.

Associative property: By theorem 1.1.6 it follows that $*$ is associative.

Existence of identity: The existence of each element in $\mathscr{A}$ follows from theorem 1.1.8.

Existence of inverse: Note that I is the identity element (see theorem 1.1.7).

Commutative property: By theorem 1.1.6 it follows that $*$ is commutative.

Hence $(\mathscr{A}, *)$ is an abelian group. □

Remark 3. *The functions μ and u are inverses of each other.*

Proof. From theorem 1.1.1 we have

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

The above equation can be written as

$$\sum_{d|n} \mu(d) u\left(\frac{n}{d}\right) = I(n). \ (\because u(n) = 1 \ \ \forall n)$$

That is

$$(\mu * u)(n) = I(n) \ \ \forall n$$

This completes the proof. □

Theorem 1.1.10 (Mobius inversion formula)**.** *We have*

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

That is

$$f = g * u \Leftrightarrow g = f * \mu.$$

Proof. Note that $u^{-1} = \mu$. Hence

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

This completess the proof. □

Corollary 1. *If $n \geq 1$ we have*

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

Proof. We have

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

By Mobius inversion formula,

$$\begin{aligned} \varphi(n) &= (N * \mu)(n) \\ &= \sum_{d|n} \mu(d) N\left(\frac{n}{d}\right) \ \ (\because N(n) = n \ \forall n) \\ &= \sum_{d|n} \mu(d)\left(\frac{n}{d}\right). \end{aligned}$$

This completes the proof. □

1.1.7 The Mangoldt function $\Lambda(n)$

Definition 1.1.8. *For every integer $n \geq 1$ the Mangoldt's function $\Lambda(n)$ is defined as:*

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

A short table values of $\Lambda(n)$ is given below:

n	1	2	3	4	5	6	7	8	9	10
$\Lambda(n)$	0	$\log 2$	$\log 3$	$\log 2$	$\log 5$	0	$\log 7$	$\log 2$	$\log 3$	0

Theorem 1.1.11. *If $n \geq 1$ we have*

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

Proof. Here we consider two cases:
Case 1: Suppose $n = 1$.
In this case

$$\sum_{d|n} \Lambda(d) = \sum_{d|1} \Lambda(d) = \Lambda(1) = 0$$

Hence the theorem is true for $n = 1$.
Case 2: Suppose $n > 1$.
In this case n can be expressed in the following form:

$$n = p_1^{\alpha_1} p_1^{\alpha_2} \cdots p_1^{\alpha_k},$$

where p_i's are distinct primes and $\alpha_i \geq 1$. Taking logarithms we have

$$\log n = \sum_{i=1}^{k} \alpha_i \log p_i. \tag{1.13}$$

Observe that non zero terms in $\sum_{d|n} \Lambda(d)$ occcurs only when

$$d = p_1, p_1^2, \ldots, p_k^{\alpha_1}; p_2, p_2^2, \ldots, p_2^{\alpha_2}; \ldots; p_k, p_k^2, \ldots, p_k^{\alpha_k}.$$

Hence

$$\begin{aligned} \sum_{d|n} \Lambda(d) &= \Lambda(p_1) + \Lambda(p_1^2) + \cdots + \Lambda(p_1^{\alpha_1}) + \Lambda(p_2) + \Lambda(p_2^2) + \cdots + \Lambda(p_2^{\alpha_2}) + \cdots \\ &\quad \Lambda(p_k) + \Lambda(p_k^2) + \cdots + \Lambda(p_k^{\alpha_k}) \\ &= \underbrace{(\log p_1 + \log p_1 + \cdots + \log p_1)}_{\alpha_1 \text{ times}} + \underbrace{(\log p_2 + \log p_2 + \cdots + \log p_2)}_{\alpha_2 \text{ times}} + \cdots \\ &\quad \underbrace{(\log_k + \log p_k + \cdots + \log p_k)}_{\alpha_k \text{ times}} \end{aligned}$$

$$= \alpha_1 \log p_1 + \alpha_2 \log p_2 + \cdots + \alpha_k \log p_k$$
$$= \sum_{i=1}^{k} \alpha_i \log p_i. \tag{1.14}$$

From the light of equations (1.13) and (1.14), we have

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

This completes the proof. □

Theorem 1.1.12. *If $n \geq 1$ we have*

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

Proof. By theorem 1.1.11, we have

$$\log n = \sum_{d|n} \Lambda(n) = \sum_{d|n} \Lambda(n) u\left(\frac{n}{d}\right) = (\Lambda * u)(n).$$

By Möbius inversion formula, we have

$$\begin{aligned}
\Lambda(n) &= \sum_{d|n} \mu(d) \log\left(\frac{n}{d}\right) \\
&= \sum_{d|n} \mu(d) \log n - \sum_{d|n} \mu(d) \log d \\
&= \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d \\
&= (\log n)\left[\frac{1}{n}\right] - \sum_{d|n} \mu(d) \log d \ (\because \sum_{d|n} \mu(d) = \left[\frac{1}{n}\right]) \\
&= -\sum_{d|n} \mu(d) \log d.
\end{aligned}$$

This completes the proof. □

1.1.8 Multiplicative functions

We have already proved that the set of all arithmetical function f with $f(1) \neq 0$(see theorem 1.1.9) forms an abelian group under Dirichlet multiplication. In this section we discuss an important subgroup of this group, called multiplicative functions.

Definition 1.1.9. *An arithmetical function f is called* multiplicative *if*

(a) f not identically zero,

(b) $f(mn) = f(m)f(n)$, *whenever* $(m, n) = 1$.

Definition 1.1.10. *An arithmetical function* f *is called* completely multiplicative *if*

(a) f *not identically zero,*

(b) $f(mn) = f(m)f(n)$, *for all* $m, n \in \mathbb{N}$.

Note : Consider the following sets:

$$\begin{aligned}\mathscr{A} &:= \{f : f \text{ is arithmetical and } f(1) \neq 0\},\\ \mathscr{M} &:= \{f \in \mathcal{A} : f \text{ is multiplicative}\},\\ \mathscr{C} &:= \{f \in \mathcal{A} : f \text{ is completely multiplicative}\}.\end{aligned}$$

Then we have

$$\mathscr{M} \subset \mathscr{C} \subseteq \mathscr{A}.$$

Moreover $\mathscr{M}$ is a subgroup of $(\mathscr{A}, *)$. Unlike $\mathscr{M}$, which is a group with respect to Dirichlet product, $\mathscr{C}$ is closed neither with respect to addition nor convolution.

Theorem 1.1.13. *If* f *is multiplicative then* $f(1) = 1$.

Proof. Since f is multiplicative, we have

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

Note that for any $n \in \mathbb{N}$, we have $(n, 1) = 1$. Hence by definition,

$$f(n) = f(n \cdot 1) = f(n)f(1)$$

This implies that

$$f(n)[f(1) - 1] = 0.$$

Since f is not identically zero, we have $f(1) - 1 = 0$. That is $f(1) = 1$. □

Theorem 1.1.14. *Let* f *be an arithmetical function with* $f(1) = 1$. *Then*

(a) f *is multiplicative if and only if*

$$f\left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\right) = f\left(p_1^{\alpha_1}\right) f\left(p_2^{\alpha_2}\right) \cdots f\left(p_k^{\alpha_k}\right)$$

for all primes p_i *and all integers* $\alpha_i \geq 1$.

(b) If f *is multiplicative, then* f *is completely multiplicative if and only if*

$$f\left(p^{\alpha}\right) = f(p)^{\alpha}$$

for all primes p *and all integers* $\alpha \geq 1$.

Proof. (a) First assume that f is multiplicative. Then $f(mn) = f(m)f(n)$ whenever $(m,n) = 1$. We prove the the result by induction on k.
Step 1: Assume that $k = 1$. In this case we have

$$f\left(p_1^{\alpha_1}\right) = f\left(p_1^{\alpha_1}\right)$$

Hence the result is true for $n = 1$.
Step 2: Assume that the result is true for all integers $< k$.
That is

$$f\left(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_i^{\alpha_i}\right) = f\left(p_1^{\alpha_1}\right)f\left(p_2^{\alpha_2}\right)\cdots f\left(p_i^{\alpha_i}\right) \quad \forall\ i < k.$$

Case 3: We will prove that the result is true for k.
Now

$$\begin{aligned} f\left(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}\right) &= f\left(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_{k-1}^{\alpha_{k-1}}p_k^{\alpha_k}\right) \\ &= f\left(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_{k-1}^{\alpha_{k-1}}\right)f(p_k^{\alpha_k}) \ (\because f \text{ is multiplicative}) \\ &= f\left(p_1^{\alpha_1}\right)f\left(p_2^{\alpha_2}\right)\cdots f\left(p_{k-1}^{\alpha_{k-1}}\right)f\left(p_k^{\alpha_k}\right) \ \text{(by induction hypothesis)} \end{aligned}$$

Hence the result is true for k. Hence by mathematical induction the result is true for all natural numbers.
Conversely assume that

$$f\left(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}\right) = f\left(p_1^{\alpha_1}\right)f\left(p_2^{\alpha_2}\right)\cdots f\left(p_k^{\alpha_k}\right) \quad \forall k \in \mathbb{N}.$$

We will prove that f is multiplicative. Let $m, n \in \mathbb{N}$ such that $(m,n) = 1$. Let

$$\begin{aligned} m &= p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}, \\ n &= q_1^{\beta_1}q_2^{\beta_2}\cdots q_s^{\beta_s} \end{aligned}$$

where p_i's and q_j's are distinct primes and $\alpha_i, \beta_i \geq 1$ are integers. Then

$$\begin{aligned} f(mn) &= f\left(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}q_1^{\beta_1}q_2^{\beta_2}\cdots q_s^{\beta_s}\right) \\ &= f\left(p_1^{\alpha_1}\right)f\left(p_2^{\alpha_2}\right)\cdots f\left(p_k^{\alpha_k}\right)f\left(q_1^{\beta_1}\right)f\left(q_2^{\beta_2}\right)\cdots f\left(q_k^{\beta_s}\right) \text{(by assumption)} \\ &= f\left(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}\right)f\left(q_1^{\beta_1}q_2^{\beta_2}\cdots q_k^{\beta_s}\right) \\ &= f(m)f(n) \end{aligned}$$

(b) First assume that f is completely multiplicative. Then

$$f(mn) = f(m)f(n) \quad \forall \ \ m, n \in \mathbb{N}$$

Claim : $f\left(p^{\alpha}\right) = f(p)^{\alpha}$ for all primes p and all integers $\alpha_i \geq 1$. We will prove the theorem by induction on α.
Step 1: Assume that $\alpha = 1$. Note that $f(p^1) = f(p)^1$. Hence the result is true for $n = 1$.

Step 2: Assume that the result is true for all integers $< k$.
That is

$$f\left(p^i\right) = f(p)^i \quad \forall i < k.$$

Step 3: We will prove that the result is true for k.
Now

$$\begin{aligned} f\left(p^\alpha\right) &= f\left(p^{\alpha-1}p\right) \\ &= f\left(p^{\alpha-1}\right) f(p) (\because \ f \text{ completely multiplicative}) \\ &= [f(p)]^{\alpha-1} f(p) = [f(p)]^\alpha \text{ (by assumption).} \end{aligned}$$

Hence by mathematical induction $f\left(p^\alpha\right) = f(p)^\alpha$ for all $\alpha \in \mathbb{N}$.
Conversely assume that

$$f\left(p^\alpha\right) = f(p)^\alpha \quad \text{for all } k.$$

We will prove that f is completely multiplicative. Let $m, n \in \mathbb{N}$. Let $(m, n) = d$. Then $m = ad$ and $n = bd$ for some $a, b \in \mathbb{N}$.Let

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \quad b = q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}, \ d = d_1^{\gamma_1} d_2^{\gamma_2} \dots d_t^{\gamma_t}$$

Then

$$\begin{aligned} m &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} d_1^{\gamma_1} d_2^{\gamma_2} \dots d_t^{\gamma_t} \\ n &= q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s} d_1^{\gamma_1} d_2^{\gamma_2} \dots d_t^{\gamma_t} \\ mn &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s} d_1^{2\gamma_1} d_2^{2\gamma_2} \dots d_t^{2\gamma_t}. \end{aligned}$$

Now

$$\begin{aligned} f(mn) &= f\left(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s} d_1^{2\gamma_1} d_2^{2\gamma_2} \dots d_t^{2\gamma_t}\right) \\ &= f\left(p_1^{\alpha_1}\right) f\left(p_2^{\alpha_2}\right) \cdots f\left(p_k^{\alpha_k}\right) f\left(q_1^{\beta_1}\right) f\left(q_2^{\beta_2}\right) \cdots f\left(q_s^{\beta_s}\right) \\ &\qquad f\left(d_1^{2\gamma_1}\right) f\left(d_2^{2\gamma_2}\right) \cdots f\left(d_t^{2\gamma_t}\right) \quad (\because f \text{ is multiplicative}) \\ &= f(p_1)^{\alpha_1} f(p_2)^{\alpha_2} \cdots f(p_k)^{\alpha_k} f(q_1)^{\beta_1} f(q_2)^{\beta_2} \cdots f(q_s)^{\beta_s} \\ &\qquad f(d_1)^{2\gamma_1} f(d_2)^{2\gamma_2} \cdots f(d_t)^{2\gamma_t} \text{ (by assumption)} \end{aligned}$$

Again

$$\begin{aligned} f(m)f(n) &= f\left(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} d_1^{\gamma_1} d_2^{\gamma_2} \dots d_t^{\gamma_t}\right) f\left(q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s} d_1^{\gamma_1} d_2^{\gamma_2} \dots d_t^{\gamma_t}\right) \\ &= f\left(p_1^{\alpha_1}\right) f\left(p_2^{\alpha_2}\right) \cdots f\left(p_k^{\alpha_k}\right) f\left(d_1^{\gamma_1}\right) f\left(d_2^{\gamma_2}\right) \cdots f\left(d_t^{\gamma_t}\right) \\ &\qquad f\left(q_1^{\beta_1}\right) f\left(q_2^{\beta_2}\right) \cdots f\left(q_s^{\beta_s}\right) f\left(d_1^{\gamma_1}\right) f\left(d_2^{\gamma_2}\right) \cdots f\left(d_t^{\gamma_t}\right) \\ &= f(p_1)^{\alpha_1} f(p_2)^{\alpha_2} \cdots f(p_k)^{\alpha_k} f(q_1)^{\beta_1} f(q_2)^{\beta_2} \cdots f(q_s)^{\beta_s} \\ &\qquad f(d_1)^{2\gamma_1} f(d_2)^{2\gamma_2} \cdots f(d_t)^{2\gamma_t} \end{aligned}$$

Hence $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$. That is f is completely multiplicative. □

1.1.9 Examples of completely multiplicative functions

1. The arithmetical function $N^\alpha(n) = n^\alpha \ \forall \ n \in \mathbb{N}$ is completely multiplicative.
   For all $m, n \in \mathbb{N}$, we have

   $$N(mn) = (mn)^\alpha = N(m)N(m).$$

   Hence N^α is completely multiplicative. In particular N is completely multiplicative.

2. The unit function $u(n) = 1$ for all $n \in \mathbb{N}$ is completely multiplicative.
   For all $m, n \in \mathbb{N}$, we have

   $$u(mn) = 1 = 1.1 = u(m)u(n).$$

3. The identity function is completely multiplicative.
   Here we consider several cases:
   Case 1: Suppose $m = 1, n = 1$.
   Then $mn = 1$. Therefore

   $$I(m) = 1, I(n) = 1, I(mn) = 1$$

   Hence

   $$I(mn) = I(m)I(n)$$

   Case 2: Suppose $m = 1$ and $n > 1$.
   In this case $mn > 1$. So we have

   $$I(m) = 1, I(n) = 0, I(mn) = 0$$

   Thus

   $$I(mn) = 0 = 1 \times 0 = I(m)I(n).$$

   Case 3: Suppose $n = 1$, $m > 1$.
   In this case $mn > 1$. Moreover $I(n) = 1$, $I(m) = 0$ and $I(mn) = 0$. Hence

   $$I(mn) = 0 = 0 \times 1 = I(m)I(n).$$

   Case 4: Suppose $m, n > 1$.
   In this case $mn > 1$. Moreover $I(m) = I(n) = I(mn) = 0$. Hence

   $$I(mn) = 0 = 0 \times 0 = I(m)I(n).$$

1.1.10 Examples of multiplicative functions

1. The Euler function φ is multiplicative but not completely multiplicative.
   Let $m, n \in \mathbb{N}$ such that $(m, n) = 1$. Then we have

   $$\varphi(mn) = \varphi(m)\varphi(n) \quad \text{(see theorem 1.20(c))}$$

Observe that φ is not completely multiplicative. Let $m = 4$ and $n = 2$. Then $(m, n) \neq 1$. By the definition of φ we have

$$\varphi(8) = 4, \varphi(4) = 2, \varphi(2) = 1.$$

Hence

$$\varphi(mn) = \varphi(8) = 4 \neq 2 \times 1 = \varphi(4)\varphi(2) = \varphi(m)\varphi(n).$$

2. The Mobius function is multiplicative but not completely multiplicative. Let $m, n \in \mathbb{N}$ such that $(m, n) = 1$.
Case 1: If either $m = 1$ or $n = 1$, then obviously

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

Case 2: m is square free and n is not square free.
Then clearly mn is not square free. Then by the definition of μ, we have $\mu(mn) = 0$ and $\mu(n) = 0$. Hence

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

Case 3: m is not square free and n is square free.
This case is exactly similar to case 2.
Case 4: Both m and n are square free.
Since m and n are relatively prime, mn is square free. Let

$$m = p_1 p_2 \cdots p_m,$$

where p_i's are distinct primes. Similarly, let

$$q = q_1 q_2 \ldots q_n,$$

where q_i's are distinct primes. Then

$$\mu(m) = (-1)^m, \mu(n) = (-1)^n \text{ and } \mu(mn) = (-1)^{m+n}.$$

Hence

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

Hence μ is completely multiplicative. Next we will show that μ is not completely multiplicative. Let $m = 2$ and $n = 2$. Then $\mu(4) = 0$ and $\mu(2) = -1$. Note that $\mu(4) \neq \mu(2)\mu(2)$. Hence μ is not completely multiplicative.

1.1.11 Multiplicative functions and Dirichlet multiplication

Theorem 1.1.15. *If f and g are multiplicative, so is their Dirichlet product $f * g$.*

Proof. Since f and g are multiplicative functions, we have $f(1) = 1$ and $g(1) = 1$. Now

$$(f * g)(1) = \sum_{d|1} f(d)g(1/d) = f(1)g(1) = 1$$

Hence $(f * g)(1) \neq 0$. Let $m, n \in \mathbb{N}$ such that $(m, n) = 1$. Note that

$$d|mn \Leftrightarrow d = ab, \text{ where } a|m, b|m \text{ and} (a, b) = 1.$$

Now

$$\begin{aligned}
(f * g)(mn) &= \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) \\
&= \sum_{\substack{a|m \\ b|n}} f(ab)g\left(\frac{mn}{ab}\right) \\
&= \sum_{\substack{a|m \\ b|n}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) \\
&\qquad (\because f \text{ and } g \text{ are multiplicative}, \quad (a, b) = 1 \& \left(\frac{m}{a}, \frac{n}{b}\right) = 1) \\
&= \sum_{a|m} f(a)g\left(\frac{m}{a}\right) \sum_{b|n} f(b)\left(\frac{n}{b}\right) \\
&= (f * g)(m)(f * g)(n).
\end{aligned}$$

This completes the proof. □

Remark 4. *The Dirichlet product of two completely multiplicative functions need not be completely multiplicative.*

Proof. Observe that the arithmetical functions u and N are completely multiplicative. We will prove that the function $f = u * N$ is not completely multiplicative. To prove that f is not completely multiplicative it suffices to prove that for any prime number p, we have $f(p^\alpha) \neq f(p)^\alpha$.
Now

$$\begin{aligned}
f(p^\alpha) &= (u * N)(p^\alpha) \\
&= \sum_{d|p^\alpha} u(d)N(p^\alpha/d) \\
&= \sum_{d|p^\alpha} \frac{p^\alpha}{d} \\
&= \frac{p^\alpha}{1} + \frac{p^\alpha}{p} + \frac{p^\alpha}{p^2} + \cdots + \frac{p^\alpha}{p^\alpha} \\
&= p^\alpha + p^{\alpha-1} + \cdots + 1.
\end{aligned}$$

Again

$$\begin{aligned} f(p) &= (u * N)(p) \\ &= \sum_{d|1} u(d)N(p/d) = u(1)N(p) = p \end{aligned}$$

Therefore

$$f(p)^\alpha = p^\alpha \neq p^\alpha + p^{\alpha-1} + \cdots + 1 = f\left(p^\alpha\right).$$

Hence f is not completely multiplicative. □

Theorem 1.1.16. *Let f, g be arithmetic functions. If both g and $f * g$ are multiplicative, then f is also multiplicative.*

Proof. Since g and $f * g$ are multiplicative, we have $g(1) = 1$ and $(f * g)(1) = 1$. Now

$$1 = (f * g)(1) = \sum_{d|1} f(d)g\left(\frac{1}{d}\right) = f(1)g(1) = f(1)(1) = f(1).$$

Hence $f \neq 0$.
Claim : f is multiplicative.That is, $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$. We prove the claim by induction on mn.

Step 1: Assume that $mn = 1$.
In this case $m = n = 1$. Note that

$$f(mn) = f(1) = 1 = f(m)f(n).$$

Hence the result is true for $mn = 1$.

Step 2: Assume that the result is true for all products ab less than mn.

Step 3: We prove the claim for mn.
Note that

$$\begin{aligned} (f * g)(mn) &= \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) \\ &= \sum_{\substack{a|m \\ b|n}} f(ab)g\left(\frac{mn}{ab}\right) \\ &= f(mn)g(1) + \sum_{\substack{a|m \\ b|n \\ ab<mn}} f(ab)g\left(\frac{mn}{ab}\right) (\because (a, b) = 1) \\ &= f(mn) + \sum_{\substack{a|m \\ b|n \\ ab<mn}} f(a)f(b)g\left(\frac{m}{a}\right) g\left(\frac{n}{b}\right) \left(\because \left(\frac{m}{a}, \frac{n}{b}\right) = 1\right) \\ &= f(mn) + \sum_{\substack{a|m \\ b|n \\ ab<mn}} f(a)g\left(\frac{m}{a}\right) f(b)g\left(\frac{n}{b}\right) + f(m)f(n) - f(m)f(n) \end{aligned}$$

$$
\begin{aligned}
&= f(mn) + \sum_{\substack{a|m\\ b|n\\ ab<mn}} f(a)g\left(\frac{m}{a}\right) f(b)g\left(\frac{n}{b}\right) + f(m)g\left(\frac{m}{m}\right) f(n)g\left(\frac{n}{n}\right) - f(m)f(n)\\
&= f(mn) + \sum_{\substack{a|m\\ b|n}} f(a)g\left(\frac{m}{a}\right) f(b)g\left(\frac{n}{b}\right) - f(m)f(n)\\
&= f(mn) + \sum_{a|m} f(a)g\left(\frac{m}{a}\right) \sum_{b|n} f(b)g\left(\frac{n}{b}\right) - f(m)f(n)\\
&= f(mn) + (f*g)(m)(f*g)(n) - f(m)f(n)\\
&= f(mn) + (f*g)(mn) - f(m)f(n) \ (\because f*g \text{ is multiplicative})
\end{aligned}
$$

This implies that $f(mn) - f(m)f(n) = 0$. That is $f(mn) = f(m)f(n)$. □

Theorem 1.1.17. *If g is multiplicative, then its Dirichlet multiplicative g^{-1} is also multiplicative.*

Proof. First observe that $I = g*g^{-1}$. We have already seen that I is completely multiplicative and hence multiplicative. Hence g and $g*g^{-1}$ are multiplicative. So by theorem 1.1.16, g^{-1} is multiplicative.
This completes the proof. □

1.1.12 The inverse of a completely multiplicative function

Theorem 1.1.18. *Let f be a multiplicative function. Then f is multiplicative if and only if*

$$f^{-1}(n) = \mu(n)f(n) \quad \text{for all } n \geq 1.$$

Proof. Assume that f is completely multiplicative. Let $g(n) = \mu(n)f(n)$. We want to show that $f^{-1}(n) = g(n)$. Now

$$
\begin{aligned}
(g*f)(n) &= \sum_{d|n} g(d)f\left(\frac{n}{d}\right)\\
&= \sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right)\\
&= \sum_{d|n} \mu(d)f\left(d\frac{n}{d}\right) \quad (\because f \text{ is completely multiplicative })\\
&= \sum_{d|n} \mu(d)f\left(n\right)\\
&= f(n)\sum_{d|n} \mu(d)\\
&= f(n)I(n)\\
&= \begin{cases} 1 & \text{if } n = 1\\ 0 & \text{if } n > 1. \end{cases}
\end{aligned}
$$

Remark 5. *The Dirichlet inverse of the Euler totient function is given by*

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

Proof. Since $\varphi = \mu * N$ we have

$$\varphi^{-1} = \mu^{-1} * N^{-1}$$

We have already proved that N is completely multiplicative. Therefore by previous theorem,

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

Hence

$$\varphi^{-1} = \mu^{-1} * N^{-1} = \mu^{-1} * \mu N = u * \mu N$$

Therefore

$$\begin{aligned}
\varphi^{-1}(n) &= (u * \mu N)(n) \\
&= \sum_{d|n} \mu N(d) u\left(\frac{n}{d}\right) \\
&= \sum_{d|n} (\mu N)(d) \\
&= \sum_{d|n} \mu(d)N(d) = \sum_{d|n} \mu(d)d.
\end{aligned}$$

This completes the proof. □

Theorem 1.1.19. *If f is multiplicative we have*

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

Proof. Let

$$\begin{aligned}
g(n) &= \sum_{d|n} f(d)\mu(d) \\
&= \sum_{d|n} (f\mu)(d) \\
&= \sum_{d|n} (f\mu)(d) u\left(\frac{n}{d}\right) \\
&= (f\mu * u)(n)
\end{aligned}$$

Hence

$$g = f\mu * u.$$

Since f and μ are multiplicative, so is $f\mu$. Also observe that u is multiplicative. This implies that $f\mu * u$ is multiplicative.
Now

$$\begin{aligned} g(p^\alpha) &= (f\mu * u)(p^\alpha) \\ &= \sum_{d|p^\alpha} (f\mu)(d) u\left(\frac{p^\alpha}{d}\right) \\ &= \sum_{d|p^\alpha} (f\mu)(d) \\ &= \sum_{d|p^\alpha} f(d)\mu(d) \\ &= f(1)\mu(1) + f(p)\mu(p) + f(p^2)\mu(p^2) + \cdots + f(p^\alpha)\mu(p^\alpha) \\ &= 1 - f(p) \quad (\because f(1) = 1, \mu(p^2) = \mu(p^3) = \cdots = 0) \end{aligned}$$

Let

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

where p_i's are distinct primes and $\alpha \geq 1$.. Since g is multiplicative we have

$$\begin{aligned} g(n) &= g(p_1^{\alpha_1}) g(p_2^{\alpha_2}) \cdots g(p_k^{\alpha_k}) \\ &= (1 - f(p_1)(1 - f(p_2)) \cdots (1 - f(p_k)) \\ &= \prod_{p|n} (1 - f(p)) \end{aligned}$$

This completes the proof. □

Corollary 2. *The Dirichlet inverse of φ is given by*

$$\varphi^{-1} = \prod_{p|n} (1 - f(p)).$$

Proof. From remark 5, we have

$$\begin{aligned} \varphi^{-1}(n) &= \sum_{d|n} \mu(d) d \\ &= \sum_{d|n} \mu(d) N(d) \\ &= \prod_{p|n} (1 - N(p)) \quad \text{(by theorem 1.1.19)} \\ &= \prod_{p|n} (1 - p) \end{aligned}$$

This completes the proof of the theorem. □

1.1.13 Liouville's function $\lambda(n)$

Definition 1.1.11. *The Liouville's function λ is defined as:*

$$\lambda(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^{\alpha_1+\alpha_2+\cdots+\alpha_k} & \text{if } n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \end{cases}$$

where p_i's distinct primes and $\alpha_i \geq 1$ are integers.

Remark 6. *The Liouville's function is a completely multiplicative function.*

Proof. From the definition of λ we have

$$\begin{aligned} \lambda(p^\alpha) &= (-1)^\alpha \\ &= [\lambda(p)]^\alpha. \end{aligned}$$

This implies that λ is completely multiplicative. □

Theorem 1.1.20. *For every $n \geq 1$, we have*

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

Moreover

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

Proof. Let

$$\begin{aligned} g(n) &= \sum_{d|n} \lambda(d) \\ &= \sum_{d|n} \lambda(d) u\left(\frac{n}{d}\right) \end{aligned}$$

Hence

$$g(n) = (\lambda * u)(n)$$

Since λ and μ are multiplicative, $\lambda * \mu$ is multiplicative. Putting $n = p^\alpha$ in the equation

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

we obtain:

$$\begin{aligned} g(p^\alpha) &= \sum_{d|n} \lambda(d) \\ &= \lambda(1) + \lambda(p) + \cdots + \lambda(p^\alpha) \\ &= 1 + (-1) + (-1)^2 + (-1)^3 + \cdots + (-1)^\alpha \end{aligned}$$

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

Let

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

where p_i' s are distinct primes and $i \geq 1$ are integers. Therefore

$$\begin{aligned} g(n) &= g(p_1^{\alpha_1}) g(p_2^{\alpha_2}) \cdots g(p_k^{\alpha_k}) \\ &= \begin{cases} 1 & \text{if each } \alpha_i \text{ is even,} \\ 0 & \text{if at least one } \alpha_i \text{ is odd.} \end{cases} \end{aligned}$$

Assume that each α_i is even. Then $\alpha_i = 2\beta_i$ for β_i,$i = 1, 2, \ldots, k$. This implies that

$$\begin{aligned} n &= p_1^{2\beta_1} p_2^{2\beta_2} \cdots p_k^{2\beta_k} \\ &= \left(p_1^{\beta_1}\right)^2 \left(p_2^{\beta_2}\right)^2 \cdots \left(p_k^{\beta_k}\right)^2, \\ &= \text{a square} \end{aligned}$$

Hence

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

Note that λ is completely multiplicative. Therefore

$$\lambda^{-1}(n) = \lambda(n)\mu(n) \tag{1.15}$$

Claim : $\lambda(n)\mu(n) = |\mu(n)|$ for all n.
We have

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k, \text{ for distinct primes,} \\ 0 & \text{otherwise.} \end{cases}$$

$$\lambda(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^{\alpha_1+\alpha_2+\cdots+\alpha_k} & \text{if } n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \\ 0 & \text{otherwise.} \end{cases}$$

Here we consider 3 cases:
Case 1: Suppose $n = 1$.
In this case $\lambda(n)\mu(n) = 1 = |\mu(1)|$.
Case 2: Suppose $n = p_1 p_2 \cdots p_k$, where p_i's are distinct primes.
Then

$$\mu(n) = (-1)^k, \quad \lambda(n) = (-1)^k.$$

Therefore

$$\lambda(n)\mu(n) = (-1)^k(-1)^k = 1 = |\mu(n)|.$$

Case 3: Suppose $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where p_i's are distinct primes and $\alpha_i \geq 1$. In this case

$$\mu(n) = 0, \quad \lambda(n) = (-1)^{\alpha_1+\alpha_2+\cdots+\alpha_n}$$

Therefore

$$\lambda(n)\mu(n) = 0 = |\mu(n)|.$$

Hence

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

□

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

Definition 1.1.12. *For any real or complex α and any integer $n \geq 1$ the divisor function is defined by*

$$\begin{aligned}\sigma_\alpha(n) &:= \sum_{d|n} d^\alpha, \\ &= \textit{sum of the } \alpha^{th} \textit{ powers of the divisors of } n\end{aligned}$$

Remark 7. *$\sigma_\alpha(n)$ is multiplicative.*

Proof. Note that N^α and u are multiplicative functions. Now

$$\begin{aligned}\sigma_\alpha(n) &= \sum_{d|n} d^\alpha \\ &= \sum_{d|n} N^\alpha(d) u\left(\frac{n}{d}\right) \\ &= (N^\alpha * u)(n).\end{aligned}$$

Hence σ_α is the Dirichlet product of two multiplicative functions N^α and u. Thus σ_α is multiplicative. □

Remark 8. *If $\alpha = 0$, then the divisor function σ_α can be written as:*

$$\begin{aligned}\sigma_0(n) &= \sum_{d|n} d^0 \\ &= \sum_{d|n} 1 \\ &= \textit{Number of the divisors of } n.\end{aligned}$$

The function σ_0 is usually denoted by $d(n)$.

Remark 9. *If $\alpha = 1$, then the divisor function σ_α can be written as:*

$$\begin{aligned}\sigma_1(n) &= \sum_{d|n} d \\ &= \textit{sum of the divisors of } n.\end{aligned}$$

The function σ_1 is denoted by $\sigma(n)$.

Theorem 1.1.21. *For $n \geq 1$, we have*

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

Proof. We have

$$\begin{aligned}\sigma_\alpha(n) &= \sum_{d|n} d^\alpha \\ &= \sum_{d|n} N^\alpha(d) u\left(\frac{n}{d}\right) \\ &= (N^\alpha * u)(n)\end{aligned}$$

Hence $\sigma_\alpha = N^\alpha * u$. Therefore

$$\sigma_\alpha^{-1} = (N_\alpha)^{-1} * u^{-1} = (N_\alpha)^{-1} * \mu. \tag{1.16}$$

Since N^α is completely multiplicative, we have

$$(N^\alpha)^{-1}(n) = N^\alpha(n)\mu(n) = (N^\alpha\mu)(n).$$

Inserting the value of $(N^\alpha)^{-1}$ in equation (1.16) we obtain

$$\begin{aligned}\sigma_\alpha^{-1}(n) &= (N^\alpha\mu) * \mu(n) \\ &= \sum_{d|n} (N^\alpha\mu)(d)\mu\left(\frac{n}{d}\right) \\ &= \sum_{d|n} N^\alpha(d)\mu(d)\mu\left(\frac{n}{d}\right) \\ &= \sum_{d|n} d^\alpha \mu(d)\mu\left(\frac{n}{d}\right).\end{aligned}$$

□

Theorem 1.1.22. *If $n > 1$ and $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where p_i's distinct primes and $\alpha_i \geq 1.$, then*

$$d(n) = \prod_{i=1}^{k} (\alpha_i + 1).$$

Proof. Since d is a multiplicative function we have

$$d\left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\right) = d\left(p_1^{\alpha_1}\right) d\left(p_2^{\alpha_2}\right) \cdots d\left(p_k^{\alpha_k}\right) \tag{1.17}$$

To compute $d\left(p_i^{\alpha_i}\right)$ we note that the divisors of $p_i^{\alpha_i}$ are

$$1, p_i, p_i^2, \ldots, p_i^{\alpha_i}$$

Hence the number of divisors of $p_i^{\alpha_i}$ are $(\alpha_i + 1)$. Therefore,

$$d\left(p_i^{\alpha_i}\right) = (\alpha_i + 1)$$

Hence

$$d(n) = \prod_{i=1}^{k} (\alpha_i + 1)$$

□

Theorem 1.1.23. *If $n > 1$ and $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where p_i's distinct primes and $\alpha_i \geq 1$., then*

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

Proof. Since σ is a multiplicative function we have

$$\sigma\left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\right) = \sigma\left(p_1^{\alpha_1}\right) \sigma\left(p_2^{\alpha_2}\right) \cdots \sigma\left(p_k^{\alpha_k}\right) \tag{1.18}$$

To compute $\sigma\left(p_i^{\alpha_i}\right)$ we note that the divisors of $p_i^{\alpha_i}$ are

$$1, p_i, p_i^2, \ldots, p_i^{\alpha_i}$$

Hence

$$\sigma\left(p_i^{\alpha_i}\right) = 1 + p_i + p_i^2 + \ldots + p_i^{\alpha_i} = \frac{p_i^{(\alpha_i+1)} - 1}{p_i - 1}.$$

Hence

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

□

1.1.15 Generalised convolution

Definition 1.1.13. *Let F be a real or complex valued function defined on the positive real axis $(0, \infty)$ such that $F(x) = 0$ for $0 < x < 1$. Let α be an arithmetical function. Then the sum*

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

is called the generalized convolution of G and α and is denoted by $\alpha \circ F$. Thus

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

Theorem 1.1.24 (Associative property relating α and $*$)**.** *For any arithmetical functions α and β, we have*

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

Proof. For $x > 0$ we have

$$\begin{aligned}
(\alpha \circ (\beta \circ F))(x) &= \sum_{n \leq x} \alpha(n)(\beta \circ F)\left(\frac{x}{n}\right) \\
&= \sum_{n \leq x} \alpha(n) \sum_{m \leq \frac{x}{n}} \beta(m) F\left(\frac{\frac{x}{n}}{m}\right) \\
&= \sum_{n \leq x} \alpha(n) \sum_{mn \leq x} \beta(m) F\left(\frac{x}{mn}\right) \\
&= \sum_{mn \leq x} \alpha(n)\beta(m) F\left(\frac{x}{mn}\right) \\
&= \sum_{k \leq x} \alpha(n)\beta\left(\frac{k}{n}\right) F\left(\frac{x}{k}\right), k = mn \\
&= \sum_{k \leq x} \left(\sum_{n|k} \alpha(n)\beta\left(\frac{k}{n}\right) \right) F\left(\frac{x}{k}\right) \\
&= \sum_{k \leq x} (\alpha * \beta)(k) F\left(\frac{x}{k}\right) \\
&= ((\alpha * \beta) \circ F)(x).
\end{aligned}$$

Therefore $\alpha \circ (\beta \circ F) = (\alpha * \beta) \circ F$. This completes the proof. □

Theorem 1.1.25 (Generalized inversion formula)**.** *Let α has Dirichlet inverse α^{-1}. Then*

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

That is

$$G = \alpha \circ F \Leftrightarrow F = \alpha^{-1} \circ G.$$

Proof. First assume that $G = \alpha \circ F$. Then

$$\begin{aligned}
\alpha^{-1} \circ G &= \alpha^{-1} \circ (\alpha \circ F) \\
&= (\alpha^{-1} * \alpha) \circ F \text{ (by theorem 1.1.24)} \\
&= I \circ F = F.
\end{aligned}$$

Conversely assume that $F = \alpha^{-1} \circ G$. Then

$$\begin{aligned}
\alpha \circ F &= \alpha \circ (\alpha^{-1} \circ G) \\
&= (\alpha * \alpha^{-1}) \circ G \text{(by theorem 1.1.24)} \\
&= I \circ G = G.
\end{aligned}$$

This completes the proof. □

Theorem 1.1.26 (Generalized Mobius inversion formula)**.** *Let α be completely multiplicative. Then*

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

That is

$$G = \alpha \circ F \Leftrightarrow F = \alpha^{-1} \circ G = (\alpha\mu) \circ G.$$

Proof. First assume that $G = \alpha \circ F$. Then

$$\begin{aligned} \alpha^{-1} \circ G &= \alpha^{-1} \circ (\alpha \circ F) \\ &= (\alpha^{-1} * \alpha) \circ F \\ &= I \circ F = F. \end{aligned}$$

That is

$$F = \alpha^{-1} \circ G = (\alpha\mu) \circ G \quad (\because \alpha \text{ is completely multiplicative})$$

Conversely assume that $F = \alpha^{-1} \circ G$. Then

$$\begin{aligned} \alpha \circ F &= \alpha \circ (\alpha^{-1} \circ G) \\ &= (\alpha * \alpha^{-1}) \circ G \\ &= I \circ G = G. \end{aligned}$$

This completes the proof. □

1.1.16 Derivatives of arithmetical functions

Definition 1.1.14. *Let f be an arithmetical function. Then the derivative of f is defined as*

$$f'(n) := f(n) \log n, \quad n \geq 1.$$

Example 1. *The derivative of the function I is 0.*

By definition, the derivative of I is

$$\begin{aligned} I'(n) &= I(n) \log(n) \\ &= \left[\frac{1}{n}\right] \log n \\ &= \begin{cases} 1 \times \log 1 & \text{if } n = 1 \\ 0 \times \log n & \text{if } n > 1. \end{cases} \\ &= 0. \end{aligned}$$

Remark 10. *We have $\Lambda * u = u'$.*

Proof. By the definition of derivative, we have

$$\begin{aligned} u'(n) &= u(n)\log n \\ &= \log n \qquad (u(n)=1) \\ &= \sum_{d|n}\Lambda(d) \text{ (by theorem 1.1.11)} \\ &= \sum_{d|n}\Lambda(d)u\left(\frac{n}{d}\right) \\ &= (\Lambda * u)(n). \end{aligned}$$

This completes the proof. □

Theorem 1.1.27. *If f and g are arithmetical functions we have:*

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

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

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

Proof. (a) By the definition of derivative, we have

$$\begin{aligned} (f+g)'(n) &= (f+g)(n)\log n \\ &= (f(n)+g(n))\log n \\ &= f(n)\log n + g(n)\log n \\ &= f'(n) + g'(n). \end{aligned}$$

(b)Note that

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

(c) Note that $I' = 0$. This implies that $(f*f^{-1})' = 0$. Then by part (b) we have

$$0 = f'*f^{-1} + f*(f^{-1})'$$

This implies that

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

This implies that

$$f^{-1} * \left(f * (f^{-1})'\right) = -f^{-1} * (f' * f^{-1})$$

That is,

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

That is

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

That is

$$(f^{-1})' = -f' * (f * f)^{-1}.$$

This completes the proof. □

1.1.17 The Selberg identity

Theorem 1.1.28. *For $n \geq 1$ we have*

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

Proof. By Remark 10 we have:

$$\Lambda * u = u'. \tag{1.19}$$

Differentiation of this equation gives:

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

That is

$$\Lambda' * u + \Lambda * (\Lambda * u) = u''.$$

Now multiply both sides by $\mu = u^{-1}$ to obtain:

$$(\Lambda' * u) * u^{-1} + (\Lambda * (\Lambda * u) * u^{-1}) = u'' * \mu.$$

That is

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

This implies that

$$(\Lambda' + \Lambda * \Lambda)(n) = (u'' * \mu)(n)$$

That is

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

$$
\begin{aligned}
&= \sum_{d|n} \mu(d) u'\left(\frac{n}{d}\right) \log(n/d) \\
&= \sum_{d|n} \mu(d) u\left(\frac{n}{d}\right) (\log(n/d))^2 \\
&= \sum_{d|n} \mu(d) (\log(n/d))^2.
\end{aligned}
$$

This completes the proof. □

1.1.18 Exercises

1. Find all integers n such that
   (a) $\varphi(n) = n/2$,
   (b) $\varphi(n) = \varphi(2n)$
   (c) $\varphi(n) = 12$.
2. For each of the following statements either give a proof or exhibit a counter example.
   (a) If $(m, n) = 1$ the $(\varphi(m), \varphi(n)) = 1$,
   (b) If n is composite, then $(n, \varphi(n)) > 1$,
   (c) If the same prime divide m and n, then $n\varphi(m) = m\varphi(n)$.
3. Prove that
$$\frac{n}{\varphi(n)} = \sum_{d|n} \frac{\mu^2(d)}{\varphi(d)}$$
4. Prove that $\varphi(n) > 6$ for all n with at most 8 distinct prime factors.
5. Prove that $\sum_{d^2|n} \mu(d) = \mu^2(n)$.
6. Let $f(n) = [\sqrt{n}] - [\sqrt{n-1}]$. Prove that f is multiplicative but not completely multiplicative.
7. Assume that f is multiplicative. Prove that
   (a) $f^{-1}(n) = \mu(n) f(n)$ for every square free n.
   (b) $f^{-1}(p^2) = f(p)^2 - f(p^2)$ for every prime p.
   (a) Assume that f is multiplicative. Prove that f is completely multiplicative if, and only if, $f^{-1}(p^\alpha) = 0$ for all primes p and all integers $a \geq 2$.
   (b) Prove that the following statement or exhibit a counter example. If f is multiplicative, then $F(n) = \sum_{d|n} f(d)$ is multiplicative.

1.2 Averages of arithmetical functions

An arithmetical function is defined to be a function $f(n)$, defined for $n \in \mathbb{N}$, which maps to a complex number such that $f : \mathbb{N} \to \mathbb{C}$. Examples of arithmetic functions include: the number of primes less than a given number n, the number of divisors of n, etc. While the behavior of values of arithmetic functions are hard to predict, it is easier to analyze the behavior of the averages of arithmetic functions which we define as

$$\lim_{n\to\infty} \frac{f(1) + f(2) + \cdots + f(n)}{n} = L$$

where L the average value of $f(n)$.

1. Let $r(n)$ be the number of representations of n as a sum of two squares

   $$n = x^2 + y^2$$

   Then average number of representations of a natural number as a sum of two squares is π. That is,

   $$\lim_{n\to\infty} \frac{r(1) + r(2) + \cdots + r(n)}{n} = \pi$$

2. Let $f(n)$ be the number of decompositions of a natural number n into a sum of one or more consecutive prime numbers. For example, $f(395) = 2$ because

   $$395 = 127 + 131 + 137 = 71 + 73 + 79 + 83 + 89.$$

   Then average number of decompositions of a natural number into a sum of one or more consecutive prime numbers is $\log 2$. That is

   $$\lim_{n\to\infty} \frac{f(1) + f(2) + \cdots + f(n)}{n} = \log 2$$

3. Consider the divisor function $d(n)$ defined by

   $$d(n) = \sum_{d|n} 1.$$

   Note that $d(p) = 2$ for all primes numbers and $d(n)$ is large when n has a large number of divisors. Thus the values of $d(n)$ fluctuate as n increases. In this case it is difficult to determine their behavior as n increases. We can prove that

   $$\frac{d(1) + d(2) + \cdots + d(n)}{n \log n} = 1$$

In chapter paper, we will examine averages of several different arithmetic functions.

1.2.1 The big oh notation. Asymptotic equality of functions

Definition 1.2.1. *Let f and g be real valued functions such that $g(x) > 0$ for all $x \geq a$. We write $f(x) = O(x)$(and say that $f(x)$ is big oh of $g(x)$) if there exists a constant $M > 0$ such that*

$$|f(x)| \leq Mg(x) \quad \textit{for all} \quad x \geq a.$$

- $f(x) = O(g(x))$ means that $|f(x)/g(x)|$ is bounded for all $x \geq a$.
- The equation of the form

  $$f(x) = h(x) + O(g(x))$$

  means that

  $$f(x) - h(x) = O(g(x))$$

- If $f(t) = O(g(t))$ for some $t \geq a$, then $\int_a^x f(t)\, dt = O(\int_a^x g(t)\, dt)$

Proof. Note that $f(t) = O(g(t))$ means that there exists a constant $M > 0$ such that

$$|f(t)| \leq Mg(t), \quad \text{for } t \geq a$$

This implies that

$$\int_a^x |f(t)|dt \leq M \int_a^x g(t)dt, \quad \text{for } x \geq a$$

That is,

$$\left|\int_a^x f(t)dt\right| \leq M \int_a^x g(x), \quad \text{for } x \geq a$$

That is

$$\int_a^x f(t)\, dt = O\left(\int_a^x g(t)\, dt\right).$$

□

Example 2. *Note that*

$$x = O(x^2), x^2 + 10x + 7 = O(x^2), x^n = O(e^x) \textit{ for all } n \in \mathbb{N}.$$

Theorem 1.2.1.

1. *If f_1 is $O(g_1)$ and f_2 is $O(g_2)$, then $(f_1 + f_2)$ is $O(\max\{g_1, g_2\})$.*
2. *If f_1 and f_2 are both $O(g)$, then $(f_1 + f_2)$ is $O(g)$.*
3. *If f_1 is $O(g_1)$ and f_2 is $O(g_2)$, then $(f_1 f_2)$ is $O(g_1 g_2)$.*
4. *If f_1 is $O(f_2)$ and f_2 is $O(f_3)$, then f_1 is $O(f_3)$.*

5. If f is $O(g)$, then (af) is $O(g)$ for any constant

Definition 1.2.2. *We say $f(x)$ is asymptotic to $g(x)$ as $x \to \infty$ if*

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$$

and write $f(x) \sim g(x)$, $x \to \infty$.

Here we need the following:

Definition 1.2.3. *Let f be an arithmetical function and x is any positive real number. Then $\sum_{n\leq x} f(n)$ is defined as:*

$$\sum_{n\leq x} f(n) = \sum_{n=1}^{[x]} f(n)$$

Definition 1.2.4. *Let f be an arithmetical function. Then the average of f is defined as*

$$f^{\sim}(n) := \frac{1}{n}\sum_{n\leq x} f(n)$$

Theorem 1.2.2. *(***Euler summation formula***) If f has a continuous derivative f' on the interval $[y, x]$, where $0 < y < x$, then*

$$\sum_{y<n\leq x} f(n) = \int_y^x f(t)dt + \int_y^x (t - [t])\, f'(t)dt + f(x)\,([x] - x) - f(y)\,([y] - y)\,.$$

Equivalently,

$$\sum_{y<n\leq x} f(n) = \int_y^x f(t)dt + \int_y^x \{t\}f'(t)dt + f(y)\{y\} - f(x)\{x\},$$

where $\{t\} = t - \{t\}$.

Let $m = [y]$ and $k = [x]$. If $n, n-1 \in [y, x]$, then:

$$\begin{aligned}
\int_m^k [t]f'(t)\,dt &= \sum_{n=m+1}^{k} \int_{n-1}^{n} [t]f'(t)\,dt \\
&= \sum_{m+1}^{k} \int_{n-1}^{n} (n-1)f'(t) \\
&= \sum_{m+1}^{k} (n-1)[f(n) - f(n-1)] \\
&= \sum_{m+1}^{k} ([nf(n) - (n-1)f(n-1)] - f(n))
\end{aligned}$$

$$\begin{aligned}
&= \sum_{m+1}^{k} ([nf(n) - (n-1)f(n-1)]) - \sum_{m+1}^{k} f(n) \\
&= kf(k) - mf(m) - \sum_{y<n\leq x} f(n)
\end{aligned}$$

$$\begin{aligned}
\sum_{y<n\leq x} f(n) &= -\int_m^k [t]f'(t)\,dt + kf(k) - mf(m) \\
&= -\int_y^x [t]f'(t)dt - \int_m^y [t]f'(t) + \int_k^x [t]f'(t)dt + kf(k) - mf(m) \\
&\qquad \left(\because \int_y^x = \int_y^k + \int_k^x = \int_m^k - \int_m^y + \int_k^x\right) \\
&= -\int_y^x [t]f'(t)dt - \int_m^y mf'(t) + \int_k^x kf'(t)dt + kf(k) - mf(m) \\
&= -\int_y^x [t]f'(t)dt - m[f(y) - f(m)] + k[f(x) - f(k)] + kf(k) - mf(m) \\
&= -\int_y^x [t]f'(t)dt - mf(y) + kf(x) \\
&= -\int_y^x [t]f'(t)dt - [y]f(y) + [x]f(x) \\
&= -\int_y^x [t]f'(t)dt + (y - [y])\,f(y) - (x - [x])\,f(x) + xf(x) - yf(y) \\
&= -\int_y^x [t]f'(t)dt + \{y\}f(y) - \{x\}f(x) + xf(x) - yf(y) \\
&= -\int_y^x [t]f'(t)dt + \{y\}f(y) - \{x\}f(x) + \int_y^x tf'(t)dt + \int_y^x f(t)dt \\
&= \int_y^x (t - [t])f'(t)dt + \{y\}f(y) - \{x\}f(x) + \int_y^x f(t)dt \\
&= \int_y^x \{t\}f'(t)dt + \int_y^x f(t)dt + \{y\}f(y) - \{x\}f(x).
\end{aligned}$$

$$\begin{aligned}
\int_y^x tf'(t)dt &= tf(t)]_y^x - \int_y^x f(t)dt \\
&= xf(x) - yf(y) - \int_y^x f(t)dt.
\end{aligned}$$

Definition 1.2.5. *The Euler's constant is defined by the equation*

$$C = \lim_{n\to\infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n\right).$$

Definition 1.2.6. *The Riemann zeta function is defined by the equation*

$$\zeta(s) = \begin{cases} \sum_{n=1}^{\infty} \frac{1}{n^s} & \text{if } s > 1 \\ \lim_{x\to\infty} \left(\sum_{n\leq x} \frac{1}{n^s} - \frac{x^{1-s}}{1-s} \right) & \text{if } 0 < s < 1. \end{cases}$$

Theorem 1.2.3. *If $x \geq 1$ we have*

(a) $\sum_{n\leq x} \frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right)$, *where C is Eulers constant.*

(b) $\sum_{n\leq x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(x^{-s})$ *if $s > 0$, $s \neq 1$.*

(c) $\sum_{n>x} \frac{1}{n^s} = O(x^{1-s})$ *if $s > 1$.*

(d) $\sum_{n\leq x} n^s = \frac{x^{\alpha+1}}{\alpha+1} + O(x^s)$ *if $\alpha \geq 0$.*

Proof. (a)By Euler's Summation formula, we have

$$\sum_{y<n\leq x} f(n) = \int_y^x f(t)dt + \int_y^x (t - [t])\, f'(t)dt + f(x)\,([x] - x) - f(y)\,([y] - y)\,. \tag{1.20}$$

Putting $y = 1$ and $f(t) = 1/t$ in the above formula, we obtain:

$$\sum_{1<n\leq x} \frac{1}{n} = \int_1^x \frac{1}{t}dt - \int_1^x (1 - [t])(-1/t^2)dt + (1/x)([x] - x)$$

That is

$$\sum_{1<n\leq x} \frac{1}{n} = \log x - \int_1^x \frac{t - [t]}{t^2}dt - \frac{x - [x]}{x}$$

Equivalently,

$$\sum_{1\leq n\leq x} \frac{1}{n} = \log x - \int_1^x \frac{t - [t]}{t^2}dt + 1 - \frac{x - [x]}{x} \tag{1.21}$$

Consider the functions

$$f(x) = -\frac{x - [x]}{x}, g(x) = \frac{1}{x}$$

Note that

$$\frac{|f(x)|}{g(x)} = x - [x] < 1.$$

Thus

$$f(x) = O(g(x)).$$

Hence equation (1.21) can be written as:

$$\begin{aligned}\sum_{1\leq n\leq x}\frac{1}{n} &= \log x - \int_1^x \frac{t-[t]}{t^2}dt + 1 + O\left(\frac{1}{x}\right)\\ &= \log x - \left[\int_1^\infty \frac{t-[t]}{t^2}dt - \int_x^\infty \frac{t-[t]}{t^2}dt\right] + 1 + O\left(\frac{1}{x}\right)\\ &= \log x - \int_1^\infty \frac{t-[t]}{t^2}dt + \int_x^\infty \frac{t-[t]}{t^2}dt + 1 + O\left(\frac{1}{x}\right) \qquad (1.22)\end{aligned}$$

Note that

$$0 \leq \int_1^\infty \frac{t-[t]}{t^2}dt < \int_1^\infty \frac{1}{t^2}dt = 1 < \infty$$

Thus

$$\int_1^\infty \frac{t-[t]}{t^2} < \infty.$$

Again note that

$$\frac{\frac{t-[t]}{t^2}}{\frac{1}{t^2}} = t-[t] < 1 \Rightarrow \frac{t-[t]}{t^2} = O\left(\frac{1}{t^2}\right) \Rightarrow \int_x^\infty \frac{t-[t]}{t^2}dt = O\left(\int_x^\infty \frac{1}{t^2}dt\right) = O\left(\frac{1}{x}\right)$$

Hence equation (1.22) can be written as:

$$\begin{aligned}\sum_{1\leq n\leq x}\frac{1}{n} &= \log x - \int_1^\infty \frac{t-[t]}{t^2}dt + \int_x^\infty \frac{t-[t]}{t^2}dt + 1 + O\left(\frac{1}{x}\right)\\ &= \log x + \underbrace{1 - \int_1^\infty \frac{t-[t]}{t^2}dt}_{B} + O\left(\frac{1}{x}\right) + O\left(\frac{1}{x}\right)\\ &= \log x + B + O\left(\frac{1}{x}\right) \qquad (1.23)\end{aligned}$$

Taking $x \to \infty$ in the above equation, we obtain:

$$\lim_{x\to\infty}\left[\sum_{1\leq n\leq x}\frac{1}{n} - \log x\right] = B$$

This implies that $B = C$. Hence equation (1.23) becomes:

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

(b) Putting $y = 1$ and $f(t) = t^{-s}$, $s > 0$, $s \neq 1$ in the Euler's summation formula, we obtain:

$$\sum_{1<n\leq x}\frac{1}{n^s} = \int_1^x \frac{1}{t^s}dt + \int_1^x (t-[t])(-st^{-s-1})dt - \frac{x-[x]}{x^s}$$

$$= \frac{x^{-s+1}}{1-s} - \frac{1}{1-s} - s\int_1^x \frac{t-[t]}{t^{s+1}}dt - \left(\frac{x-[x]}{x^s}\right)$$
$$= \frac{x^{-s+1}}{1-s} - \frac{1}{1-s} - s\int_1^x \frac{t-[t]}{t^{s+1}}dt + O\left(\frac{1}{x^s}\right)$$

Therefore,

$$\begin{aligned}\sum_{1\le n\le x}\frac{1}{n^s} &= \frac{x^{-s+1}}{1-s} + 1 - \frac{1}{1-s} - s\int_1^x \frac{t-[t]}{t^{s+1}}dt + O\left(\frac{1}{x^s}\right)\\ &= \frac{x^{1-s}}{1-s} - \frac{1}{1-s} + 1 - s\left[\int_1^\infty \frac{t-[t]}{t^{s+1}}dt - \int_x^\infty \frac{t-[t]}{t^{s+1}}dt\right] + O\left(\frac{1}{x^s}\right)\\ &= \frac{x^{1-s}}{1-s} - \frac{1}{1-s} + 1 - s\int_1^\infty \frac{t-[t]}{t^{s+1}}dt + O\left(\frac{1}{x^s}\right) + O\left(\frac{1}{x^s}\right)\\ &= \frac{x^{1-s}}{1-s} + \underbrace{\left[1 - \frac{1}{1-s} - s\int_1^\infty \frac{t-[t]}{t^{s+1}}dt\right]}_{B(s)} + O\left(\frac{1}{x^s}\right). \qquad (1.24)\end{aligned}$$

$$\begin{aligned}s\frac{t-[t]}{t^{s+1}} &= O\left(\frac{s}{t^{s+1}}\right)\\ \Rightarrow \int_x^\infty s\frac{t-[t]}{t^{s+1}}dt &= O\left(\int_x^\infty \frac{s}{t^{s+1}}dt\right)\\ &= O\left(\frac{1}{x^s}\right)\end{aligned}$$

Case 1: Suppose $s > 1$.

Letting $x \to \infty$ in the above equation, we obtain:

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

That is $\zeta(s) = B(s)$. Hence if $s > 1$, $\sum_{n\le x}\frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(x^{-s})$. Thus equation (2.31) becomes:

$$\sum_{n\le x}\frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(x^{-s}).$$

Case 2: Suppose $0 < s < 1$.

Letting $x \to \infty$ in equation (2.31), we obtain

$$\lim_{x\to\infty}\left[\sum_{n\le x}\frac{1}{n^s} - \frac{x^{1-s}}{1-s}\right] = B(s)$$

1.2.2 Partial sums of a Dirichlet product

Theorem 1.2.4. *If $h = f * g$, let*

$$H(x) = \sum_{n \le x} h(n), \qquad F(x) = \sum_{n \le x} f(n) \quad \text{and} \quad G(x) = \sum_{n \le x} g(n).$$

Then we have

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

Proof. Let

$$U(x) = \begin{cases} 0 & \text{if} \quad 0 < x < 1, \\ 1 & \text{if} \quad x \ge 1. \end{cases}$$

Claim 1: $F = f \circ U$.
Now

$$\begin{aligned} (f \circ U)(x) &= \sum_{n \le x} f(n) U\left(\frac{x}{n}\right) \\ &= \sum_{n \le x} f(n) \qquad \left(\because 0 < x \le n \Rightarrow \frac{x}{n} > 1 \Rightarrow U(x/n) = 1.\right) \\ &= F(x). \end{aligned}$$

Claim 2: $G = g \circ U$.
Now

$$\begin{aligned} (g \circ U)(x) &= \sum_{n \le x} g(n) U\left(\frac{x}{n}\right) \\ &= \sum_{n \le x} g(n) \qquad \left(\because 0 < x \le n \Rightarrow \frac{x}{n} > 1 \Rightarrow U(x/n) = 1.\right) \\ &= G(x). \end{aligned}$$

Claim 3: $h \circ U = H$.

$$\begin{aligned} (h \circ U)(x) &= \sum_{n \le x} h(n) U\left(\frac{x}{n}\right) \\ &= \sum_{n \le x} h(n) = H(x). \end{aligned}$$

Claim 4: $H = f \circ G$.
Now

$$f \circ G = f \circ (g \circ U) = (f * g) \circ U = h \circ U = H.$$

Claim 5: $H = g \circ F$.
Now

$$g \circ F = g \circ (f \circ U) = (g * f) \circ U = h \circ U = H.$$

This completes the proof. □

Theorem 1.2.5. *thm33 If $F(x) = \sum_{n\leq x} f(n)$ we have*

$$\sum_{n\leq x}\sum_{d|n} f(d) = \sum_{n\leq x} f(n)\left[\frac{x}{n}\right] = \sum_{n\leq x} F\left(\frac{x}{n}\right).$$

Proof. From the above theorem, we have

$$H = f \circ G, \quad \text{and}$$
$$H = g \circ F.$$

If $g = 1$, then we have:

$$G(x) = \sum_{n\leq x} 1 = [x].$$

Now

$$\begin{aligned} H(x) &= (f \circ G)(x) \\ &= \sum_{n\leq x} f(n) G\left(\frac{x}{n}\right) \\ &= \sum_{n\leq x} f(n)\left[\frac{x}{n}\right] \end{aligned} \tag{1.25}$$

Again

$$\begin{aligned} H(x) &= (g \circ F)(x) \\ &= \sum_{n\leq x} g(n) F\left(\frac{x}{n}\right) \\ &= \sum_{n\leq x} F\left(\frac{x}{n}\right) \end{aligned} \tag{1.26}$$

Also

$$\begin{aligned} H(x) &= \sum_{n\leq x} h(n) \\ &= \sum_{n\leq x} (f * g)(n) \\ &= \sum_{n\leq x}\sum_{d|n} f(n) g\left(\frac{x}{n}\right). \end{aligned} \tag{1.27}$$

From equations (1.25), (1.26) and (1.27), we have

$$\sum_{n\leq x}\sum_{d|n} f(d) = \sum_{n\leq x} f(n)\left[\frac{x}{n}\right] = \sum_{n\leq x} F\left(\frac{x}{n}\right).$$

This completes the proof. □

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

Theorem 1.2.6. *For $n \geq 1$ we have*

$$\sum_{n\leq x} \mu(n) \left[\frac{x}{n}\right] = 1$$

and

$$\sum_{n\leq x} \Lambda(n) \left[\frac{x}{n}\right] = \log[x]!.$$

Proof. Putting $f(n) = \mu(n)$ theorem we obtain:

$$\sum_{n\leq x} \mu(n) \left[\frac{x}{n}\right] = \sum_{n\leq x} \sum_{d|n} \mu(d) = \sum_{n\leq x} \left[\frac{1}{n}\right] = 1.$$

Again putting $f(n) = \Lambda(n)$ theorem we obtain:

$$\sum_{n\leq x} \Lambda(n) \left[\frac{x}{n}\right] = \sum_{n\leq x} \sum_{d|n} \Lambda(d) = \sum_{n\leq x} \log n = \log[x]!.$$

This completes the proof. □

Theorem 1.2.7. *For all $x \geq 1$ we have*

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

with equality holding only if $x < 2$.

Proof. Here we consider two cases:
Case1: Suppose $x < 2$.
In this case

$$\sum_{n\leq x} \frac{\mu(n)}{n} = \frac{\mu(1)}{1} = 1.$$

Note that in this case equality occurs.
Case 2: Suppose $x \geq 2$.
For each real number y, let

$$\{y\} := y - [y].$$

From theorem 1.2.3 we have:

$$\begin{aligned} 1 &= \sum_{n\leq x} \mu(n) \left[\frac{x}{n}\right] \\ &= \sum_{n\leq x} \mu(n) \left(\frac{x}{n} - \left\{\frac{x}{n}\right\}\right) \end{aligned}$$

$$= x \sum_{n \leq x} \frac{\mu(n)}{n} - \sum_{n \leq x} \mu(n) \left\{ \frac{x}{n} \right\}$$

This implies that

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

Therefore

$$\begin{aligned} x \left| \sum_{n \leq x} \frac{\mu(n)}{n} \right| &= \left| 1 + \sum_{n \leq x} \mu(n) \left\{ \frac{x}{n} \right\} \right| \\ &\leq 1 + \sum_{n \leq x} \left\{ \frac{x}{n} \right\} \\ &= 1 + \{x\} + \sum_{2 \leq n \leq x} \left\{ \frac{x}{n} \right\} \\ &< 1 + \{x\} + \sum_{2 \leq n \leq x} 1 \quad (\because 0 \leq \{y\} < 1) \\ &= 1 + \{x\} + [x] - 1 \quad \left(\because \sum_{n \leq x} 1 = [x] \right) \\ &= 1 + x - [x] + [x] - 1 = x. \end{aligned}$$

Dividing by x we obtain:

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

This completes the proof. □

Theorem 1.2.8 (Legendre's identity)**.** *For every $x \geq 1$ we have*

$$[x]! = \prod_{p \leq x} p^{\alpha(p)},$$

where the product is extended over all primes $\leq x$, and

$$\alpha(p) = \sum_{m=1}^{\infty} \left[\frac{x}{p^m} \right]$$

Proof. We have

$$\sum_{n \leq x} \Lambda(n) \left[\frac{x}{n} \right] = \log[x]! \quad \text{(see theorem 1.2.3)}$$

Putting $n = p^m$ in the above equation, we obtain:

$$\begin{aligned}
\log[x]! &= \sum_{p^m \leq x} \Lambda(p^m) \left[\frac{x}{p^m}\right] \\
&= \sum_{2,2^2,\ldots 2^m \leq x} \Lambda(2^m) \left[\frac{x}{2^m}\right] + \sum_{3,3^2,\ldots 3^m \leq x} \Lambda(3^m) \left[\frac{x}{3^m}\right] + \cdots \\
&= \sum_{p \leq x} \left(\sum_{\substack{m=1 \\ p^m \leq x}}^{\infty} \Lambda(p^m) \left[\frac{x}{p^m}\right] \right) \\
&= \sum_{p \leq x} \left(\sum_{\substack{m=1 \\ p^m \leq x}}^{\infty} \log p \left[\frac{x}{p^m}\right] \right) \\
&= \sum_{p \leq x} \log p \left(\sum_{\substack{m=1 \\ p^m \leq x}}^{\infty} \left[\frac{x}{p^m}\right] \right) \\
&= \sum_{p \leq x} \alpha(p) \log p, \qquad \alpha(p) = \sum_{\substack{m=1 \\ p^m \leq x}}^{\infty} \left[\frac{x}{p^m}\right] \\
&= \sum_{p \leq x} \log p^{\alpha(p)} \\
&= \log \left(\prod_{p \leq x} p^{\alpha(p)} \right)
\end{aligned}$$

Hence $[x]! = \prod_{p \leq x} p^{\alpha(p)}$. This completes the proof. □

Theorem 1.2.9. *If $x \geq 2$ we have*

$$\log[x]! = x \log x - x + O(\log x),$$

and hence

$$\sum_{n \leq x} \Lambda(n) \left[\frac{x}{n}\right] = x \log x - x + O(logx).$$

Proof. Putting $f(t) = \log t$ in Euler's summation formula with $y = 1$ we obtain:

$$\begin{aligned}
\sum_{1 < n \leq x} \log n &= \int_1^x \log t dt + \int_1^x (t - [t]) \frac{1}{t} dt + \log x([x] - x) - 0 \\
&= x \log x - x + 1 + O\left(\int_1^x \frac{1}{t} dt \right) + O(\log x) \qquad (1.28)
\end{aligned}$$

Note that

$$\frac{t-[t]1/t}{1/t} = t - [t] < 1 \Rightarrow (t-[t])1/t = O(1/t)$$

Therefore

$$\int_1^x \frac{t-[t]1/t}{1/t} dt = O\left(\int_1^x \frac{1}{t} dt\right)$$

Also

$$\left|\frac{\log x([x]-x)}{\log x}\right| = |[x]-x| < 1 \Rightarrow \log x([x]-x) = O(\log x)$$

Adding 1 on both sides of equation (1.28) we obtain:

$$\begin{aligned}\sum_{n\leq x} \log n &= x\log x - x + 2 + O(\log x) + O(\log x)\\ &= x\log x - x + O(\log x)\end{aligned}$$

That is

$$\log[x]! = x\log x - x + O(\log x).$$

From the light of theorem 1.2.3 it follows that

$$\sum_{n\leq x} \Lambda(n)\left[\frac{x}{n}\right] = x\log x - x + O(\log x)..$$

This completes the proof. □

Theorem 1.2.10. *For $x \geq 2$ we have*

$$\sum_{p\leq x}\left[\frac{x}{p}\right]\log p = x\log x + O(x),$$

where the sum is extended over all primes $\leq x$.

Proof. We have

$$\log[x]! = \sum_{n\leq x}\Lambda(n)\left[\frac{x}{n}\right].$$

Therefore,

$$\begin{aligned}\log[x]! &= \sum_{p^m\leq x}\Lambda(p^m)\left[\frac{x}{p^m}\right]\\ &= \sum_{2,2^2,\ldots 2^m\leq x}\Lambda(2^m)\left[\frac{x}{2^m}\right] + \sum_{3,3^2,\ldots 3^m\leq x}\Lambda(3^m)\left[\frac{x}{3^m}\right] + \cdots\end{aligned}$$

$$
\begin{aligned}
&= \sum_{p\le x}\left(\sum_{\substack{m=1\\ p^m\le x}}^{\infty}\Lambda(p^m)\left[\frac{x}{p^m}\right]\right)\\
&= \sum_{p\le x}\left(\sum_{\substack{m=1\\ p^m\le x}}^{\infty}\log p\left[\frac{x}{p^m}\right]\right)\\
&= \sum_{p\le x}\log p\left(\sum_{\substack{m=1\\ p^m\le x}}^{\infty}\left[\frac{x}{p^m}\right]\right)\\
&= \sum_{p\le x}\Lambda(p)\left[\frac{x}{p}\right]+\sum_{p\le x}\sum_{m=2}^{\infty}\Lambda(p^m)\left[\frac{x}{p^m}\right]\\
&= \sum_{p\le x}\Lambda(p)\left[\frac{x}{p}\right]+\sum_{p\le x}\sum_{m=2}^{\infty}\log p\left[\frac{x}{p^m}\right].
\end{aligned}
$$

Therefore

$$
\begin{aligned}
\sum_{p\le x}\Lambda(p)\left[\frac{x}{p}\right] &= \log[x]! - \sum_{p\le x}\sum_{m=2}^{\infty}\log p\left[\frac{x}{p^m}\right]\\
&= x\log x - x + O(\log x) - \sum_{p\le x}\sum_{m=2}^{\infty}\log p\left[\frac{x}{p^m}\right] \quad \text{(by theorem 1.2.9)}
\end{aligned}
\tag{1.29}
$$

Claim : $\sum_{p\le x}\sum_{m=2}^{\infty}\log p\left[\frac{x}{p^m}\right] = O(x)$.

$$
\begin{aligned}
\sum_{p\le x}\sum_{m=2}^{\infty}\log p\left[\frac{x}{p^m}\right] &\le \sum_{p\le x}\sum_{m=2}^{\infty}\log p\frac{x}{p^m}\\
&= \sum_{p\le x}\log p\sum_{m=2}^{\infty}\frac{x}{p^m}\\
&= x\sum_{p\le x}\sum_{m=2}^{\infty}\log p\frac{1}{p^m}\\
&= x\sum_{p\le x}\log p\left[\frac{1}{p^2}+\frac{1}{p^3}+\cdots\right]\\
&= x\sum_{p\le x}\log p\frac{1}{p^2}\left[1+\frac{1}{p}+\cdots\right]\\
&= x\sum_{p\le x}\log p\frac{1}{p^2}\left[\frac{1}{1-1/p}\right]
\end{aligned}
$$

$$= x \sum_{p \leq x} \log p \frac{1}{p^2} \frac{p}{p-1}$$
$$\leq x \underbrace{\sum_{n \leq x} \frac{\log n}{n(n-1)}}_{< \infty}$$

This implies that

$$\sum_{p \leq x} \sum_{m=2}^{\infty} \log p \left[\frac{x}{p^m} \right] = O(x).$$

Hence equation (1.29) can be written as:

$$\sum_{p \leq x} \Lambda(p) \left[\frac{x}{p} \right] = x \log x - x + O(\log x) - O(x)$$
$$= x \log x + O(x).$$

This completes the proof. □

1.2.4 Another identity for the partial sums of a Dirichlet product

Theorem 1.2.11. *If a and b are positive real numbers such that $ab = x$, then*

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

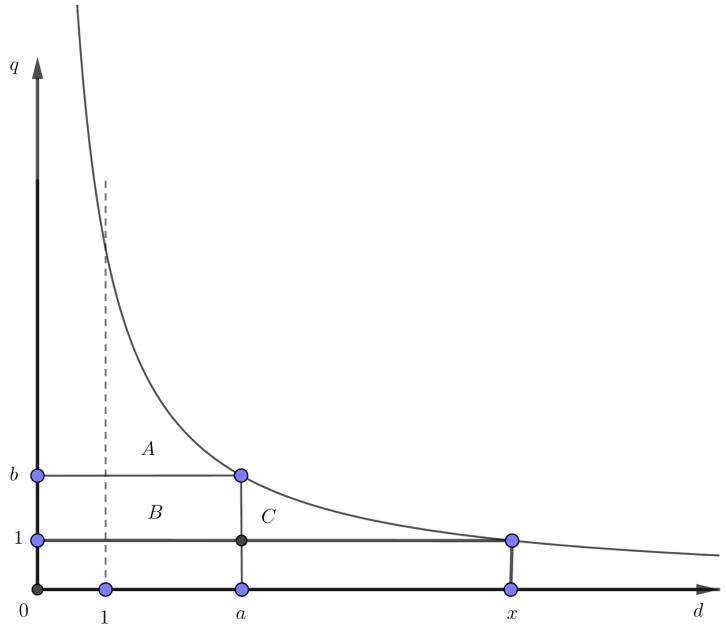
Proof. Let

$$F(x) = \sum_{n \leq x} f(n),$$
$$G(x) = \sum_{n \leq x} g(n) \text{ and}$$
$$H(x) = \sum_{n \leq x} h(x), \quad h = f * g. \tag{1.30}$$

Then

$$H(x) = \sum_{n \leq x} \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$
$$= \sum_{\substack{q,d \\ qd \leq x}} f(d)g(q). \tag{1.31}$$

Since a and b are positive real numbers such that $ab = x$ it follows that (a, b) is a point on the rectangular hyperbola $qd = x$.



The sum $H(x)$ in equation (1.31) is extended over all lattice points in the first quadrant of (q, d)- plane, below the rectangular hyperbola $qd = x$ between the two lines $q = 1$ and $d = 1$. Let

$$\begin{aligned} D &= \{(d, q) : q \geq 1, d \geq 1, qd \leq x\} \\ A &= \{(d, q) : d \geq 1, q > b, qd \leq x\} \\ B &= \{(d, q) : q \in [1, a], d \in [1, b]\} \\ C &= \{(d, q) : d > a, q \geq 1, qd \leq x\}. \end{aligned}$$

Then

$$D = A \cup B \cup C.$$

Now

$$\begin{aligned} \sum_{(d,q)\in A\cup B} &= \sum_{d\leq a} \sum_{q\leq x/d} f(d)g(q) \\ &= \sum_{d\leq a} f(d) \sum_{q\leq x/d} g(q) \\ &= \sum_{d\leq a} f(d)G\left(\frac{x}{d}\right) \end{aligned}$$

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

$$\begin{aligned}
\sum_{(d,q) \in B \cup C} f(d)g(q) &= \sum_{q \le b} \sum_{d \le x/q} f(d)g(q) \\
&= \sum_{q \le b} g(q) \sum_{d \le x/q} f(d) \\
&= \sum_{q \le b} g(q) F\left(\frac{x}{q}\right) \\
&= \sum_{n \le b} g(n) F\left(\frac{x}{n}\right).
\end{aligned}$$

$$\begin{aligned}
\sum_{(d,q) \in B} &= \sum_{d \le a} \sum_{q \le b} f(d)g(q) \\
&= \sum_{d \le a} f(d) \sum_{q \le b} g(q) \\
&= F(a)G(b).
\end{aligned}$$

Hence

$$\begin{aligned}
\sum_{\substack{d,q \\ qd \le x}} f(d)g(q) &= \sum_{(d,q) \in D} f(d)g(q) \\
&= \sum_{(d,q) \in A \cup B} f(d)g(q) + \sum_{(d,q) \in B \cup C} - \sum_{(d,q) \in B} \\
&= \sum_{n \le a} f(n) G\left(\frac{x}{n}\right) + \sum_{n \le b} g(n) F\left(\frac{x}{n}\right) - F(a)G(b).
\end{aligned}$$

□

1.2.5 Exercises

1. Use Euler's summation formula to deduce the following for $x \ge 2$:
   (a) $\sum_{n \le x} \frac{\log n}{n} = \frac{1}{2} \log^2 x + A + O\left(\frac{\log x}{x}\right)$, where A is constant.
   (b) $\sum_{2 \le n \le x} \frac{1}{n \log n} = \log(\log x) + B + O\left(\frac{1}{x \log x}\right)$, where B is a constant.
   (a) Prove that $[2x] - [x]$ is either 0 or 1.

Module 2

Some elementary theorems on distribution of prime numbers

2.1 Chebyshev's functions $\psi(x)$ and $\vartheta(x)$

Definition 2.1.1. *For $x > 0$ the Chebyshev's ψ-function is defined as*

$$\psi(x) = \sum_{n \leq x} \Lambda(n).$$

Recall the Mangoldt Λ function:

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

Using this function we can write the definition of ψ as follows:

$$\begin{aligned} \psi(x) &= \sum_{n \leq x} \Lambda(n) \\ &= \sum_{p \leq x} \sum_{\substack{m=1 \\ p^m \leq x}}^{\infty} \Lambda(p^m) \\ &= \sum_{\substack{m=1 \\ p^m \leq x}}^{\infty} \sum_{p} \Lambda(p^m) \\ &= \sum_{m=1}^{\infty} \sum_{p \leq x^{1/m}} \log p \end{aligned} \tag{2.1}$$

Note that the sum in (2.1) is a finite sum. For, if $x^{1/m} < 2$ then $\sum_{p \le x^{1/m}} \log p = 0$ (that is the summation is empty). Now

$$x^{1/m} < 2 \Rightarrow \frac{1}{m} \log x < \log 2 \Rightarrow m > \frac{\log x}{log2} = \log_2 x.$$

Hence if $m > \log_2 x$, the sum in (2.1) is zero. Hence $\psi(x)$ can be written as:

$$\psi(x) = \sum_{m \le \log_2 x} \sum_{p \le x^{1/m}} \log p.$$

Definition 2.1.2. *If $x > 0$ the Chebyshev's ϑ function is defined as*

$$\vartheta(x) = \sum_{p \le x} \log p,$$

where p runs over all primes $\le x$.

Using Chebyshev's ϑ function, we can write Chebyshev's ψ function as follows:

$$\psi(x) = \sum_{m \le \log_2 x} \vartheta\left(x^{1/m}\right).$$

Theorem 2.1.1. *For $x > 0$ we have*

$$0 \le \frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \le \frac{(\log x)^2}{2\sqrt{x} \log 2}.$$

Proof. Note that

$$\begin{aligned}
\psi(x) - \vartheta(x) &= \sum_{m \le \log_2 x} \sum_{p \le x^{1/m}} \log p - \sum_{p \le x} \log p \\
&= \sum_{2 \le m \le \log_2 x} \log p + \sum_{p \le x} \log p - \sum_{p \le x} \log p \\
&= \sum_{2 \le m \le \log_2 x} \sum_{p \le x^{1/m}} \log p \ge 0.
\end{aligned}$$

Hence

$$\begin{aligned}
0 \le \psi(x) - \vartheta(x) &= \sum_{2 \le m \le \log_2 x} \sum_{p \le x^{1/m}} \log p \\
&= \sum_{2 \le m \le \log_2 x} \vartheta(x^{1/m}) \qquad (2.2)
\end{aligned}$$

We have

$$\vartheta(x) = \sum_{p \le x} \log p$$

$$\begin{aligned} &< \sum_{p \le x} \log x \\ &< x \log x. \end{aligned}$$

Therefore

$$\vartheta(x^{1/m}) < x^{1/m} \log x^{1/m}$$

Hence (2.2) can be written as

$$\begin{aligned} 0 \le \psi(x) - \vartheta(x) &< \sum_{2 \le m \le \log_2 x} x^{1/m} \log(x^{1/m}) \\ &= x^{1/2} \log x^{1/2} + x^{1/3} \log x^{1/3} + \cdots + x^{1/\log_2 x} \log \left(x^{1/\log_2 x} \right) \\ &= \frac{1}{2} x^{1/2} \log x + \frac{1}{3} x^{1/3} \log x + \cdots + \frac{x^{1/\log_2 x}}{\log_2 x} \log x \\ &\le \frac{1}{2} x^{1/2} \log x + \frac{1}{3} x^{1/2} \log x + \cdots + \frac{1}{\log_2 x} x^{1/2} \log x \quad (\because \log \text{ is increasing}) \\ &\le \frac{1}{2} x^{1/2} \log x + \frac{1}{2} x^{1/2} \log x + \cdots + \frac{1}{2} x^{1/2} \log x \\ &\le \frac{1}{2} x^{1/2} \log x \log_2 x = \frac{1}{2} x^{1/2} \log x \log x \frac{1}{\log 2} \\ &= \frac{\sqrt{x}}{2} \frac{(\log x)^2}{\log 2} \end{aligned}$$

Dividing by x we obtain:

$$0 \le \frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \le \frac{(\log x)^2}{2\sqrt{x} \log 2}$$

This completes the proof. □

Corollary 3. *We have*

$$\lim_{n \to \infty} \left(\frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \right) = 0.$$

Proof. We have

$$0 \le \frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \le \frac{(\log x)^2}{2\sqrt{x} \log 2}$$

To prove the result it suffices to show that

$$\lim_{x \to \infty} \frac{(\log x)^2}{2\sqrt{x} \log 2} = 0.$$

By L Hospital rule we have

$$\lim_{n \to \infty} \frac{(\log x)^2}{2\sqrt{x} \log 2} = \lim_{n \to \infty} \frac{2(\log x) \frac{1}{x}}{2 \frac{1}{2\sqrt{x}} \log 2}$$

$$= \lim_{n\to\infty} \frac{2(\log x)}{\sqrt{x}\log 2} = \lim_{n\to\infty} \frac{2(\frac{1}{x})}{\frac{1}{2\sqrt{x}}\log 2} = \lim_{n\to\infty} \frac{4}{\sqrt{x}\log 2} = 0.$$

This completes the proof of the theorem. □

2.2 Relations connecting $\vartheta(x)$ and $\pi(x)$

Theorem 2.2.1 (Abel's identity)**.** *For any arithmetical function $a(n)$ let*

$$A(x) = \sum_{n\leq x} a(n),$$

where $A(x) = 0$ if $x < 1$. Assume that f has a continuous derivative on the interval $[y, x]$, where $0 < y < x$. Then we have

$$\sum_{y<n\leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$$

Proof. Let $k = [x]$ and $m = [y]$. Then

$$\begin{aligned} A(x) &= \sum_{n\leq x} a(n) \\ &= \sum_{n=1}^{[x]} a(n) = \sum_{n=1}^{k} a(n) = A(k). \end{aligned}$$

Similarly $A(y) = A(m)$. Now

$$\begin{aligned} \sum_{y<n\leq x} a(n)f(n) &= \sum_{n=[y]+1}^{[x]} a(n)f(n) \\ &= \sum_{n=m+1}^{k} a(n)f(n) \\ &= \sum_{n=m+1}^{k} [A(n) - A(n-1)]f(n) \\ &= \sum_{n=m+1}^{k} A(n)f(n) - \sum_{n=m+1}^{k} A(n-1)f(n) \\ &= \sum_{n=m+1}^{k} A(n)f(n) - \sum_{n=m}^{k-1} A(n)f(n+1) \\ &= \sum_{n=m+1}^{k-1} A(n)f(n) + A(k)f(k) - \sum_{n=m}^{k-1} A(n)f(n+1) \end{aligned}$$

$$= \sum_{n=m+1}^{k-1} A(n)f(n) + A(k)f(k) - A(m)f(m+1) - \sum_{n=m+1}^{k-1} A(n)f(n+1)$$
$$= \sum_{n=m+1}^{k-1} A(n)[f(n) - f(n+1)] + A(k)f(k) - A(m)f(m+1)$$
$$= -\sum_{n=m+1}^{k-1} A(n)\int_n^{n+1} f'(t)dt + A(k)f(k) - A(m)f(m+1)$$

Note that if $t \in [n, n+1]$,we have

$$A(t) = \sum_{n \le t} a(n) = \sum_{i=1}^{n} a(i) = A(n)$$

. Therefore the above equation can be written as:

$$\sum_{y<n\le x} a(n)f(n) = -\sum_{n=m+1}^{k-1}\int_n^{n+1} A(t)f'(t)dt + A(k)f(k) - A(m)f(m+1)$$
$$= -\int_{m+1}^{k} A(t)f'(t) + A(k)f(k) - A(m)f(m+1) \tag{2.3}$$

Now

$$\int_y^{m+1} A(t)f'(t) = \int_y^{m+1} A(m)f'(t)dt$$
$$= A(m)[f(m+1) - f(y)]$$
$$= A(m)f(m+1) - A(m)f(y)$$
$$= A(m)f(m+1) - A(y)f(y)$$

Therefore

$$A(m)f(m+1) = A(y)f(y) + \int_y^{m+1} A(t)f'(t)dt \tag{2.4}$$

Again

$$\int_k^x A(t)f'(t) = \int_k^x A(k)f'(t)dt$$
$$= A(k)[f(x) - f(k)]$$
$$= A(k)f(x) - A(k)f(k)$$
$$= A(x)f(x) - A(k)f(k)$$

Therefore

$$A(k)f(k) = -\int_k^x A(t)f'(t)dt + A(x)f(x) \tag{2.5}$$

Putting the values $A(m)f(m+1)$ and $A(k)f(k)$ in equation (2.3), we obtain:

$$\begin{aligned}\sum_{y<n\leq x} a(n)f(n) &= -\int_{m+1}^{k} A(t)f'(t)dt - \int_{k}^{x} A(t)f'(t)dt + A(x)f(x) - A(y)f(y)\\ &\quad - \int_{y}^{m+1} A(t)f'(t)dt\\ &= -\left[\int_{y}^{m+1} A(t)f'(t)dt + \int_{m+1}^{k} A(t)f'(t)dt + \int_{k}^{x} A(t)f'(t)dt\right]\\ &\quad + A(x)f(x) - A(y)f(y)\\ &= -\int_{y}^{x} A(t)f'(t)dt + A(x)f(x) - A(y)f(y).\end{aligned}$$

This completes the proof of the theorem. □

Corollary 4. *(Euler summation formula) If f has a continuous derivative f' on the interval $[y,x]$, where $0<y<x$, then*

$$\sum_{y<n\leq x} f(n) = \int_{y}^{x} f(t)dt + \int_{y}^{x} (t-[t])f'(t)dt + f(x)([x]-x) - f(y)([y]-y).$$

Proof. Note that when $a(n)=1$ for all $n\in\mathbb{N}$, then

$$A(x) = \sum_{n\leq xx} a(n) = \sum_{n\leq x} 1 = [x].$$

Puttting $a(n)=1$ for all $n\in\mathbb{N}$ in the Abel's formula we obtain:

$$\begin{aligned}\sum_{y<n\leq x} f(n) &= [x]f(x) - [y]f(y) - \int_{y}^{x} [t]f'(t)dt\\ &= [x]f(x) - [y]f(y) - \int_{y}^{x} ([t]-t)f'(t)dt - \int_{y}^{x} tf'(t)dt\\ &= [x]f(x) - [y]f(y) - \int_{y}^{x} ([t]-t)f'(t)dt - [tf(t)]_{y}^{x} - \int_{y}^{x} f(t)dt\\ &= [x]f(x) - [y]f(y) - \int_{y}^{x} ([t]-t)f'(t)dt - xf(x) + yf(y) + \int_{y}^{x} f(t)dt\\ &= \int_{y}^{x} f(t)dt + ([x]-x)f(x) - ([y]-y)f(y) + \int_{y}^{x} (t-[t])f'(t)dt.\end{aligned}$$

□

Alternate proof of Abel's Identity

Note that every finite sum can be written as a Riemann Stieltjes integral. That is,

$$\sum_{y<n\leq x} a(n)f(n) = \int_{y}^{x} f(t)dA(t)$$

Integration by parts gives us:

$$\begin{aligned}\sum_{y<n\leq x} a(n)f(n) &= [f(t)A(t)]_y^x - \int_y^x f'(t)A(t)dt \\ &= f(x)A(x) - f(y)A(y) - \int_y^x f'(t)A(t)dt.\end{aligned}$$

Theorem 2.2.2. *For $x \geq 2$ we have*

$$\vartheta(x) = \pi(x)\log x - \int_2^x \frac{\pi(t)}{t}dt \tag{2.6}$$

$$\pi(x) = \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t\log^2 t}dt \tag{2.7}$$

Proof. Define an arithmetical function $a(n)$ by

$$a(n) = \begin{cases} 1 & \text{if } n \text{ is a prime} \\ 0 & \text{otherwise.} \end{cases}$$

Then we have

$$\begin{aligned}\pi(x) &= \sum_{p\leq x} 1 \\ &= \sum_{n\leq x} a(n) = A(x).\end{aligned}$$

and

$$\vartheta(x) = \sum_{p\leq x} \log p = \sum_{n\leq x} a(n)\log n$$

We have

$$\sum_{y<n\leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$$

Putting $f(t) = \log t$ and $y = 1$ in the above equation, we obtain:

$$\sum_{1<n\leq x} a(n)\log n = A(x)\log x - A(1)\log 1 - \int_1^x A(t)\frac{1}{t}dt.$$

This implies that

$$\vartheta(x) = \pi(x)\log x - \int_1^x \frac{\pi(t)}{t}dt$$

$$= \pi(x)\log x - \int_1^2 \frac{\pi(t)}{t}dt - \int_2^x \frac{\pi(t)}{t}dt$$
$$= \pi(x)\log x - \int_2^x \frac{\pi(t)}{t}dt \,(\pi(t) = 0 \text{ if } t < 2)$$

Let $b(n) = a(n)\log n$. Then

$$B(x) = \sum_{n\leq x} b(n) = \sum_{n\leq x} a(n)\log n$$

Therefore we have

$$\vartheta(x) = \sum_{p\leq x} \log p$$
$$= \sum_{n\leq x} a(n)\log n = B(x)$$

and

$$\pi(x) = \sum_{n\leq x} a(n) = \sum_{n\leq x} \frac{b(n)}{\log n}$$

Putting $f(t) = \frac{1}{\log t}$ and $y = 3/2$ in the Abel's identity, we obtain:

$$\sum_{3/2<n\leq x} \frac{b(n)}{\log n} = B(x)\frac{1}{\log x} - B(3/2)\frac{1}{\log(3/2)} - \int_{3/2}^x B(t)\left(\frac{-1}{(\log t)^2}\right)dt.$$

This implies that

$$\pi(x) = \frac{\vartheta(x)}{\log x} - \frac{\vartheta(3/2)}{\log(3/2)} + \int_{3/2}^x \frac{\vartheta(t)}{t\log^2 t}dt.$$
$$= \frac{\vartheta(x)}{\log x} + \int_{3/2}^2 \frac{\vartheta(t)}{t\log^2 t}dt + \int_2^x \frac{\vartheta(t)}{t\log^2 t}dt$$
$$= \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t\log^2 t}dt.$$

□

2.3 Some equivalent forms of the prime number theorem

Theorem 2.3.1. *The following relations are logically equivalent*

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

$$\lim_{x\to\infty}\frac{\vartheta(x)}{x}=1. \tag{2}$$

$$\lim_{x\to\infty}\frac{\psi(x)}{x}=1. \tag{3}$$

Proof. (1) $\Rightarrow$ (2):
Assume that

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

We want to show that

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

From theorem 2.2.2, we have

$$\vartheta(x)=\pi(x)\log x-\int_2^x\frac{\pi(t)}{t}dt \tag{2.8}$$

The above equation can be written as:

$$\frac{\vartheta(x)}{x}=\frac{\pi(x)\log x}{x}-\frac{1}{x}\int_2^x\frac{\pi(t)}{t}dt$$

Therefore, we have

$$\begin{aligned}\lim_{x\to\infty}\frac{\vartheta(x)}{x}&=\lim_{x\to\infty}\frac{\pi(x)\log x}{x}-\lim_{x\to\infty}\frac{1}{x}\int_2^x\frac{\pi(t)}{t}dt\\&=1-\lim_{x\to\infty}\frac{1}{x}\int_2^x\frac{\pi(t)}{t}dt\end{aligned} \tag{2.9}$$

To prove that (1) $\Rightarrow$ (2), we need only show that

$$\lim_{x\to\infty}\frac{1}{x}\int_2^x\frac{\pi(t)}{t}dt=0.$$

Note that

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

The above limit can be written as:

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

This implies that

$$\frac{\pi(t)}{t}=O\left(\frac{1}{\log t}\right)$$

This implies that

$$\frac{1}{x}\int_2^{\infty}\frac{\pi(t)}{t}dt = O\left(\frac{1}{x}\int_2^{\infty}\frac{1}{\log t}dt\right)$$

This implies that there exists a constant $M > 0$ such that

$$\frac{1}{x}\int_2^{\infty}\frac{\pi(t)}{t}dt \leq M\left(\frac{1}{x}\int_2^{\infty}\frac{1}{\log t}dt\right) \tag{2.10}$$

Now,

$$\begin{aligned}\int_2^x \frac{1}{\log t}dt &= \int_2^{\sqrt{x}}\frac{1}{\log t}dt + \int_{\sqrt{x}}^x \frac{1}{\log t}dt\\ &\leq \int_2^{\sqrt{x}}\frac{1}{\log 2}dt + \int_{\sqrt{x}}^x \frac{1}{\log x}dt\\ &\leq \frac{1}{\log 2}(\sqrt{x}-2) + \frac{1}{\log\sqrt{x}}(x-\sqrt{x})\\ &\leq \frac{1}{\log 2}\sqrt{x} + \frac{1}{\log\sqrt{x}}(x-\sqrt{x})\end{aligned}$$

Therefore, we have

$$0 \leq \frac{1}{x}\int_2^x \frac{1}{\log t}dt \leq \frac{1}{\sqrt{x}\log 2} + \frac{1}{x\log\sqrt{x}}(x-\sqrt{x})$$

This implies that

$$\lim_{x\to\infty}\frac{1}{x}\int_2^x\frac{1}{\log t}dt = 0.$$

In the light of equation (2.10), we have

$$\lim_{x\to\infty}\frac{1}{x}\int_2^x\frac{\pi(t)}{t}dt = 0.$$

This completes the proof of (1) $\Rightarrow$ (2).
(2) $\Rightarrow$ (1):
Assume that $\lim_{x\to\infty}\frac{\vartheta(x)}{x} = 1$. To prove that

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

From theorem 2.2.2, we have

$$\pi(x) = \frac{\vartheta(x)}{\log x} + \int_2^x \frac{\vartheta(t)}{t\log^2 t}dt$$

The above equation can be written as:

$$\frac{\pi(x)\log x}{x} = \frac{\theta(x)}{x} + \frac{\log x}{x}\int_2^x \frac{\vartheta(t)}{t\log^2 t}dt$$

Therefore

$$\begin{aligned}\lim_{x\to\infty}\frac{\pi(x)\log x}{x} &= \lim_{x\to\infty}\frac{\theta(x)}{x} + \lim_{x\to\infty}\frac{\log x}{x}\int_2^x \frac{\vartheta(t)}{t\log^2 t}dt \\ &= 1 + \lim_{x\to\infty}\frac{\log x}{x}\int_2^x \frac{\vartheta(t)}{t\log^2 t}dt\end{aligned}$$

To prove the result, we need only show that

$$\lim_{x\to\infty}\frac{\log x}{x}\int_2^x \frac{\vartheta(t)}{t\log^2 t}dt = 0.$$

By hypothesis,

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

This implies that

$$\theta(t) = O(t).$$

Therefore

$$\frac{\log x}{x}\int_2^x \frac{\vartheta(t)}{t\log^2 t}dt = O\left(\frac{\log x}{x}\int_2^x \frac{\vartheta(t)dt}{\log^2 t}\right) \tag{2.11}$$

Now

$$\begin{aligned}\int_2^x \frac{\vartheta(t)dt}{\log^2 t} &= \int_2^{\sqrt{x}} \frac{1}{\log^2 t}dt + \int_{\sqrt{x}}^x \frac{1}{\log^2 t}dt \\ &\le \int_2^{\sqrt{x}} \frac{1}{\log^2 2}dt + \int_{\sqrt{x}}^x \frac{1}{\log^2\sqrt{x}}dt \\ &= \frac{1}{\log^2 2}[\sqrt{x}-2] + \frac{1}{\log^2\sqrt{x}}(x-\sqrt{x}) \\ &\le \frac{\sqrt{x}}{\log^2 2} + \frac{4}{\log^2 x}(x-\sqrt{x})\end{aligned}$$

Therefore

$$\begin{aligned}\frac{\log x}{x}\int_2^x \frac{\vartheta(t)dt}{\log^2 t} &\le \frac{\log x}{x}\frac{\sqrt{x}}{\log^2 2} + \frac{\log x}{x}\frac{4}{\log^2 x}(x-\sqrt{x}) \\ &= \frac{1}{\log^2 2}\frac{\log x}{\sqrt{x}} + \frac{4(x-\sqrt{x})}{x\log x}\end{aligned}$$

This implies that

$$\lim_{x\to\infty}\frac{\log x}{x}\int_2^x\frac{\vartheta(t)}{t\log^2 t}dt=0 \quad \left(\because \lim\frac{\log x}{x}=0, \lim\frac{(x-\sqrt{x})}{x\log x}=0\right)$$

This completes the proof of (2) $\Rightarrow$ (1).
(2) $\Rightarrow$ (3).
Assume that $\lim_{x\to\infty}\frac{\vartheta(x)}{x}=1$. We want to show that $\lim_{x\to\infty}\frac{\psi(x)}{x}=0$. By corollary 3, we have

$$\lim_{n\to\infty}\left(\frac{\psi(x)}{x}-\frac{\vartheta(x)}{x}\right)=0.$$

This implies that $\lim_{x\to\infty}\frac{\psi(x)}{x}=0$.
(3) $\Rightarrow$ (1).
Assume that $\lim_{x\to\infty}\frac{\psi(x)}{x}=0$. We want to prove that $\lim_{x\to\infty}\frac{\vartheta(x)}{x}=0$. By corollary 3, we have

$$\lim_{n\to\infty}\left(\frac{\psi(x)}{x}-\frac{\vartheta(x)}{x}\right)=0.$$

This implies that $\lim_{x\to\infty}\frac{\vartheta(x)}{x}=0$.

□

Theorem 2.3.2. *Let p_n denote the n th prime. Then the following asymptotic relations are logically equivalent:*

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

$$\lim_{x\to\infty}\frac{\pi(x)\log\pi(x)}{x}=1. \tag{2}$$

$$\lim_{n\to\infty}\frac{p_n}{n\log n}=1. \tag{2}$$

Proof. (1) $\Rightarrow$ (2):
Asuume that (1) holds. That is

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

Taking logarithms we obatin:

$$\lim_{x\to\infty}[\log\pi(x)+\log\log x-\log x]=0.$$

This implies that

$$\lim_{x\to\infty}\log x\left[\frac{\log\pi(x)}{\log x}+\frac{\log\log x}{\log x}-1\right]=0.$$

This implies that

$$\lim_{x\to\infty}\left[\frac{\frac{\log\pi(x)}{\log x}+\frac{\log\log x}{\log x}-1}{1/\log x}\right]=0.$$

This implies that

$$\frac{\log \pi(x)}{\log x} + \frac{\log \log x}{\log x} - 1 = O(1/\log x)$$

This implies that there exists a constant $M > 0$ such that

$$\frac{\log \pi(x)}{\log x} + \frac{\log \log x}{\log x} - 1 \leq M \left(\frac{1}{\log x}\right).$$

This implies that

$$\lim_{x\to\infty} \left[\frac{\log \pi(x)}{\log x} + \frac{\log \log x}{\log x} - 1\right] = 0.$$

This implies that

$$\lim_{x\to\infty} \frac{\log \pi(x)}{\log x} + \underbrace{\lim_{x\to\infty} \frac{\log \log x}{\log x}}_{=0} - 1 = 0.$$

This implies that

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

Now

$$\begin{aligned}\lim_{x\to\infty} \frac{\pi(x)\log \pi(x)}{x} &= \lim_{x\to\infty} \frac{\log \pi(x)}{\log x} \times \frac{\pi(x)\log x}{x} \\ &= \lim_{x\to\infty} \frac{\log \pi(x)}{\log x} \times \lim_{x\to\infty} \frac{\pi(x)\log x}{x} = (1)(1) = 1.\end{aligned}$$

(2) $\Rightarrow$ (3):
Assume that (2) holds. That is

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

Putting $x = p_n$ in the above equation we obtain:

$$\lim_{n\to\infty} \frac{\pi(p_n)\log \pi(p_n)}{p_n} = 1.$$

This implies that

$$\lim_{n\to\infty} \frac{n \log n}{p_n} = 1. \ (\because \pi(p_n) = n)$$

This implies that

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

Thus (2) $\Rightarrow$ (3).
(3) $\Rightarrow$ (2) :
Assume that (2) holds. That is

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

We want to show that

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

Given $x \in [2,\infty)$. Then we can find consecutive prime numbers p_n and p_{n+1} such that

$$p_n \leq x \leq p_{n+1}. \tag{2.12}$$

Then by the definition of π, we have $\pi(x) = n$. Equation (2.12) can be written as

$$\frac{p_n}{n\log n} \leq \frac{x}{n\log n} \leq \frac{p_{n+1}}{n\log n}. \tag{2.13}$$

Taking limits as $n \to \infty$, we obtain:

$$\lim_{n\to\infty} \frac{p_n}{n\log n} \leq \lim_{n\to\infty} \frac{x}{n\log n} \leq \lim_{n\to\infty} \frac{p_{n+1}}{n\log n}. \tag{2.14}$$

This implies that

$$1 \leq \lim_{n\to\infty} \frac{x}{n\log n} \leq \lim_{n\to\infty} \frac{p_{n+1}}{n\log n}. \tag{2.15}$$

We will show that $\lim_{n\to\infty} \frac{p_{n+1}}{n\log n} = 1$. Now

$$\frac{p_{n+1}}{n\log n} = \frac{p_{n+1}}{(n+1)\log(n+1)} \times \frac{(n+1)\log(n+1)}{n\log n}$$

Therefore

$$\begin{aligned}\lim_{n\to\infty} \frac{p_{n+1}}{n\log n} &= \lim_{n\to\infty} \frac{p_{n+1}}{(n+1)\log(n+1)} \times \lim_{n\to\infty} \frac{(n+1)\log(n+1)}{n\log n} \\ &= (1)(1) = 1.\end{aligned}$$

Thus

$$\lim_{n\to\infty} \frac{p_{n+1}}{n\log n} = 1.$$

Inserting $\lim_{n\to\infty} \frac{p_{n+1}}{n\log n} = 1$ in equation (2.13), we obtain:

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

Equivalently,

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

(2) $\Rightarrow$ (1) :
Assume that (2) holds. That is

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

Taking log on both sides, we obtain:

$$\lim_{x\to\infty} \log\pi(x) + \log\log\pi(x) - \log(x) = 0.$$

Equivalently,

$$\lim_{x\to\infty} \left[\log\pi(x)\left(1 + \frac{\log\log\pi(x)}{\log\pi(x)} - \frac{\log x}{\log\pi(x)}\right)\right] = 0.$$

That is

$$\lim_{x\to\infty} \left[\frac{1 + \frac{\log\log\pi(x)}{\log\pi(x)} - \frac{\log x}{\log\pi(x)}}{1/\log\pi(x)}\right] = 0.$$

This implies that

$$1 + \frac{\log\log\pi(x)}{\log\pi(x)} - \frac{\log x}{\log\pi(x)} = O(1/\log\pi(x))$$

This implies that there is a constant $M > 0$ such that

$$1 + \frac{\log\log\pi(x)}{\log\pi(x)} - \frac{\log x}{\log\pi(x)} \leq M(1/\log\pi(x))$$

This implies that

$$\lim_{x\to\infty} \left[1 + \frac{\log\log\pi(x)}{\log\pi(x)} - \frac{\log x}{\log\pi(x)}\right] = 0.$$

This implies that

$$1 + \underbrace{\lim_{x\to\infty} \frac{\log\log\pi(x)}{\log\pi(x)}}_{=0} - \lim_{x\to\infty} \frac{\log x}{\log\pi(x)} = 0.$$

This implies that

$$\lim_{x\to\infty} \frac{\log x}{\log\pi(x)} = 0.$$

Now

$$\begin{aligned}\lim_{x\to\infty}\frac{\pi(x)\log x}{x} &= \lim_{x\to\infty}\left[\frac{\log x}{\log\pi(x)}\times\frac{\pi(x)\log\pi(x)}{x}\right]\\ &= \lim_{x\to\infty}\frac{\log x}{\log\pi(x)}\times\lim_{x\to\infty}\frac{\pi(x)\log\pi(x)}{x}\\ &= (1)(1) = 1.\end{aligned}$$

This completes the proof of the theorem. □

2.4 Inequalities for $\pi(n)$ and p_n

Lemma 1. *For $n \geq 1$ we have*

$$2^n < \binom{2n}{n} < 4^n.$$

Proof. Note that

$$4^n = (1+1)^{2n} = \sum_{k=0}^{2n}\binom{2n}{k} > \binom{2n}{n}.$$

Next we show that

$$2^n < \binom{2n}{n}$$

We will prove the inequality by induction on n.
Step 1: Suppose $n = 1$.
In this case

$$2^1 = \binom{2}{1} = \binom{2\times 1}{1}$$

Thus the result is true when $n = 1$.
Step 2: Assume that the result is true for $n = m$. That is

$$2^m < \binom{2m}{m}.$$

Step 3: To prove that the result is true for $n = m+1$. That is we have to prove that

$$2^m < \binom{2m+2}{m}$$

Note that

$$\begin{aligned}\binom{2(m+1)}{m+1} = \binom{2m+2}{m+1} &= \binom{2m+1}{m} + \binom{2m+1}{m+1}\\ &= \binom{2m}{m} + \binom{2m}{m-1} + \binom{2m}{m} + \binom{2m}{m+1}\end{aligned}$$

$$= 2\binom{2m}{m} + \binom{2m}{m-1} + \binom{2m}{m+1}$$
$$> 2\binom{2m}{m} > 2 \times 2^m = 2^{m+1}.$$

□

Theorem 2.4.1. *For $n \geq 2$ we have*

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

Proof. By lemma 1, we have

$$2^n < \binom{2n}{n} < 4^n.$$

That is,

$$2^n < \frac{2n!}{(n!)^2} < 4^n.$$

Taking logarithms we obtain

$$n \log 2 \leq \log(2n)! - 2\log n! < n \log 4. \tag{2.16}$$

But theorem 1.2.8 implies that

$$[x]! = \prod_{p \leq x} p^{\alpha(p)},$$

where $\alpha(p) = \sum_{m=1}^{\infty} \left[\frac{x}{p^m}\right]$.
Taking logarithms we obtain:

$$\log[x]! = \sum_{p \leq n} \alpha(p) \log p,$$

That is

$$\log[x]! = \sum_{p \leq x} \sum_{m=1}^{\infty} \left[\frac{x}{p^m}\right] \log p \tag{2.17}$$

Note that if $x < p^m$, we have $x/p^m < 1$ and hence $\left[\frac{x}{p^m}\right] = 0$. Now

$$x < p^m \Rightarrow \log x < m \log p$$
$$\frac{\log x}{\log p} < m.$$

This implies that

$$\left[\frac{x}{p^m}\right] = 0 \quad \text{if} \quad m > \left[\frac{\log x}{\log p}\right].$$

Hence equation (2.17) can be written as:

$$\log[x]! = \sum_{p\leq x} \sum_{m=1}^{\left[\frac{\log x}{\log p}\right]} \left[\frac{x}{p^m}\right] \log p \tag{2.18}$$

Putting $x = n$ in (2.18) equation, we obtain:

$$\log n! = \sum_{p\leq n} \sum_{m=1}^{\left[\frac{\log n}{\log p}\right]} \left[\frac{n}{p^m}\right] \log p$$

Again putting $x = 2n$ in equation (2.18), we obtain

$$\log 2n! = \sum_{p\leq 2n} \sum_{m=1}^{\left[\frac{\log 2n}{\log p}\right]} \left[\frac{2n}{p^m}\right] \log p$$

Hence

$$\begin{aligned}
\log 2n! - 2\log n! &= \sum_{p\leq 2n} \sum_{m=1}^{\left[\frac{\log 2n}{\log p}\right]} \left[\frac{2n}{p^m}\right] \log p - 2\sum_{p\leq n} \sum_{m=1}^{\left[\frac{\log n}{\log p}\right]} \left[\frac{n}{p^m}\right] \log p \\
&= \sum_{p\leq 2n} \sum_{m=1}^{\left[\frac{\log 2n}{\log p}\right]} \left[\frac{2n}{p^m}\right] \log p - 2\sum_{p\leq n} \sum_{m=1}^{\left[\frac{\log n}{\log p}\right]} \left[\frac{n}{p^m}\right] \log p \\
&\qquad \underbrace{- 2\sum_{p>n} \sum_{m=\left[\frac{\log n}{\log p}\right]+1}^{\left[\frac{\log 2n}{\log p}\right]} \left[\frac{n}{p^m}\right] \log p}_{=0} \\
&= \sum_{p\leq 2n} \sum_{m=1}^{\left[\frac{\log 2n}{\log p}\right]} \left(\underbrace{\left[\frac{2n}{p^m}\right] - 2\left[\frac{n}{p^m}\right]}_{0 \text{ or } 1} \right) \log p \qquad (2.19) \\
&\leq \sum_{p\leq 2n} \sum_{m=1}^{\left[\frac{\log 2n}{\log p}\right]} \log p = \sum_{p\leq 2n} \left[\frac{\log 2n}{\log p}\right] \log p \\
&\leq \sum_{p\leq 2n} \frac{\log 2n}{\log p} \log p = \log 2n \sum_{p\leq 2n} 1 = \log(2n)\pi(2n).
\end{aligned}$$

Thus

$$\log 2n! - 2\log n! \leq \pi(2n)\log(2n). \tag{2.20}$$

Consider the leftmost inequality in (2.16):

$$n \log 2 \leq \log(2n)! - 2 \log n!. \tag{2.21}$$

In the light of equation (2.20), we have

$$n \log 2 \leq \pi(2n) \log(2n).$$

This implies that

$$\begin{aligned}
\pi(2n) \geq \frac{n \log 2}{\log(2n)} &= \frac{2n}{\log 2n} \times \frac{\log 2}{2} \\
&> \frac{2n}{\log 2n} \frac{1}{2} \times \frac{1}{2} \quad (\because \log 2 > 1/2) \\
&= \frac{1}{4} \frac{2n}{\log 2n} \\
&> \frac{1}{6} \frac{2n}{\log 2n}
\end{aligned}$$

Thus

$$\frac{1}{6} \frac{2n}{\log 2n} < \pi(2n) \tag{2.22}$$

Since π is an increasing function, we have

$$\begin{aligned}
\pi(2n+1) \geq \pi(2n) &> \frac{1}{4} \frac{2n}{\log 2n} \\
&> \frac{1}{4} \frac{2n}{\log(2n+1)} \times \frac{2n+1}{\log(2n+1)} \\
&> \frac{1}{4} \frac{2}{3} \frac{2n+1}{\log(2n+1)} = \frac{1}{6} \frac{2n+1}{\log(2n+1)}
\end{aligned}$$

That is

$$\frac{1}{6} \frac{2n+1}{\log(2n+1)} < \pi(2n+1). \tag{2.23}$$

From equations (2.22) and (2.23), we have:

$$\frac{1}{6} \frac{n}{\log n} < \pi(n) \quad \text{for all } n \geq 2. \tag{2.24}$$

This proves the leftmost inequality in the theorem. To prove the other inequality we consider equation (2.19):

$$\log 2n! - 2 \log n! = \sum_{p \leq 2n} \sum_{m=1}^{\left[\frac{\log 2n}{\log p}\right]} \left(\underbrace{\left[\frac{2n}{p^m}\right] - 2 \left[\frac{n}{p^m}\right]}_{0 \text{ or } 1} \right) \log p$$

$$
\begin{aligned}
&= \sum_{p\le 2n}\left(\left[\frac{2n}{p}\right]-2\left[\frac{n}{p}\right]\right)\log p + \sum_{p\le 2n}\sum_{m=2}^{\left[\frac{\log 2n}{\log p}\right]}\left(\left[\frac{2n}{p}\right]-2\left[\frac{n}{p}\right]\right)\log p\\
&\ge \sum_{p\le 2n}\left(\left[\frac{2n}{p}\right]-2\left[\frac{n}{p}\right]\right)\log p\\
&\ge \sum_{n<p\le 2n}\left(\underbrace{\left[\frac{2n}{p}\right]}_{=1}-2\underbrace{\left[\frac{n}{p}\right]}_{=0}\right)\log p\\
&= \sum_{n<p\le 2n}\log p\\
&= \sum_{p\le 2n}\log p - \sum_{p\le n}\log p\\
&= \vartheta(2n)-\vartheta(n).
\end{aligned}
$$

Hence

$$\vartheta(2n)-\vartheta(n)\le \log(2n)!-\log(n)!<n\log 4. \quad \text{(by Eqn(2.16))}$$

Taking $n=2^r$ in the above inequality we obtain:

$$\vartheta(2^{r+1})-\vartheta(2^r)<\log(2n)!-\log(n)!<2^r\log 4=2^{r+1}\log 2.$$

Summing the above inequality from $r=0$ to $r=k$, we obtain:

$$\sum_{r=0}^{k}\left[\vartheta(2^{r+1})-\vartheta(2^r)\right]<\sum_{r=0}^{k}2^{r+1}\log 2.$$

The above inequality can be written as:

$$\vartheta(2^{r+1})<(2^{k+1}-1)\log 4<2^{k+1}\log 2.$$

Hence

$$\vartheta(2^{r+1})<2^{k+1}\log 2. \tag{2.25}$$

Now we choose k so that $2^k\le n\le 2^{k+1}$. Since ϑ is an increasing function we have

$$\vartheta(n)\le\vartheta(2^{r+1})<2^{k+2}\log 2\le 4n\log 2. \quad \left(\because 2^k\le n\right) \tag{2.26}$$

But if $0<\alpha<1$, we have

$$(\pi(n)-\pi(n^\alpha))=\left(\sum_{n^\alpha<p\le n}1\right)\log n^\alpha$$

$$\begin{aligned} &< \sum_{n^\alpha < p \le n} \log p \quad (\because \log n^\alpha < \log p) \\ &\le \vartheta(n) < 4n \log 2 \quad (\text{by Eqn } (2.26)) \end{aligned}$$

Hence

$$\begin{aligned} \pi(n) &< \frac{4n \log 2}{\alpha \log n} + \pi(n^\alpha) \\ &< \frac{4n \log 2}{\alpha \log n} + n^\alpha \\ &= \frac{n}{\log n}\left(\frac{4 \log 2}{\alpha} + \frac{\log n}{n^{1-\alpha}}\right) \end{aligned} \tag{2.27}$$

Consider the function

$$f(x) = x^{-c} \log x, \quad c > 0, x \ge 1$$

Note that the function f attains its maximum at $x = e^{1/c}$ and the maximum value of f is $1/ce$.
Putting $\alpha = 2/3$ in equation (2.27), we obtain:

$$\begin{aligned} \pi(n) &< \frac{n}{\log n}\left[\frac{4 \log 2}{2/3} + \frac{\log n}{n^{1/3}}\right] \\ &= \frac{n}{\log n}[6 \log 2 + n^{-1/3} \log n] \\ &\le \frac{n}{\log n}[6 \log 2 + 3/e] < 6n/\log n \end{aligned}$$

□

Theorem 2.4.2. *For $n \ge 1$ the nth prime p_n satisfies the inequalities*

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

Proof. For $k \ge 2$ we have(Theorem 2.4.1)

$$\frac{1}{6} \frac{k}{\log k} < \pi(k) < 6 \frac{k}{\log k}. \tag{2.28}$$

If $k = p_n$ then $k \ge 2$ and $n = \pi(k)$. Putting $k = p_n$ in the righttmost inequality in 2.28 we obtain:

$$n = \pi(p_n) < 6 \frac{p_n}{\log p_n}$$

This implies that

$$p_n < 6n \log p_n \tag{2.29}$$

Again consider the leftmost inequality in (2.4.1):

$$\frac{1}{6}\frac{k}{\log k} < \pi(k)$$

Putting $k = p_n$ in the above inequality we obtain

$$\frac{1}{6}\frac{p_n}{\log p_n} < \pi(p_n) = n$$

This implies that

$$p_n < 6n \log p_n$$

The above equation can be written as:

$$\frac{p_n}{\sqrt{p_n}} < \frac{6n \log p_n}{\sqrt{p_n}} \tag{2.30}$$

Now consider the function

$$f(x) = \frac{\log x}{\sqrt{x}}$$

Then we have

$$f'(x) = \frac{2 - \log x}{2x^{3/2}}$$

Also $f'(x) = 0$ implies that $x = e^2$. One can easily verify that $f''(e^2) < 0$. Hence the function f has a maximum at $x = e^2$ and the maximum value is given by $2/e$. Hence equation (2.31) can be written as:

$$\sqrt{p_n} < \frac{6n \log p_n}{\sqrt{p_n}} < 6n\left(\frac{2}{e}\right) = \frac{12n}{e}. \tag{2.31}$$

Taking logarithms we obtain:

$$\frac{1}{2}\log p_n < \log\left(\frac{12}{e} + \log n\right)$$

This implies that

$$\log p_n < 2\log\left(\frac{12}{e}\right) + 2\log n \tag{2.32}$$

Hence equations (2.29) and (2.32) we have:

$$\begin{aligned} p_n &< 6n\left[2\log\left(\frac{12}{e}\right) + 2\log n\right] \\ &= 12\left(n\log n + n\log\left(\frac{12}{e}\right)\right) \end{aligned}$$

This completes the proof of the theorem. □

Corollary 5. *The series* $\sum_{k=1}^{\infty} \frac{1}{p_n}$ *is divergent.*

Proof. From the leftmost inequality in theorem 2.4.2 we have

$$\frac{1}{6} n \log n < p_n.$$

This implies that

$$\frac{1}{p_n} < \frac{6}{n \log n}$$

Note that the series $\sum_{n=2}^{\infty} \frac{1}{n \log n}$ is a divergent series. So by comparison test, the series $\sum_{n=1}^{\infty} \frac{1}{p_n}$ is divergent. □

2.5 Shapiro's Tauberian theorem

Theorem 2.5.1. *Let* $\{a_n\}$ *be a sequence such that*

$$\sum_{n \leq x} a(n) \left[\frac{x}{n}\right] = x \log x + O(x) \quad \textit{for all} \quad x \geq 1.$$

Then

(a) For $x \geq 1$ *we have*

$$\sum_{n \leq x} \frac{a(n)}{n} = \log x + O(1).$$

(b) There is a constant $B > 0$ *such that*

$$\sum_{n \leq x} a(n) \leq Bx \quad \textit{for all} \quad x \geq 1.$$

(c) There is a constant $A > 0$ *and an* $x_0 > 0$ *such that*

$$\sum_{n \leq x} a(n) \geq Ax \quad \textit{for all} \quad x \geq x_0.$$

Proof. Let

$$S(x) = \sum_{n \leq x} a(n),$$
$$T(x) = \sum_{n \leq x} a(n) \left[\frac{x}{n}.\right]$$

It is given that

$$\sum_{n\leq x} a(n)\left[\frac{x}{n}\right] = x\log x + O(x) \quad \text{for all} \quad x \geq 1.$$

That is,

$$T(x) = x\log x + O(x) \quad \text{for all} \quad x \geq 1. \tag{2.33}$$

First we prove (b). For this first we establish the following inequality:

$$S(x) - S\left(\frac{x}{2}\right) \leq T(x) - T\left(\frac{x}{2}\right).$$

Now

$$\begin{aligned}
T(x) - 2T\left(\frac{x}{2}\right) &= \sum_{n\leq x} a(n)\left[\frac{x}{n}\right] - 2\sum_{n\leq x/2} a(n)\left[\frac{x}{2n}\right] \\
&= \sum_{n\leq x/2} a(n)\left[\frac{x}{n}\right] + \sum_{x/2<n\leq x} a(n)\left[\frac{x}{n}\right] - 2\sum_{n\leq x/2} a(n)\left[\frac{x}{2n}\right] \\
&= \sum_{n\leq x/2} a(n)\left(\underbrace{\left[\frac{x}{n}\right] - 2\left[\frac{x}{2n}\right]}_{0 \text{ or } 1}\right) + \sum_{x/2n\leq x} a(n)\left[\frac{x}{n}\right] \\
&\geq \sum_{x/2<n\leq x} a(n)\left[\frac{x}{n}\right] \\
&= \sum_{n\leq x} a(n)\left[\frac{x}{n}\right] - \sum_{n\leq x/2} a(n)\left[\frac{x}{n}\right] \\
&= S(x) - S\left(\frac{x}{2}\right)
\end{aligned}$$

Hence

$$S(x) - S\left(\frac{x}{2}\right) \leq T(x) - T\left(\frac{x}{2}\right)$$

Now

$$\begin{aligned}
T(x) - T\left(\frac{x}{2}\right) &= [x\log x + O(x)] - 2\left[\frac{x}{2}\log\frac{x}{2} + O\left(\frac{x}{2}\right)\right] \\
&= x\log x + O(x) - x\log x + x\log 2 + O\left(\frac{x}{2}\right) \\
&= x\log 2 + O(x) = O(x) + O(x) = O(x).
\end{aligned}$$

Hence

$$T(x) - T\left(\frac{x}{2}\right) = O(x)$$

This implies that

$$S(x) - S\left(\frac{x}{2}\right) \leq O(x).$$

This means that there is some constant $K > 0$ such that

$$S(x) - S\left(\frac{x}{2}\right) \leq Kx \quad \text{for all} \quad x \geq 1.$$

Replace x successively by $x/2, x/4, \ldots$ to get

$$\begin{aligned} S\left(\frac{x}{2}\right) - S\left(\frac{x}{4}\right) &\leq K\ \frac{x}{2}, \\ S\left(\frac{x}{4}\right) - S\left(\frac{x}{8}\right) &\leq K\ \frac{x}{4}, \\ &\vdots \end{aligned}$$

Adding the above inequalities we get

$$S(x) \leq K\left[x + (x/2) + (x/2^2) + \cdots\right] = \underbrace{2K}_{B} x$$

That is

$$S(x) \leq Bx$$

That is,

$$\sum_{n \leq x} a(n) \leq Bx.$$

This completes the proof of (b). Next we prove (a). Note that

$$\frac{x}{n} - \left[\frac{x}{n}\right] < 1$$

This implies that

$$\left[\frac{x}{n}\right] - \frac{x}{n} = O(1).$$

Hence

$$\begin{aligned} T(x) &= \sum_{n \leq x} \left[\frac{x}{n}\right] a(n) \\ &= \sum_{n \leq x} \left(\frac{x}{n} + O(1)\right) a(n) \\ &= x \sum_{n \leq x} \frac{a(n)}{n} + O\left(\sum_{n \leq x} a(n)\right) \end{aligned}$$

$$= x \sum_{n \leq x} \frac{a(n)}{n} + O(S(x))$$
$$= x \sum_{n \leq x} \frac{a(n)}{n} + O(x) \quad (\because S(x) \leq Bx)$$

Hence

$$\sum_{n \leq x} \frac{a(n)}{n} = \frac{1}{x} T(x) + O(1)$$
$$= \frac{1}{x} [x \log x + O(x)]$$
$$= \log x + O(1).$$

This completes the proof of (a).
Finally, we prove (c). Let

$$A(x) = \sum_{n \leq x} \frac{a(n)}{n}$$

Then by part (a) of the theorem, we have

$$A(x) = \log x + O(1)$$

Equivalently,

$$A(x) = \log x + R(x),$$

where $R(x) = O(1)$. Since $R(x) = O(1)$ we have $|R(x)| \leq M$ for some $M > 0$. Choose α such that $0 < \alpha < 1$. Consider

$$\begin{aligned} A(x) - A(\alpha x) &= \sum_{n \leq x} \frac{a(n)}{n} - \sum_{n \leq \alpha x} \frac{a(n)}{n} \\ &= \log x + R(x) - [\log \alpha x + R(\alpha x)] \quad (\text{if } \ x \geq 1 \ \text{ and } \ \alpha x \geq 1) \\ &= \log x + R(x) - \log \alpha - \log x - R(\alpha x) \\ &= -\log \alpha + R(x) - R(\alpha x) \\ &\geq -\log \alpha - |R(x)| - |R(\alpha x)| \\ &\geq -\log \alpha - 2M \end{aligned}$$

Now choose α so that $-\log \alpha - 2M = 1$. This implies that $\alpha = e^{-(2M+1)}$. Obviously $0 < \alpha < 1$. For this α we have the inequality

$$A(x) - A(\alpha x) \geq 1 \ \text{ if } \ x \geq \frac{1}{\alpha}.$$

But

$$A(x) - A(\alpha x) = \sum_{n \leq x} \frac{a(n)}{n} - \sum_{n \leq \alpha x} \frac{a(n)}{n} = \sum_{\alpha x < n \leq x} \frac{a(n)}{n}$$

$$\leq \sum_{n\leq x} \frac{a(n)}{n} < \frac{1}{\alpha x} \sum_{n\leq x} a(n) = \frac{1}{\alpha x} S(x).$$

Thus

$$\frac{S(x)}{\alpha x} > A(x) - A(\alpha x) \geq 1 \text{ if } x \geq \frac{1}{\alpha}.$$

Thus

$$S(x) \geq \alpha x \quad \text{if } x \geq \frac{1}{\alpha}.$$

Taking $A = \alpha$ and $x_0 = 1/\alpha$ we have

$$S(x) \geq Ax, \quad x > x_0.$$

This completes the proof of the theorem. □

2.6 Applications of Shapiro's theorem

Theorem 2.6.1. *For all $x \geq 1$ we have*

$$\sum_{n\leq x} \frac{\Lambda(n)}{n} = \log x + O(1).$$

Also, there exist positive constants c_1 and c_2 such that

$$\psi(x) \geq c_1 x \text{ for all } x \geq 1$$

and

$$\psi(x) \geq c_2 x \text{ for all sufficiently large } x.$$

Proof. We have

$$\begin{aligned}\sum_{n\leq x} \Lambda(n) \left[\frac{x}{n}\right] &= \log[x]! \\ &= x\log x - x + O(\log x) \\ &= x\log x + O(x) + O(\log x) \\ &= x\log x + O(x).\end{aligned}$$

Hence

$$\sum_{n\leq x} \underbrace{\Lambda(n)}_{a(n)} \left[\frac{x}{n}\right] = x\log x + O(x)$$

So by Shapiros theorem we have

$$(a) \sum_{n\leq x} \frac{\Lambda(n)}{n} = \log x + O(1).$$

Also there exists $c_1 > 0$ and $c_2 > 0$ such that

$$(b) \underbrace{\sum_{n \le x} \Lambda(n)}_{\psi(x)} \le c_1 x \quad \text{for} \quad x \ge 1.$$

$$(c) \underbrace{\sum_{n \le x} \Lambda(n)}_{\psi(x)} \ge c_2 x \quad \text{for sufficiently large} \quad x.$$

This completes the proof of the theorem. □

Theorem 2.6.2. *For all $x \ge 1$ we have*

$$\sum_{p \le x} \frac{\log p}{p} = \log x + O(1).$$

Also there exist positive constants c_1 and c_2 such that

$$\vartheta(x) \le c_1 x \quad \textit{for all} \quad x \ge 1.$$

and

$$\vartheta(x) \ge c_2 x \quad \textit{for sufficiently large} \quad x.$$

Proof. We know that for $x \ge 2$,

$$\sum_{p \le x} \log p \left[\frac{x}{p}\right] = x \log x + O(x). \tag{2.34}$$

Define

$$\Lambda_1(n) = \begin{cases} \log p & \text{if } n \text{ is a prime} \\ 0 & \text{otherwise} \end{cases}$$

Then equation (2.34) can be written as:

$$\sum_{n \le x} \underbrace{\Lambda_1(n)}_{a(n) \ge 0} \left[\frac{x}{n}\right] = x \log x + O(x).$$

So by Shapiros theorem, we have the following

$$(a) \sum_{n \le x} \frac{\Lambda_1(n)}{n} = \log x + O(1)$$

This implies that

$$\sum_{p \le x} \frac{\log p}{p} = \log x + O(1).$$

$$(b)\ \sum_{n\leq x}\Lambda_1(n)\leq C_1x,\quad \text{for all}\ \ x\geq 1.$$

This implies that

$$\underbrace{\sum_{p\leq x}\log p}_{\vartheta(x)}\leq c_1x$$

for all $x\geq 1$.

$$(c)\ \sum_{n\leq x}\Lambda_1(n)\geq C_2x,$$

for sufficiently large x. This implies that

$$\vartheta(x)\geq c_2x,$$

for sufficiently large x. □

Theorem 2.6.3. *For all $x\geq 1$ we have*

$$\sum_{n\leq x}\psi\left(\frac{x}{n}\right)=x\log x-x+O(\log x)$$

and

$$\sum_{n\leq x}\vartheta\left(\frac{x}{n}\right)=x\log x+O(x).$$

Proof. Note that if $f(n)$ is an arithmetical function, then

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

where $F(x)=\sum_{n\leq x}f(n)$.
We have

$$\psi(x)=\sum_{n\leq x}\Lambda(n).$$

Then

$$\sum_{n\leq x}\Lambda(n)\left[\frac{x}{n}\right]=\sum_{n\leq x}\psi\left(\frac{x}{n}\right)\tag{2.35}$$

We have already proved that

$$\sum_{n\leq x}\Lambda(n)\left[\frac{x}{n}\right]=x\log x-x+O(\log x)\tag{2.36}$$

In the light of equations (2.35) and (2.36) we have

$$\sum_{n\leq x}\psi\left(\frac{x}{n}\right)=x\log x-x+O(\log x)$$

Again we have

$$\vartheta(x)=\sum_{n\leq x}\log p=\sum_{n\leq x}\Lambda_1(n).$$

Then

$$\sum_{n\leq x}\Lambda_1(n)\left[\frac{x}{n}\right]=\sum_{n\leq x}\vartheta\left(\frac{x}{n}\right)$$

But

$$\sum_{n\leq x}\Lambda_1(n)\left[\frac{x}{n}\right]=x\log x+O(x).$$

Hence

$$\sum_{n\leq x}\vartheta\left(\frac{x}{n}\right)=x\log x+O(x).$$

This completes the proof of the theorem. □

2.7 An asymptotic formula for the partial sums

Theorem 2.7.1. *There is a constant A such that*

$$\sum_{p\leq x}\frac{1}{p}=\log\log x+A+O\left(\frac{1}{\log x}\right)\quad \textit{for all}\quad x\geq 2.$$

Proof. Let

$$A(x)=\sum_{n\leq x}\frac{\log p}{p}$$

and let

$$a(n)=\begin{cases}1 & \text{if } n \text{ is prime,}\\ 0 & \text{otherwise}\end{cases}$$

Then

$$\sum_{n\leq x}\frac{1}{p}=\sum_{n\leq x}\frac{a(n)}{n}\quad\text{and}\quad A(x)=\sum_{n\leq x}\frac{a(n)}{n}\log n.$$

Recall Abel's identity:

$$\sum_{y<n\leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$$

Putting $y = 3/2$, $f(t) = \frac{1}{\log t}$ and $a_n = \frac{a(n)}{n}\log n$ in the Abel's identity, we obtain:

$$\sum_{3/2<n\leq x} \frac{a(n)}{n}\log n\frac{1}{\log n} = A(x)\frac{1}{\log x} - A(3/2)\frac{1}{\log(3/2)} + \int_{3/2}^x \frac{A(t)}{t\log^2 t}dt.$$

That is

$$\sum_{3/2<n\leq x} \frac{a(n)}{n} = \frac{A(x)}{\log x} + \int_{3/2}^x \frac{A(t)}{t\log^2 t}dt.$$

Thta is

$$\begin{aligned}\sum_{p\leq x}\frac{1}{p} &= \frac{A(x)}{\log x} + \int_{3/2}^2 \frac{A(t)}{t\log^2 t}dt + \int_2^x \frac{A(t)}{t\log^2 t}dt \\ &= \frac{A(x)}{\log x} + \int_2^x \frac{A(t)}{t\log^2 t}dt \end{aligned} \tag{2.37}$$

Now

$$\begin{aligned}A(x) &= \sum_{n\leq x} a(n)\frac{\log n}{n} \\ &= \sum_{p\leq x}\frac{\log p}{p} \\ &= \log x + O(1)\end{aligned}$$

Inserting the value of $A(x)$ in equation (2.37) we obtain:

$$\begin{aligned}\sum_{p\leq x}\frac{1}{p} &= \frac{\log x + O(1)}{\log x} + \int_2^x \frac{\log t + R(t)}{t\log^2 t}dt, R(t) = O(1). \\ &= 1 + O\left(\frac{1}{\log x}\right) + \int_2^x \frac{1}{t\log t}dt + \int_2^x \frac{R(t)}{t\log^2 t}dt \end{aligned} \tag{2.38}$$

Now

$$\begin{aligned}\int_2^x \frac{1}{t\log t}dt &= \int_2^x \frac{1/t}{\log t}dt \\ &= (\log\log t)_2^x = \log(\log x) - \log(\log 2).\end{aligned}$$

Also

$$\int_2^x \frac{R(t)}{t\log^2 t}dt = \int_2^\infty \frac{R(t)}{t\log^2 t}dt - \int_x^\infty \frac{R(t)}{t\log^2 t}dt \tag{2.39}$$

Note that

$$R(t) = O(1)$$

Therefore

$$\int_x^\infty \frac{R(t)}{t\log^2 t}dt = O\left(\int_x^\infty \frac{1}{t\log^2 t}dt\right) = O\left(\int_x^\infty \frac{d}{dt}\left(\frac{-1}{\log t}\right)\right) = O\left(\frac{1}{\log x}\right)$$

Hence equation (2.39) can be written as:

$$\begin{aligned}\int_x^\infty \frac{1}{t\log t}dt &= \underbrace{\int_2^\infty \frac{R(t)}{t\log^2 t}dt}_{=B} + O\left(\frac{1}{\log x}\right)\\ &= B + O\left(\frac{1}{\log x}\right).\end{aligned}$$

Hence equation (2.38) becomes:

$$\begin{aligned}\sum_{p\leq x}\frac{1}{p} &= 1 + O\left(\frac{1}{\log x}\right) + + \log(\log x) - \log(\log 2) + B + O\left(\frac{1}{\log x}\right).\\ &= \log\log x + O\left(\frac{1}{\log x}\right) + A.\end{aligned}$$

□

2.8 The partial sums of the Mobius function

Definition 2.8.1. *If $x \geq 1$ we define*

$$M(x) = \sum_{n\leq x}\mu(n).$$

The exact bounds of $M(x)$ is not known. Numerical evidence suggests that

$$|M(x)| < \sqrt{x}, \text{ if } x > 1.$$

Definition 2.8.2. *If $x \geq 1$ we define*

$$H(x) = \sum_{n\leq x}\mu(n)\log n.$$

Theorem 2.8.1. *We have*

$$\lim_{x\to\infty}\left(\frac{M(x)}{x} - \frac{H(x)}{x\log x}\right) = 0.$$

Proof. Recall Abel's identity:

$$\sum_{y<n\leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$$

Putting $y = 1$, $a(n) = \mu(n)$ and $f(t) = \log t$ in the Abel's identity we obtain

$$\sum_{1<n\leq x} \mu(n)\log(n) = M(x)\log x - M(1)\log 1 - \int_y^x M(t)\frac{1}{t}dt.$$

That is,

$$\underbrace{\sum_{1<n\leq x} \mu(n)\log(n)}_{H(x)} = M(x)\log x - \int_1^x \frac{M(t)}{t}dt.$$

That is

$$H(x) = M(x)\log x - \int_1^x \frac{M(t)}{t}dt.$$

Dividing both sides by $x\log x$ we obtain:

$$\frac{H(x)}{x\log x} = \frac{M(x)}{x} - \frac{1}{x\log x}\int_1^x \frac{M(t)}{t}dt.$$

That is

$$\frac{M(x)}{x} - \frac{H(x)}{x\log x} = \frac{1}{x\log x}\int_1^x \frac{M(t)}{t}dt$$

Therefore

$$\lim_{x\to\infty}\left(\frac{M(x)}{x} - \frac{H(x)}{x\log x}\right) = \lim_{x\to\infty}\frac{1}{x\log x}\int_1^x \frac{M(t)}{t}dt.$$

Claim: $\lim_{x\to\infty}\left(\frac{1}{x\log x}\int_1^x \frac{M(t)}{t}dt\right) = 0$. But we have the trivial estimate $M(x) = O(x)$ so

$$\int_1^x \frac{M(t)}{t}dt = O\left(\int_1^x dt\right) = O(x),$$

Therefore

$$\begin{aligned}\frac{1}{x\log x}\int_1^x \frac{M(t)}{t}dt &= \frac{1}{x\log x}O(x)\\ &= O\left(\frac{1}{\log x}\right)\end{aligned}$$

This implies that $\lim_{x\to\infty}\left(\frac{1}{x\log x}\int_1^x \frac{M(t)}{t}dt\right) = 0$. □

Theorem 2.8.2. *The prime number theorem implies that*

$$\lim_{x\to\infty}\frac{M(x)}{x}=0.$$

Proof. By theorem 2.8.1 we have

$$\lim_{x\to\infty}\left(\frac{M(x)}{x}-\frac{H(x)}{x\log x}\right)=0.$$

To prove the theorem it suffices to show that

$$\lim_{x\to\infty}\frac{H(x)}{x\log x}=0.$$

By definition of $H(x)$ we have

$$-H(x)=-\sum_{n\leq x}\mu(n)\log n$$

Claim:$-\sum_{n\leq x}\mu(n)\log n=\sum_{n\leq x}\mu(n)\psi\left(\frac{x}{n}\right)$. We have

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

So by Mobius inversion formula, we have

$$\begin{aligned}\Lambda(n)&=\sum_{d|n}\mu(d)\log\left(\frac{n}{d}\right)\\&=\sum_{d|n}\mu(d)\log n-\sum_{d|n}\mu(d)\log(d)\\&=\log n\left[\frac{1}{n}\right]-\sum_{d|n}\mu(d)\log d\\&=-\sum_{d|n}\mu(d)\log d.\end{aligned}$$

Hence

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

Again by Mobius inversion formula,

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

Hence

$$\begin{aligned}-\sum_{n\leq x}\mu(n)\log n &= \sum_{n\leq x}\sum_{d|n}\mu(d)\Lambda\left(\frac{n}{d}\right)\\ &= \sum_{n\leq x}(\mu*\Lambda)(n)\\ &= \sum_{n\leq x}\mu(n)\sum_{n\leq x/n}\Lambda(n)\\ &= \sum_{n\leq x}\mu(n)\psi\left(\frac{x}{n}\right)\end{aligned}$$

Hence

$$-H(x) = -\sum_{n\leq x}\mu(n)\log n = \sum_{n\leq x}\mu(n)\psi\left(\frac{x}{n}\right)$$

We know that

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

Hence prime number theorem is equivalent to $\psi(x)\sim x$. Since $\lim_{x\to\infty}\frac{\psi(x)}{x}=1$, given $\epsilon>0$ there exists $A>0$ such that

$$\left|\frac{\psi(x)}{x}-1\right| < \epsilon \quad \text{for all} \quad x\geq A.$$

This implies that

$$|\psi(x)-x| < \epsilon \quad \text{for all} \quad x\geq A. \tag{2.40}$$

Choose $x\geq A$. Let $y=\left[\frac{x}{A}\right]$. We have

$$\begin{aligned}\underbrace{-H(x)}_{I} &= \sum_{n\leq x}\mu(n)\psi\left(\frac{x}{n}\right)\\ &= \underbrace{\sum_{n\leq y}\mu(n)\psi\left(\frac{x}{n}\right)}_{I_1} + \underbrace{\sum_{y<n\leq x}\mu(n)\psi\left(\frac{x}{n}\right)}_{I_2}\end{aligned} \tag{2.41}$$

Now

$$\begin{aligned}n\leq y \Rightarrow n &\leq \left[\frac{x}{A}\right] < \frac{x}{A}\\ \Rightarrow A &\leq \frac{x}{n}.\end{aligned}$$

Hence from equation (2.40) we have

$$\left|\psi\left(\frac{x}{n}\right)-\frac{x}{n}\right| < \frac{x}{n}\epsilon \quad \text{for all} \quad n\leq y.$$

Consider

$$\begin{aligned} I_1 &= \sum_{n\leq y} \mu(n)\psi\left(\frac{x}{n}\right) \\ &= \sum_{n\leq y} \mu(n)\left[\frac{x}{n} + \psi\left(\frac{x}{n}\right) - \frac{x}{n}\right] \\ &= x\sum_{n\leq y}\frac{\mu(n)}{n} + \sum_{n\leq y}\mu(n)\left[\psi\left(\frac{x}{n}\right) - \frac{x}{n}\right] \end{aligned}$$

Therefore

$$\begin{aligned} |I_1| &\leq y\sum_{n\leq y}\left|\frac{\mu(n)}{n}\right| + \sum_{n\leq y}|\mu(n)|\left|\psi\left(\frac{x}{n}\right) - \frac{x}{n}\right| \\ &\leq x(1) + \sum_{n\leq y}\frac{x}{n}\,\epsilon \\ &= x + x\sum_{n\leq y}\frac{1}{n}\epsilon < x + x\epsilon\int_1^y \frac{1}{x}dx \\ &= x + \epsilon x(\log y - 1) < x + \epsilon x(\log y + 1) \\ &< x + \epsilon x(\log x + 1) \end{aligned}$$

Consider the integral

$$I_2 = \sum_{y<n\leq x}\mu(n)\psi\left(\frac{x}{n}\right)$$

Now

$$\begin{aligned} y < n \leq x &\Rightarrow \left[\frac{x}{A}\right] < n \leq [x] \\ &\Rightarrow \left[\frac{x}{A}\right] + 1 \leq n \\ &\Rightarrow y + 1 \leq n \\ &\Rightarrow \frac{1}{y+1} \geq \frac{1}{n} \\ &\Rightarrow \frac{x}{y+1} \geq \frac{x}{n} \end{aligned} \tag{2.42}$$

Also

$$y \leq \frac{x}{A} < y + 1 \Rightarrow \frac{A}{x} > \frac{1}{y+1} \tag{2.43}$$

From equations (2.42) and (2.43), we have

$$\frac{x}{n} \leq \frac{x}{y+1} < A.$$

Since ψ is an increasing function, we have

$$\psi\left(\frac{x}{n}\right) < \psi(A).$$

Therefore

$$\begin{aligned} |I_2| &< \left| \sum_{y<n\leq x} \mu(n)\psi\left(\frac{x}{n}\right) \right| \\ &< x\psi(A). \end{aligned}$$

Hence

$$\begin{aligned} |H(x)| &\leq |I_1| + |I_2| \\ &< x + \epsilon x(\log x + 1) + x\psi(A) \ \text{ if } \ x \geq A \\ &= \epsilon x \log x + (2 + \psi(A))x. \end{aligned}$$

Dividing throughout by $x \log x$, we obtain:

$$\frac{|H(x)|}{x \log x} < \epsilon + \frac{2 + \psi(A)}{\log x} \ \text{ for all } \ x \geq A. \tag{2.44}$$

Note that

$$\lim_{x\to\infty} \frac{2 + \psi(A)}{x \log x} = 0.$$

This implies that there exists $B > 0$ such that

$$\frac{2 + \psi(A)}{x \log x} < \epsilon \ \text{ for all } \ x \geq B. \tag{2.45}$$

Hence

$$\frac{|H(x)|}{x \log x} < \epsilon + \epsilon \ \text{ for all } \ x \geq \max\{A, B\}. \tag{2.46}$$

This implies that

$$\lim_{x\to\infty} \frac{H(x)}{x \log x} = 0.$$

□

Definition 2.8.3. *We say that f is little oh of g as $x \to \infty$($f = o(g)$ as $x \to \infty$) if*

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$$

Remark 11. $\lim \frac{M(x)}{x} = 0$ *implies that* $M(x) = o(x)$ *as* $x \to \infty$.

Theorem 2.8.3. *The relation*

$$M(x) = o(x) as x \to \infty$$

implies that $\psi(x) \sim x$ *as* $x \to \infty$.

Proof. Consider

$$[x] - \psi(x) - 2C,$$

where C is the Euler constant. now

$$\begin{aligned}[x] - \psi(x) - 2C &= \sum_{n\leq x} 1 - \sum_{n\leq x} \Lambda(n) - 2c \sum_{n\leq x} \left[\frac{1}{n}\right] \\ &= \sum_{n\leq x} \left(1 - \Lambda(n) - 2c\left[\frac{1}{n}\right]\right) \end{aligned} \tag{2.47}$$

We have

$$\sigma_0(n) = \sum_{n\leq x} 1$$

Therefore by Mobius inversion formula

$$1 = \sum_{d|n} \mu(d)\sigma_0\left(\frac{n}{d}\right) \tag{2.48}$$

Also we have

$$\Lambda(n) = \sum_{d|n} \mu(d)\log\left(\frac{n}{d}\right) \tag{2.49}$$

$$\left[\frac{1}{n}\right] = \sum_{d|n} \mu(d) \tag{2.50}$$

Using equations (2.48), (2.49) and (2.50) in equation (2.47) we obtain

$$\begin{aligned}[x] - \psi(x) - 2C &= \sum_{n\leq x}\sum_{d|n} \{\mu(d)\sigma_0\left(\frac{n}{d}\right) - \mu(d)\log\left(\frac{n}{d}\right) - 2C\mu(d)\} \\ &= \sum_{n\leq x}\sum_{d|n} \mu(d)\{\sigma_0\left(\frac{n}{d}\right) - \log\left(\frac{n}{d}\right) - 2C\} \\ &= \sum_{\substack{q,d \\ qd\leq x}} \mu(d) \underbrace{\{\sigma_0\left(\frac{n}{d}\right) - \log\left(\frac{n}{d}\right) - 2C\}}_{f(q)} \\ &= \sum_{\substack{q,d \\ qd\leq x}} \mu(d) f(q). \end{aligned} \tag{2.51}$$

Claim: $\sum_{\substack{q,d \\ qd\leq x}} \mu(d)f(q) = o(x)$ as $x \to \infty$.

By theorem 1.2.11 we can write $\sum_{\substack{q,d \\ qd\leq x}} \mu(d)f(q)$ in the following form:

$$\underbrace{\sum_{\substack{q,d \\ qd\leq x}} \mu(d)f(q)}_{I} = \underbrace{\sum_{n\leq b} \mu(n)F\left(\frac{x}{n}\right)}_{I_1} + \underbrace{\sum_{n\leq a} f(n)M\left(\frac{x}{n}\right)}_{I_2} - \underbrace{F(a)M(b)}_{I_3},$$

where a and b are any positive numbers such that $ab = x$ and

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

Now

$$\begin{aligned}
F(x) &= \sum_{n\leq x} f(n) \\
&= \sum_{n\leq x} [\sigma_0(n) - \log n - 2C] \\
&= \sum_{n\leq x} \sigma_0(n) - \sum_{n\leq x} \log n - 2C \sum_{n\leq x} 1 \\
&= [x\log x + (2C-1)x + O(\sqrt{x})] - [x\log x - x + O(\log x)] - 2C[x + O(1)] \\
&= O(\sqrt{x}) + O(\log x) + O(1) \\
&= O(\sqrt{x}) + O(\sqrt{x}) + O(\sqrt{x}) \\
&= O(\sqrt{x}).
\end{aligned}$$

Hence

$$F(x) = O(\sqrt{x}).$$

This implies that there exists $B > 0$ such that

$$|F(x)| \leq B\sqrt{x} \quad \text{for} \quad x \geq 1. \tag{2.52}$$

Now

$$\begin{aligned}
|I_1| = \left|\sum_{n\leq b} \mu(n)F\left(\frac{x}{n}\right)\right| &\leq \sum_{n\leq x} \left|F\left(\frac{x}{n}\right)\right| \\
&\leq B\sum_{n\leq b} \sqrt{\frac{x}{n}} = B\sqrt{x}\sum_{n\leq x} \frac{1}{\sqrt{n}} \\
&\leq B\sqrt{x}\int_1^b \frac{1}{\sqrt{t}}dt = 2B[\sqrt{b} - 1] < 2B\sqrt{x}\sqrt{b} \\
&= A\sqrt{x}\sqrt{b} = \frac{Ax}{\sqrt{a}} < \epsilon x \quad \text{if} \quad \frac{A}{\sqrt{a}} < \epsilon
\end{aligned}$$

Hence

$$|I_1| < \epsilon x.$$

By hypothesis

$$\lim_{x\to\infty} \frac{M(x)}{x} = 0.$$

Then corresponding to the same $\epsilon > 0$ there exits $c > 0$ such that

$$\frac{|M(x)|}{x} \leq \frac{\epsilon}{K} \quad \text{for} \quad x \geq c,$$

where $K = \sum_{n\leq x} \frac{|f(n)|}{n}$. Now

$$\begin{aligned} |I_2| = |\sum_{n\leq a} f(n) M\left(\frac{x}{n}\right)| & \\ &\leq \sum_{n\leq x} |f(n)||M(x/n)| \\ &\leq \sum_{n\leq x} |f(n)| \left(\frac{x}{n}\right) \frac{\epsilon}{K} \quad \text{for} \quad \frac{x}{n} \geq c \\ &= \epsilon \quad \text{for} \quad \frac{x}{n} \geq c. \end{aligned}$$

Hence

$$|I_2| < \epsilon \quad \text{for} \quad x \geq ac.$$

Now

$$\begin{aligned} |I_3| &= |F(a)||M(b)| \\ &\leq B\sqrt{a}\sqrt{b} \quad (\because |F(x)| \leq B\sqrt{x}, |M(x)| < \sqrt{x}) \\ &\leq 2B\sqrt{a}\sqrt{b} = A\sqrt{ab} < A\sqrt{a}b < (\sqrt{a}\epsilon)\sqrt{a}b = \epsilon ab = \epsilon x \end{aligned}$$

Hence

$$|I_3| < \epsilon x$$

Thus

$$|I| < 3x\epsilon.$$

provided $x > a$ and $x > ac$. □

Theorem 2.8.4. *If*

$$A(x) = \sum_{n\leq x} \frac{\mu(n)}{n}$$

the relation

$$A(x) = o(1) \quad as \quad x \to \infty$$

implies prime number theorem. In other words, the prime number theorem is a consequence of the statement that the series

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

converges and has sum 0.

Proof. It suffices to show that

$$\lim_{x\to\infty} \frac{M(x)}{x} = 0.$$

Recall the Abel's identity:

$$\sum_{y<n\leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$$

Taking $y = 1$, $f(t) = t$ and $a(n) = \frac{\mu(n)}{n}$ in Abel's identity we obtain:

$$\sum_{1<n\leq x} \frac{\mu(n)}{n} n = A(x)x - \int_1^x A(t)dt$$

That is,

$$\sum_{n\leq x} \mu(n) = A(x)x - \int_1^x A(t)dt$$

That is,

$$M(x) = A(x)x - \int_1^x A(t)dt$$

Therefore

$$\frac{M(x)}{x} = A(x) - \frac{1}{x}\int_1^x A(t)dt \tag{2.53}$$

Since $A(x) = o(1)$,

$$\lim_{x\to\infty} A(x) = 0. \tag{2.54}$$

Claim: $\lim_{x\to\infty} \frac{1}{x}\int_1^x A(t)dt = 0$. Since $\lim_{x\to\infty} A(x) = 0$, given $\epsilon > 0$ there exists $c > 0$ such that

$$|A(x)| < \epsilon \quad \forall x \geq c.$$

Now

$$\begin{aligned}\left|\frac{1}{x}\int_1^x A(t)dt\right| &= \left|\frac{1}{x}\int_1^c A(t)dt + \frac{1}{x}\int_c^x A(t)dt\right| \\ &\leq \left|\frac{1}{x}\int_1^c A(t)dt\right| + \left|\frac{1}{x}\int_c^x A(t)dt\right| \\ &= \frac{1}{x}\left|\int_1^c A(t)dt\right| + \frac{1}{x}\left|\int_c^x A(t)dt\right| \\ &\leq \frac{1}{x}\int_1^c \underbrace{|A(t)|}_{<1}dt + \frac{1}{x}\int_c^x \underbrace{|A(t)|}_{<\epsilon}dt \\ &< \frac{1}{x}(c-1) + \frac{\epsilon}{x}(x-c) = \frac{c}{x} - \frac{1}{x}\left(1+\epsilon c+\epsilon\right)\end{aligned}$$

Therefore

$$\lim_{x\to\infty}\left|\frac{1}{x}\int_1^x A(t)dt\right| = 0.$$

Hence from equation (2.53) it follows that

$$\lim_{x\to\infty}\frac{M(x)}{x} = 0.$$

This completes the proof of the theorem. □

Module 3

Quadratic Residues

In first section of this chapter, we will introduce quadratic residues of an odd prime p. In the second section we will discuss Euler's criterion, which specifies when an integer is a quadratic residue modulo p. Whether an integer n is a quadratic residue of p is indicated by a symbol called Legendre's symbol. We will also discuss properties of Legendre Symbol. In the fourth chapter we prove quadratic reciprocity law. In the last section we discuss a generalization of Legendre symbol viz Jacobi symbol.

3.1 Definition and Examples

Definition 3.1.1. *Let p be an odd prime and $(n, p) = 1$. We say that n is a quadratic residue modulo p if the equation*

$$x^2 \equiv n(mod\ p)$$

has a solution. If n is not a quadratic residue of p, we call it a quadratic non-residue modulo p.

Remark 12. *Let x be a solution of $x^2 \equiv n(mod\ p)$. Then $-x$ is also a solution of $x^2 \equiv n(mod\ p)$.*
Note that

$$(-x)^2 = (p - x)^2 = p^2 - 2px + x^2 \equiv x^2(mod\ p)$$

Example 3. *Find the quadratic residues modulo* 11.

$1^2 \equiv 1(\text{mod } 11)$	$10^2 \equiv (-1)^2 \equiv 3(\text{mod } 11)$
$2^2 \equiv 4(\text{mod } 11)$	$9^2 \equiv (-2)^2 \equiv 4(\text{mod } 11)$
$3^2 \equiv 9(\text{mod } 11)$	$8^2 \equiv (-3)^2 \equiv 9(\text{mod } 11)$
$4^2 \equiv 5(\text{mod } 11)$	$7^2 \equiv (-4)^2 \equiv 5(\text{mod } 11)$
$5^2 \equiv 3(\text{mod } 11)$	$6^2 \equiv (-5)^2 \equiv 3(\text{mod } 11)$

Hence the quadratic residues mod 11 are $1, 3, 4, 5, 9$, and the non residues are $2, 6, 7, 8, 10$.

Remark 13. *Since $(-x)^2 \equiv x^2 (mod\ p)$, to find the quadratic residues mod p we need only consider x^2, $0 < x < [p/2]$.*

Remark 14. *The nonzero residues (mod p) can be listed as:*

$$\mathbb{Z}_p^\times = \{1, 2, 3, \ldots, p-1\}.$$

Note that $\mathbb{Z}_p^\times$ is a group under multiplication. The elements of $\mathbb{Z}_p^\times$ can be written as:

$$\begin{aligned}\mathbb{Z}_p^\times &= \{\underbrace{1, 2, 3, \ldots, (p-1)/2}_{<p/2}, \underbrace{(p+1)/2, \ldots, p-1}_{>p/2}\} \\ &= \{1, 2, 3, \ldots, (p-1)/2, p-(p-1)/2, p-(p-3)/2 \ldots, p-1\} \\ &= \{j, p-j : j = 1, 2, 3, \ldots, (p-1)/2\}\end{aligned}$$

Moreover, $p - j \equiv -j (mod\ p)$. Thus,

$$\begin{aligned}\mathbb{Z}_p^\times &= \left\{\pm j : 1 \leq j \leq \frac{p-1}{2}\right\} \\ &. = \left\{-\frac{p-1}{2}, -\frac{p-2}{2}, \ldots, -1, 1, 2, \ldots, \frac{p-1}{2}\right\}\end{aligned}$$

Hence

$$\left\{|a_j| : a_j \in \mathbb{Z}_p^\times\right\} = \left\{1, 2, 3, \ldots, \frac{p-1}{2}\right\}$$

Observe that

$$\frac{p+1}{2} \leq x \leq p-1 \Leftrightarrow 1 \leq p - x \leq \frac{p-1}{2}$$

Theorem 3.1.1. *If a and b are quadratic residues mod p, then so is ab.*

Proof. Suppose

$$a \equiv r^2 (\text{mod } p), b \equiv r^2 (\text{mod } p)$$

Then

$$ab \equiv (rs)^2 (\text{mod } p).$$

This completes the proof. □

Theorem 3.1.2. *Let p be a prime. Then every reduced residue system mod p:*

$$\mathbb{Z}_p^\times = \{1, 2, \ldots, (p-1)\}$$

contains exactly $\frac{p-1}{2}$ quadratic residues and exactly $\frac{p-1}{2}$ quadratic nonresidues. Moreover the quadratic residues are

$$\left\{1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\}$$

Proof. Note that $\mathbb{Z}_p^\times$ is a field. Let Q denote the set of quadratic residues mod p. Define a map $\varphi\colon \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ by

$$\varphi(r) = r^2 (\text{mod } p)$$

Then

$$\begin{aligned}\ker(\varphi) &= \{x \in \mathbb{Z}_p^\times : \varphi(x) = 1\} \\ &= \{x \in \mathbb{Z}_p^\times : r^2 \equiv 1 (\text{mod } p)\} \\ &= \{1, -1\}.\end{aligned}$$

Also

$$\begin{aligned}\text{im}(\varphi) &= \{r \in \mathbb{Z}_p^\times : \varphi(x) = r\} \\ &= \{r : r \equiv x^2 (\text{mod } p)\} \\ &= Q.\end{aligned}$$

By the first isomorphism theorem of group theory,

$$|\ker(\varphi)||\text{im}(\varphi)| = |\mathbb{Z}_p^\times|$$

That is

$$2|Q| = \frac{p-1}{2}$$

Threfore $|Q| = \frac{p-1}{2}$. This implies that the number of quadratic nonresidues in $\mathbb{Z}_p^\times$ is also $\frac{p-1}{2}$. Since $\mathbb{Z}_p^\times$ is a group, $x^2 (\text{mod } p) \in \mathbb{Z}_p^\times$ for $x = 1, 2, \cdots, (p-1)/2$. Next, we will show that $1^2, 2^2, 3^2, \ldots, ((p-1)/2)^2$ are all distinct.
Assume that

$$\begin{aligned}&x^2 \equiv y^2 (\text{mod } p), 1 \leq x, y \leq \frac{p-1}{2} \\ \Rightarrow &(x-y)(x+y) \equiv (\text{mod } p) \\ \Rightarrow &(x-y) \equiv (\text{mod } p) (\because 1 < x+y < p) \\ \Rightarrow &x \equiv y (\text{mod } p).\end{aligned}$$

□

3.2 Legendre's symbol and its properties

The Legendre symbol is a convenient notation to indicate whether an integer n is a quadratic residue modulo of an odd prime p. The Legendre symbol of n modulo p is denoted by $(a \mid p)$.

Definition 3.2.1. *Let p be an odd prime. We define Legendre's symbol $(n|p)$ as follows:*

$$(n \mid p) = \begin{cases} 0 & \text{if } p \text{ divides } n; \\ 1 & \text{if } n \text{ is a quadratic residue modulo } p; \\ -1 & \text{if } n \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

Theorem 3.2.1. *(**Euler's criterion**)Let p be an odd prime. Then for all n we have*

$$(n \mid p) \equiv n^{(p-1)/2}(mod\ p).$$

Proof.

Case 1: Suppose n is a multiple of p. In this case $(n|p) = 0$ and $n^{(p-1)/2} \equiv 0(\text{mod } p)$. Hence the result is obvious if n is a multiple of p.

Case 2: Assume that $(n \mid p) = 1$.
Since n is a quadratic residue modulo p, we have

$$n \equiv m^2(\text{mod } p), \text{for some integer } m$$

This implies that

$$\begin{aligned} n^{(p-1)/2} &\equiv m^{p-1}(\text{mod } p) \\ &\equiv 1(\text{mod } p) \text{ (By Fermat's Theorem)} \end{aligned}$$

Hence

$$n^{(p-1)/2} \equiv (n|p)(\text{mod } p)$$

Case 3: Suppose that $(n \mid p) = -1$.
In this case n is not a quadratic residue mod p. Consider the polynomial

$$f(x) \equiv x^{(p-1)/2} - 1(\text{mod } p). \tag{3.1}$$

Claim 1:$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are roots of equation(3.1)
For $x = 1, 2, \ldots, (p-1)/2$, we have

$$\left(x^2\right)^{(p-1)/2} = x^{p-1} \equiv 1(\text{mod } p) \text{ (by Fermats theorem)}$$

Thus every quadratic residues in $\mathbb{Z}_p^\times$ is a root of equation(3.1). Since $\mathbb{Z}_p^\times$ is a field, the equation $f(x) \equiv x^{(p-1)/2} - 1(\text{mod } p)$ has at most $(p-1)/2$ solutions. Note that $\mathbb{Z}_p^\times$ contains $(p-1)/2$ quadratic residues, viz, $1^2, 2^2, \ldots, ((p-1)/2)^2$. Hence the equation $f(x) = x^{(p-1)/2} - 1$ has exactly $(p-1)/2$ solutions in $\mathbb{Z}_p^\times$. So quadratic nonresidue is not a root of the polynomial $f(x) = x^{(p-1)/2} - 1$.
Claim 2: $x^{(p-1)/2} \equiv \pm 1(\text{mod } p)$.
By Fermats theorem we have

$$x^{p-1} \equiv 1(\text{mod } p)$$

The above equation can be written as:

$$\left(x^{(p-1)/2} - 1\right)\left(x^{(p-1)/2} + 1\right) \equiv 0(\text{mod } p)$$

This implies that

$$x^{(p-1)/2} \equiv \pm 1(\text{mod } p).$$

If n is a quadratic residue modulo p, then by claim 1, $n^{(p-1)/2} \equiv 1(\text{mod } p)$. Therefore, if n is not a quadratic residue modulo p, we must have $x^{(p-1)/2} \equiv -1(\text{mod } p)$. Hence

$$n^{(p-1)/2} \equiv (n \mid p)(\text{mod } p)$$

This completes the proof. □

Theorem 3.2.2. *Legendre's symbol $(n|p)$ is a completely multiplicative function.*

Proof. Let $f(n) = (n \mid p)$, for all $n \in \mathbb{N}$.

Case 1: Suppose $p \mid m$ or $p \mid n$.
Then $p \mid mn$. In this case $(m \mid p)(n \mid p) = 0$ and $(mn \mid p) = 0$. Hence

$$(mn \mid p) = (m \mid p)(n \mid p).$$

Case 2: Suppose $p \nmid m$ and $p \nmid n$.
Note that

$$\begin{aligned}(mn|p) &\equiv (mn)^{(p-1)/2}(\text{mod } p)(\text{by Eulers criteria}) \\ &\equiv m^{(p-1)/2}n^{(p-1)/2}(\text{mod } p) \\ &\equiv (m \mid p)(n \mid p)(\text{mod } p)(\text{by Eulers criteria})\end{aligned}$$

Therefore

$$(mn \mid p) - (m \mid p)(n \mid p) \equiv 0(\text{mod } p). \tag{3.2}$$

Note that $(m \mid p), (n \mid p), (mn \mid p) \in \{0, 1, -1\}$. So

$$(mn \mid p) - (m \mid p)(n \mid p) \in \{0, 2, -2\}.$$

Since p is an odd prime and $(mn \mid p) - (m \mid p)(n \mid p)$ is divislble by p(see (3.2)) it follows that $(mn \mid p) - (m \mid p)(n \mid p) = 0$. Hence

$$(mn \mid p) = (m|p)(n \mid p).$$

That is

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

This completes the proof. □

3.3 Evalution of $(-1 \mid p)$ and $(2 \mid p)$

Theorem 3.3.1. *For every odd prime p we have*

$$(-1 \mid p) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1(\text{mod } 4) \\ -1 & \text{if } p \equiv 3(\text{mod } 4) \end{cases}$$

Proof. By Euler's criterion,

$$(-1 \mid p) \equiv (-1)^{(p-1)/2} (\text{mod } p)$$

Equivalently,

$$(-1 \mid p) - (-1)^{(p-1)/2} \equiv 0 (\text{mod } p)$$

Note that $(-1 \mid p) \in \{1, -1\}$ and $(-1)^{(p-1)/2} \in \{1, -1\}$. So

$$(-1 \mid p) - (-1)^{(p-1)/2} \in \{0, 2, -2\}$$

Since p is an odd prime, we have $(-1 \mid p) - (-1)^{(p-1)/2} = 0$. Equivalently

$$(-1 \mid p) = (-1)^{(p-1)/2}$$

Now

$$\begin{aligned}(-1 \mid p) = 1 &\Leftrightarrow (-1)^{(p-1)/2} = 1 \\ &\Leftrightarrow (p-1)/2 = 2m \text{ for some } m \in \mathbb{Z} \\ &\Leftrightarrow p = 1 + 4m \\ &\Leftrightarrow p \equiv 1 (\text{mod } 4)\end{aligned}$$

Also,

$$\begin{aligned}(-1 \mid p) = -1 &\Leftrightarrow (-1)^{(p-1)/2} = -1 \\ &\Leftrightarrow (p-1)/2 = 2m + 1 \text{ for some } m \in \mathbb{Z} \\ &\Leftrightarrow p = 3 + 4m \\ &\Leftrightarrow p \equiv 3 (\text{mod } 4)\end{aligned}$$

This completes the proof. □

Theorem 3.3.2. *For every odd prime p we have*

$$(2 \mid p) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv \pm 1 (mod\ 8) \\ -1 & \text{if } p \equiv \pm 3 (mod\ 8) \end{cases}$$

Proof. Consider the following $(p-1)/2$ congruences:

$$\begin{aligned} p - 1 &\equiv 1(-1)^1 (\text{mod } p) \\ 2 &\equiv 2(-1)^2 (\text{mod } p) \\ p - 3 &\equiv 3(-1)^3 (\text{mod } p) \\ 4 &\equiv 4(-1)^4 (\text{mod } p) \\ &\vdots \\ r &\equiv \frac{p-1}{2} (-1)^{(p-1)/2} (\text{mod } p) \end{aligned}$$

where $r = p + 1/2$ or $(p-1)/2$.
Multiply the above congruences, we obtain:

$$2 \cdot 4 \cdot 6 \cdots (p-1) \equiv \left(\frac{p-1}{2}\right)!(-1)^{1+2+\cdots+(p-1)/2} (\text{mod } p)$$

This gives us:

$$2^{(p-1)/2} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!(-1)^{(p^2-1)/8} (\text{mod } p)$$

This implies that

$$2^{(p-1)/2} \equiv (-1)^{(p^2-1)/8} (\text{mod } p)$$

By Eulers criterion,

$$(2 \mid p) \equiv 2^{(p-1)/2} \equiv (-1)^{(p^2-1)/8} (\text{mod } p) \tag{3.3}$$

Case 1 Suppose $p \equiv \pm 1 (\text{mod } 8)$.
Then $p \pm 1 = 8m$ for some $m \in \mathbb{Z}$. So $p = 8m \pm 1$. Hence

$$p^2 = (8m \pm 1)^2 = 64m^2 \pm 16m + 1$$

Consequently, $(p^2 - 1)/8 = 0$. Thus $(-1)^{(p^2-1)/8} = (-1)^0 = 1$.

Case 2 Suppose $p \equiv \pm 3 (\text{mod } 8)$.
Then $p \pm 3 = 8m$ for some $m \in \mathbb{Z}$. So $p = 8m \pm 3$. Therefore

$$p^2 = (8m \pm 3)^2 = 64m^2 \pm 48m + 9$$

Hence

$$\frac{p^2 - 1}{8} \equiv 1 (\text{mod } 8)$$

Thus $(-1)^{(p^2-1)/8} = (-1)^1 = -1$.

□

Theorem 3.3.3. *(Gauss' lemma)Let p be an odd prime and let $n \in \mathbb{Z}$ with $(n, p) = 1$. Consider the set:*

$$S = \left\{n, 2n, 3n, \ldots, \left(\frac{p-1}{2}\right) n\right\}$$

and let

$$jn \equiv a_j (mod\ p),\ 1 \leq j \leq \left(\frac{p-1}{2}\right)$$

Let m be the number of a_j's which are negative. In other words, let m denote the number of integers in the set S whose residues (mod p) are greater than $p/2$. Then

$$(n \mid p) = (-1)^m.$$

Proof. Note that

$$a_j \in \mathbb{Z}_p^\times, j = 1, 2, \ldots, (p-1)/2.$$

First we prove that $a_1, a_2, \ldots, a_{(p-1)/2}$ are all distinct.
For $1 \leq j \leq \frac{p-1}{2}$,

$$\begin{aligned} a_j \equiv a_k (\text{mod } p) &\Leftrightarrow jn \equiv kn (\text{mod } p) \\ &\Leftrightarrow (jn - kn) \equiv 0 (\text{mod } p) \\ &\Leftrightarrow (j-k)n \equiv 0 (\text{mod } p) \\ &\Leftrightarrow (j-k) \equiv 0 (\text{mod } p) (\because (p,n) = 1) \\ &\Leftrightarrow j = k. \end{aligned}$$

Hence $a_1, a_2, \ldots, a_{(p-1)/2}$ are all distinct.
Also note that

$$\begin{aligned} \mathbb{Z}_p^\times &= \left\{1, 2, 3, \ldots, \frac{p-1}{2}, \frac{p+1}{2}, \ldots, p-1\right\} \\ &= \left\{1, 2, 3, \ldots, \frac{p-1}{2}, p - \frac{p-1}{2}, p - \frac{p-3}{2} \ldots, p-1\right\} \\ &= \left\{j, p-j : j = 1, 2, 3, \ldots, \frac{p-1}{2}\right\} \\ &= \left\{\pm j : 1 \leq j \leq \frac{p-1}{2}\right\} (\because p - j \equiv -j (\text{mod } p)) \\ &= \left\{-\frac{p-1}{2}, -\frac{p-2}{2}, \ldots, -1, 1, 2, \ldots, \frac{p-1}{2}\right\} \end{aligned}$$

Since $\{a_1, a_2, \ldots, a_{(p-1)/2}\} \subset \mathbb{Z}_p^\times$, and a_i's are distinct we have

$$\left\{|a_j| : 1 \leq j \leq \frac{p-1}{2}\right\} = \left\{1, 2, 3, \ldots, \frac{p-1}{2}\right\}$$

Now

$$n(2n)(3n)\cdots\left(\frac{p-1}{2}\right)n \equiv a_1 a_2 \cdots a_{(p-1)/2} (\text{mod } p)$$

This implies

$$n^{(p-1)/2} 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) \equiv (-1)^m 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) (\text{mod } p)$$

That is,

$$n^{(p-1)/2} \left(\frac{p-1}{2}\right)! \equiv (-1)^m \left(\frac{p-1}{2}\right)! (\text{mod } p)$$

This implies that

$$n^{(p-1)/2} \equiv (-1)^m (\text{mod } p)$$

This completes the proof. □

Example 4. *Let us consider $p = 13$ and $n = 5$. Then*

$$\begin{aligned} S &= \left\{n, 2n, 3n, \ldots, \left(\frac{p-1}{2}\right)n\right\} (mod\ 13) \\ &= \{5, 2\times 5, 3\times 5, 4\times 5, 5\times 5, 6\times 5\}\ (mod\ 13) \\ &= \{5, 10, 2, 7, 12, 4\} = \{\underbrace{2, 4, 5}_{<p/2}, \underbrace{7, 10, 12}_{>p/2}\} \\ &= \{\underbrace{2, 4, 5}_{0<r<p/2}, \underbrace{-6, -3, -1}_{-p/2<r<0}\} \end{aligned}$$

Therefore $(5|13) = (-1)^3 = -1$.

Theorem 3.3.4. *Let m be the number defined in Gauss' lemma. Then*

$$m \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right] + (n-1)\frac{p^2-1}{8} (mod\ 2).$$

If n is odd,

$$m \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right] (mod\ 2).$$

Proof. Let

$$S = \left\{n, 2n, 3n, \ldots, \left(\frac{p-1}{2}\right)n\right\}$$

For $t = 1, 2, \ldots, (p-1)/2$, write

$$\frac{tn}{p} = \left[\frac{tn}{p}\right] + \left\{\frac{tn}{p}\right\},$$

where $0 < \left\{\frac{tn}{p}\right\} < 1$.[Note that $\{x\} = x - [x]$ for all $x \in \mathbb{R}$ with $0 \leq \{x\} < 1$ and $\{x\} = 0$ if and only if x is an integer]
So for $t = 1, 2, \ldots, (p-1)/2$

$$\begin{aligned} tn &= p\left[\frac{tn}{p}\right] + p\left\{\frac{tn}{p}\right\} \\ &= p\left[\frac{tn}{p}\right] + r_t, \end{aligned} \tag{3.4}$$

where $r_t \in \mathbb{Z}_p^\times$. Note that r_t is nothing but the remainder in the Euclidean division of tn by p. Let

$$\begin{aligned} A &= \{r_t : r_t < p/2\} = \{a_1, a_2, \ldots, a_k\} \\ B &= \{r_t : r_t > p/2\} = \{b_1, b_2, \ldots, b_m\}. \end{aligned}$$

Then $k+m=\frac{p-1}{2}$ and $A\cup B=\{r_1,r_2,\ldots,r_{(p-1)/2}\}$. That is,

$$\{r_1,r_2,\ldots,r_{(p-1)/2}\}=\{a_1,a_2,\ldots,a_k,b_1,b_2,\ldots,b_m\} \tag{3.5}$$

Note that

$$\begin{aligned} p/2<b_i<p &\Rightarrow -p/2>-b_i>-p \\ &\Rightarrow p-p/2>p-b_i>-p+p \\ &\Rightarrow 0<p-b_i<p/2. \end{aligned}$$

Therefore

$$\begin{aligned} \left\{1,2,3,\ldots,\frac{p-1}{2}\right\} &= \{a_1,a_2,\ldots,a_k,\underbrace{p-b_1}_{c_1},\underbrace{p-b_2}_{c_2},\ldots,\underbrace{p-b_m}_{c_m}\} \\ &= \{\underbrace{a_1,a_2,\ldots,a_k}_{0<r_t<p/2},\underbrace{c_1,c_2,\ldots,c_m}_{0<r_t<p/2}\} \end{aligned} \tag{3.6}$$

Now, summing Equation (3.4) from 1 to $(p-1)/2$, we get:

$$n\sum_{t=1}^{(p-1)/2}t=p\underbrace{\sum_{t=1}^{(p-1)/2}\left[\frac{tn}{p}\right]}_{S(n,p)}+\sum_{t=1}^{(p-1)/2}r_t$$

$$\begin{aligned} n\frac{p^2-1}{8} &= pS(n,p)+\sum_{i=1}^{k}a_i+\sum_{i=1}^{m}b_i \\ &= pS(n,p)+\sum_{i=1}^{k}a_i+\sum_{i=1}^{m}(p-c_i) \\ &= pS(n,p)+\sum_{i=1}^{k}a_i+mp-\sum_{i=1}^{m}c_i \\ &\equiv pS(n,p)+\left(\sum_{i=1}^{k}a_i+\sum_{i=1}^{m}c_i\right)+mp(\mathrm{mod}\ 2)(\because -1\equiv 1(\mathrm{mod}\ 2)) \\ &\equiv pS(n,p)+\sum_{t=1}^{(p-1)/2}t+mp(\mathrm{mod}\ 2) \\ &\equiv pS(n,p)+\frac{p^2-1}{8}+mp(\mathrm{mod}\ 2). \end{aligned}$$

This implies that

$$mp\equiv -pS(n,p)+(n-1)\frac{p^2-1}{8}(\mathrm{mod}\ 2)$$

Hence

$$m \equiv S(n,p) + (n-1)\frac{p^2-1}{8} (\text{mod } 2) \quad (\because p \equiv 1(\text{mod } 2), -1 \equiv 1(\text{mod } 2)$$

If n is odd, then $n - 1 \equiv 0(\text{mod } 2)$. So

$$m \equiv \sum_{t=1}^{(p-1)/2} \left[\frac{tn}{p}\right] (\text{mod } 2).$$

□

3.4 Quadratic reciprocity law

Let p and q be distinct odd primes. The question is whether the the following pair of quadratic congruence are solvable.

$$x^2 \equiv p(\text{mod } q), y^2 \equiv q(\text{mod } p)$$

Using Legendre's symbol the question is how $(p \mid q)$ is related to $(q|p)$. Consider the following bivariate table:

q/p	3	5	7	11	13	17	19	-
3	0	-1	1	-1	+1	-1	+1	-
5	-1	0	-1	+1	-1	-1	+1	-
7	-1	-1	0	+	-1	-1	-1	-
11	+1	+1	-1	0	-1	-1	-1	-
13	+1	-1	-1	-1	0	+1	-1	-
17	-1	-1	-1	-1	+1	0	+1	-
19	-1	+1	+1	+	-1	+1	0	-
-	-	-	-	-	-	-	-	-

We observe that row-5 and column-5 are identical in the above table. Similar is the case for row-13, column-13, and row-17, column-17. There is slightly more complicated regularity in cases of 3, 7, 11, and 19. There is a flip in sign when both

$$p, q \equiv 3(\text{mod } 4).$$

If one of p or q is of the form $4k+1$, then it seems that $(p \mid q)(q \mid p) = 1$. and if both are of the form 4k + 3, then it seems that $(p \mid q)(q \mid p) = -1$. The relation was guessed by Euler and an incomplete proof was given by Legendre. Gauss rediscovered it at the age of 18 and obtained the first complete proof. In fact he gave several proofs. It is well known as Quadratic Reciprocity Law,

$$(p|q)(q|p) = (-1)^{((p-1)/2)((q-1)/2)}$$

The law states that if one of p or q has remainder 1 when divided by 4, then either both are solvable or both are unsolvable. If the remainders of both p and q are 3, then if one is solvable then the other is not.

Theorem 3.4.1. *(Quadratic Reciprocity Law) Let p and q are distinct odd primes. Then*

$$(p|q)(q|p) = (-1)^{((p-1)/2)((q-1)/2)} = \begin{cases} -1 & \text{if } p \equiv q \equiv 3(mod\ 4) \\ 1 & p \equiv 1(mod\ 4) \text{ or } q \equiv 1(mod\ 4) \end{cases}$$

Proof. (**Ferdinand Eisenstine's proof**) By Gauss' lemma we have

$$(q|p) = (-1)^m,$$

where

$$m \equiv \sum_{x=1}^{(p-1)/2} \left[\frac{xq}{p}\right] (\text{mod } 2)..$$

Similarly,

$$(p|q) = (-1)^n,$$

where

$$n \equiv \sum_{y=1}^{(q-1)/2} \left[\frac{yp}{q}\right] (\text{mod } 2).$$

Hence

$$(p|p)(q|p) = (-1)^m(-1)^n = (-1)^{m+n}.$$

Claim: $m + m = \frac{p-1}{2}\frac{q-1}{2}$
Consider the set:

$$S = \left\{(x, y) : 1 \le x \le \frac{p-1}{2}, 1 \le y \le \frac{q-1}{2}\right\}$$
$$= \text{the set of lattice points in the rectangle } \left[1, \frac{p-1}{2}\right] \times \left[1, \frac{p-1}{2}\right]$$

Clearly the number of elements in S is equal to

$$\#(S) = \frac{p-1}{2}\frac{q-1}{2}. \tag{3.7}$$

Consider the line joining $(0, 0)$ and $(p/2, q/2)$. Its equation is $y = mx$, where $m = q/p$ i.e. $py = qx$. We claim that there is no lattice point on the line $py = qx$ within S. If a lattice point (u, v) is on the line $py = qx$ within S, then $pv = qu$, implies that $q \mid pv$. But $\gcd(p, q) = 1$ and $0 < v < q$- so it is impossible. Let S_1 and S_2 be the regions of S above and below the line $py = qx$. Therefore

$$S_1 = \{(x, y) : qx < py\},$$
$$S_2 = \{(x, y) : qx > py\}.$$

Number of lattice points within S are the number of lattice points of S_1 and S_2. That is

$$S = S_1 \cup S_2.$$

We know that the number of integers in the interval $(0, py/q)$ are $[py/q]$.

(i) Note that S_1 can be written as:

$$\begin{aligned} S_1 &= \{(x,y) : qx < py\} \\ &= \bigcup_{y=1}^{\frac{q-1}{2}} \left\{(x,y) : x < \frac{py}{q}\right\} \\ &= \bigcup_{y=1}^{\frac{q-1}{2}} S_y, \end{aligned}$$

where $S_y = \left\{(x,y) : x < \frac{py}{q}\right\}$. Note that, number of lattice points in S_y is equal to number of integers in the interval $(0, py/q)$. Therefore $\#(S_y) = [py/q]$. Thus

$$\#(S_1) = \sum_{y=1}^{\frac{q-1}{2}} \#(S_y) = \sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right]$$

(ii) The number of elements in S_2 is

$$\#(S_2) = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right]$$

Hence the number of elements in S is

$$\#(S_1) + \#(S_2) = \sum_{x=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right] + \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right] = m + n \tag{3.8}$$

From eqquations (3.7) and (3.8), we have:

$$m + n = \frac{p-1}{2}\frac{q-1}{2}.$$

This completes the proof. □

3.5 Jacobi symbol

Definition 3.5.1. *Let P be an odd integer. Then Jacobi symbol $(n|P)$ is defined as:*

$$(n|P) = \begin{cases} 1 & \text{if } P = 1 \\ \prod_{i=1}^{r} (n|p_i)^{a_i} & \text{if } P = \prod_{i=1}^{r} p_i^{a_i} \end{cases}$$

Note that $(n|P) \in \{0, 1, -1\}$.

Theorem 3.5.1. *If P and Q are odd positive integers, we have*

(a) $(m \mid P)(n \mid P) = (mn \mid P)$

(b) $(n|P)(n|Q) = (n|PQ)$

(c) $(m|P) = (n|P)$ *whenever* $m \equiv n (mod\ P)$

(d) $(a^2 n|P) = (n|P)$ *whenever* $(a, P) = 1$.

Proof. (a) Let $P = p_1 p_2 \cdots p_k$, where p_i's are prime not necessarily distinct. Then

$$\begin{aligned}(m \mid P)(n \mid P) &= \prod_{i=1}^{k}(m \mid p_i)\prod_{i=1}^{k}(n \mid p_i)\\ &= \prod_{i=1}^{k}(m \mid p_i)(n \mid p_i)\\ &= \prod_{i=1}^{k}(mn \mid p_i) = (mn \mid P)\end{aligned}$$

(b) Let $P = p_1 p_2 \cdots p_k$ and $Q = q_1 q_2 \cdots q_s$, where p_i's and q_i's are primes not necessarily distinct.

$$\begin{aligned}(n|P)(n|Q) &= \prod_{i=1}^{k}(n \mid p_i)\prod_{i=1}^{s}(n \mid q_i)\\ &= (n \mid PQ)\end{aligned}$$

(c) Let $P = p_1 p_2 \cdots p_k$. Assume that $m \equiv n (\text{mod } P)$. Then $m \equiv n (\text{mod } p_i)$ for all i. Then $(m \mid p_i) = (n \mid p_i)$ for all i. Therefore

$$\prod_{i=1}^{k}(m \mid p_i) = \prod_{i=1}^{k}(m \mid p_i)$$

That is $(m \mid P) = (n|P)$.

(d)

$$\begin{aligned}(a^2 n \mid P) &= (a^2 \mid P)(n \mid P)\\ &= (a \mid P)(a \mid P)(n \mid P)\\ &= (a \mid P)^2(n \mid P)\\ &= (n \mid P)\end{aligned}$$

□

Theorem 3.5.2. *If P is an odd positive integer we have*

$$(-1|P) = (-1)^{(P-1)/2}$$

Proof. Let

$$P = p_1 p_2 \dots p_m$$

where p_i's are not necessarily distinct primes. This can also be written as

$$P = \prod_{i=1}^{m} p_i = \prod_{i=1}^{m}(1 + p_i - 1) = 1 + \sum_{i=1}^{m}(p_i - 1) + \underbrace{\sum_{i \neq j}(p_i - 1)(p_j - 1)}_{\text{divisible by 4}} + \cdots$$

Hence

$$P - 1 \equiv \sum_{i=1}^{m}(p_i - 1) (\text{mod } 4)$$

or

$$\frac{P-1}{2} \equiv \sum_{i=1}^{m} \frac{(p_i - 1)}{2} (\text{mod } 2)$$

Therefore

$$\begin{aligned}(-1|P) &= \prod_{i=1}^{m}(-1|p_i) \\ &= \prod_{i=1}^{m}(-1)^{(p_i-1)/2} \\ &= (-1)^{\sum_{i=1}^{m}(p_i-1)/2} \\ &= (-1)^{(P-1)/2}\end{aligned}$$

□

Theorem 3.5.3. *If P is an odd positive integer we have*

$$(2|P) = (-1)^{(P^2-1)/8}$$

Proof. Let

$$P = p_1 p_2 \dots p_m$$

where p_i's are not necessarily distinct primes. This can also be written as

$$P^2 = \prod_{i=1}^{m} p_i^2 = \prod_{i=1}^{m}(1 + p_i^2 - 1) = 1 + \sum_{i=1}^{m}(p_i^2 - 1) + \sum_{i \neq j} \underbrace{(p_i^2 - 1)}_{\equiv 0 (\text{mod } 8)} \underbrace{(p_j^2 - 1)}_{\equiv 0 (\text{mod } 8)} + \cdots$$

Hence

$$P^2 - 1 \equiv \sum_{i=1}^{m}(p_i^2 - 1) (\text{mod } 64)$$

or

$$\frac{P^2-1}{8} \equiv \sum_{i=1}^{m} \frac{(p_i^2-1)}{8} (\text{mod } 8)$$

This implies that

$$\sum_{i=1}^{m} \frac{(p_i^2-1)}{8} = \frac{P^2-1}{8} + 8m \text{ for some } m \in \mathbb{Z}$$

Therefore

$$\begin{aligned}(2|P) &= \prod_{i=1}^{m} (2|p_i) \\ &= \prod_{i=1}^{m} (-1)^{(p_i^2-1)/8} \\ &= (-1)^{\sum_{i=1}^{m}(p_i^2-1)/8} \\ &= (-1)^{(P^2-1)/8+8m} = (-1)^{(P^2-1)/8}\end{aligned}$$

□

Theorem 3.5.4. *(Reciprocity law for Jacobi symbols)If P and Q are positive odd integers with $(P,Q)=1$, then*

$$(P|Q)(Q|P) = (-1)^{(P-1)(Q-1)/4}$$

Proof. Let $P = p_1 p_2 \cdots p_m$ and $Q = q_1 q_2 \cdots q_n$, where the p_i and q_i are primes not necessarily distinct. Then

$$\begin{aligned}(P|Q)(Q|P) &= \left(\prod_{j=1}^{n}(P|q_j)\right)\left(\prod_{i=1}^{m}(Q|p_i)\right) \text{(By the definition of Legendre symbol)} \\ &= \left(\prod_{i=1}^{m}\left(\prod_{j=1}^{n}(p_i|q_j)\right)\right)\left(\prod_{j=1}^{n}\left(\prod_{i=1}^{m}(q_j|p_i)\right)\right) \\ &= \prod_{i=1}^{m}\prod_{j=1}^{n}(p_i|q_j)(q_j|p_i) \\ &= \prod_{i=1}^{m}\prod_{j=1}^{n}(-1)^{(p_i-1)(q_i-1)/4} \text{(By the reciprocity of Legendre symbols)} \\ &= (-1)^{\sum_{i=1}^{m}\sum_{j=1}^{n}(p_i-1)(q_j-1)/4} \\ &= (-1)^{\sum_{i=1}^{m}(p_i-1)/2\sum_{j=1}^{n}(q_j-1)/2} \\ &= (-1)^{(P-1)/2(Q-1)/2}\left(\because \sum_{i=1}^{m}\frac{(p_i-1)}{2} \equiv \frac{P-1}{2}(\text{mod } 2), \sum_{i=1}^{m}\frac{(q_i-1)}{2} \equiv \frac{Q-1}{2}(\text{mod } 2)\right).\end{aligned}$$

This completes the proof. □

Definition 3.5.2. *Equations to be solved in integers are called* Diophantine equations.

Definition 3.5.3. *The equation*

$$y^2 = x^3 + k,\ k \in \mathbb{Z} \setminus \{0\}$$

is called Mordell's equation.

A natural number-theoretic task is the description of all integral solutions to Mordell's equation. Mordell, in 1920, showed that for each $k \in \mathbb{Z}$ the equation $y^2 = x^3 + k$ has only finitely many integral solutions. The following table describes all the integral solutions for some k of Mordell's equation:

k	Integer solution	k	Integer solution
1	$(-1, 0), (0, -1), (2, -3)$	-6	None
-1	(1, 0)	7	None
-2	(3, -5)	11	None
-4	(2, -2), (5, -11)	16	(0, 4), (0, -4)
-5	None	-24	None
6	None	-26	(3, -1), (35, -207)

Theorem 3.5.5. *The Mordell's equation:*

$$y^2 = x^3 + k \tag{3.9}$$

has no integer solution if k is of the form

$$k = (4n - 1)^2 - 4m^2 \tag{3.10}$$

where m and n integers such that no prime $p \equiv -1(mod\ 4)$ divides m.

Proof. Assume there is an integral solution (x, y). Note that

$$\begin{aligned} k &= (4n-1)^3 - 4m^2 \\ &= (4n)^2 - 3(4n)^2 + 3(4n) - 1 + 4m^2 \\ &\equiv -1(\text{mod } 4) \end{aligned}$$

Hence Mordell's equation $y^2 = x^3 + k$ can be written as:

$$y^2 \equiv x^3 - 1(\text{mod } 4) \tag{3.11}$$

Here is a table of values of y^2 and $x^3 - 1$ modulo 4:

y	$y^2(\text{mod } 4)$	x	$(x^3 - 1)(\text{mod } 4)$
0	0	0	3
1	1	1	0
2	0	2	3
3	1	3	2
4	0	4	3
5	1	5	0

Note that $y^2 \equiv 0(\text{mod } 4)$ or $y^2 \equiv 1(\text{mod } 4)$.

Case 1: Suppose x is even.
Suppose $x = 2m$ for some $m \in \mathbb{Z}$. Then $x^3 - 1 = 8m^3 - 1$. Therefore $x^3 - 1 \equiv -1(\text{mod } 4)$. But $y^2 \equiv 0(\text{mod } 4)$ or $y^2 \equiv 1(\text{mod } 4)$. Hence (3.11) is not satisfied if x is even.

Case 2: Suppose x is odd.
Then we have

$$x \equiv \pm 1(\text{mod } 4)$$

Subclaim 1: Suppose $x \equiv -1(\text{mod } 4)$.
Then $x = 4m - 1$ for some $m \in \mathbb{Z}$. Then

$$x^3 - 1 = (4m-1)^3 - 1 \equiv -2(\text{mod } 4).$$

Hence eqution (3.11) is not satisfied if $x \equiv -1(\text{mod } 4)$.

Subclaim 2: Suppose $x \equiv 1(\text{mod } 4)$.
Then $x = 4m + 1$ for some $m \in \mathbb{Z}$. Then

$$x^3 - 1 = (4m+1)^3 - 1 \equiv (\text{mod } 4).$$

Hence eqution (3.11) is satisfied if $x \equiv 1(\text{mod } 4)$. Thus y is even and $x \equiv 1(\text{mod } 4)$.

Let $a = (4n - 1)$. Then equation (3.10) can be writen as:

$$k = (4n-1)^3 - 4m^2 = a^3 - 4m^2$$

Then equation (3.9) can be written as $y^2 = x^3 + a^3 - 4m^2$. or

$$y^2 + 4m^2 = x^3 + a^3 = (x+a)(x^2 - ax + a^2) \tag{3.12}$$

Now

$$\begin{aligned} x^2 - ax + a^2 &\equiv 1 - a + a^2(\text{mod } 4)(\because x \equiv 1(\text{mod } 4)) \\ &\equiv 3(\text{mod } 4)(\because a \equiv -1(\text{mod } 4)) \\ &\equiv -1(\text{mod } 4) \end{aligned}$$

Let $x^2 - ax + a^2 = p_1 p_2 \cdots p_k$, where p_i' s are primes(not necessarily distinct). Then

$$p_1 p_2 \cdots p_k \equiv -1(\text{mod } 4) \tag{3.13}$$

Equation (3.13) tells us that all its prime factors cannot be $\equiv 1(\text{mod } 4)$. There fore some prime $p_i \equiv -1(\text{mod } 4)$. We denote the prime number p_i by p. Then $p \equiv -1(\text{mod } 4)$. Now

$$p | p_1 p_2 \cdots p_k \Rightarrow p \mid x^2 - ax + a^2$$

$$
\begin{aligned}
&\Rightarrow p \mid y^2 + 4m^2 \\
&\Rightarrow y^2 + 4m^2 \equiv 0 (\text{mod } 4) \\
&\Rightarrow y^2 \equiv -4m^2 (\text{mod } 4) \\
&\Rightarrow (y^2|p) = (-4m^2|p) \\
&\Rightarrow 1 = (-4m^2|p) (\because p \nmid y) \\
&\Rightarrow 1 = (2^2|p)(m^2|p)(-1|p) \\
&\Rightarrow 1 = 1(-1|p) (\because p \nmid m) \\
&\Rightarrow 1 = -1 (\text{by theorem } 3.3.1), \text{which is absurd.}
\end{aligned}
$$

□

- $(-1)^{(n-1)/2} = 1$ if and only if $n \equiv 1 (\text{mod } 4)$
- $(-1)^{(n^2-1)/8} = 1$ if and only if $n \equiv \pm 1 (\text{mod } 8)$
- $(-1)^{(n-1)(m-1)/4} = 1$ if and only if $n \equiv 1 (\text{mod } 4)$ or $m \equiv 1 (\text{mod } 4)$

3.6 Problems

Problem 1. *Determine whether* 219 *is a quadratic residue or nonresidue mod* 383.

$$(219|383) = (3 \times 73|383) = (3|383)(73|383) (\text{theorem }) \tag{3.14}$$

$$
\begin{aligned}
(3|383) &= (383|3)(-1)^{(383-1)(3-1)/4} = -(383|3) \\
&= -(-1|3) (\because 383 \equiv -1 (\text{mod } 3)) \\
&= (-1)(-1)^{(3-1)/2} = 1 \\
(73|383) &= (383|73)(-1)^{(383-1)(73-1)/4} \\
&= (383|73) = (18|73) (\because 383 \equiv 18 (\text{mod } 73))) \\
&= (2|73)(9|73) = (2|73) = (-1)^{(73^2-1)/8} = 1
\end{aligned}
$$

Hence from equation (3.14), we have

$$(219|383) = 1$$

Hence 219 is a quadratic residue mod 383.

Problem 2. *Determine whether* 888 *is a quadratic residue or nonresidue mod* 1999.

$$\begin{aligned}(888|1999) &= (4|1999)(2|1999)(111|1999)\\ &= (1)(-1)^{(1999^2-1)/8}(111|1999)\\ &= (111|1999)\\ &= -(1999|111)(\text{by Reciprocity law})\\ &= -(1|111)(\because 1999 \equiv -1(\text{mod } 111))\\ &= -1\end{aligned}$$

Therefore 888 is a quadratic nonresidue of 1999.

Problem 3. *Determine whether* -104 *is a quadratic residue or nonresidue mod* 997.

$$\begin{aligned}(-104|997) &= (-1 \times 2 \times 13|997)\\ &= (-1|997)(2|997)(13|997)\\ &= -(13|997)\\ &= (997|13) = -(9|13) = -1\end{aligned}$$

Therefore -104 is a quadratic nonresidue of 997.

Problem 4. *Determine those odd primes* p *for which* 3 *is a quadratic residue and those for which it is a nonresidue.*

Let q be an odd prime > 3. Let $p = 3$ so we have $p = 3 \equiv 3(\text{mod}4)$. We already know

$$(p \mid q) = \begin{cases}(q \mid p) & \text{if } p \equiv 1(\text{mod } 4) \text{ or } q \equiv 1(\text{mod } 4),\\ -(q \mid p) & \text{if } p \equiv 3(\text{mod } 4) \text{ and } q \equiv 3(\text{mod } 4).\end{cases}$$

So

$$(3 \mid q) = \begin{cases}(q \mid 3) & \text{if } q \equiv 1(\text{mod } 4),\\ -(q \mid 3) & \text{if } q \equiv 3(\text{mod } 4).\end{cases}$$

But $q \equiv \pm 1(\text{mod } 3)$. If $q \equiv 1(\text{mod } 3)$, then $(q \mid 3) = (1 \mid 3) = 1$. If $q \equiv -1(\text{mod } 3)$, then $(q \mid 3) = (-1 \mid 3) = (-1)^{(3-1)/2} = -1$. Hence

$$(q \mid 3) = \begin{cases}1 & \text{if } \ q \equiv 1(\text{mod } 3)\\ -1 & \text{if } \ q \equiv -1(\text{mod } 3).\end{cases}$$

So the value of $(3 \mid q) = 1$ if and only if $[q \equiv 1(\text{mod } 4)$ and $q \equiv 1(\text{mod } 3)\ ]$ or $[q \equiv 3(\text{mod}4)$ and $q \equiv -1(\text{mod}3)]$. This is equivalent to,$(3 \mid q) = 1$ if and only if $q \equiv \pm 1(\text{mod}12)$. Moreover the value of $(3 \mid q) = -1$ if and only if $[\ q \equiv 1(\text{mod } 4)$ and $q \equiv 1(\text{mod } 3)]$ or $[\ q \equiv 3(\text{mod } 4)$ and $q \equiv 1(\text{mod } 3)]$

3.7 Exercise

1. Determine whether 219 is a quadratic residue or nonresidue mod 383.
2. Determine those odd primes p for which $(-3|p) = 1$ and those for which $(-3|p) = -1$.
3. Prove that 5 is a quadratic residue of an odd prime if $p \equiv \pm 1 (\text{mod } 10))$ and that 5 is a non residue if $p \equiv \pm 1 (\text{mod } 10))$.
4. Find all quadratic residues a mod p (in the range $-p/2 < a < p/2$) for $p = 17, 19$ and 23.
5. Use Gauss' Lemma to compute the following Legendre symbols

$$(7|11) \quad (5|13) \quad (-3|17) \quad (5|19)$$

6. Evaluate each of the following Legendre symbols using quadratic reciprocity.

$$(511|881) \quad (-257|541) \quad (221|347) \quad (105|1009)$$

Module 4

Cryptography

4.1 Introduction

The fundamental goal of cryptography is to allow two people, Alice and Bob, to exchange messages over an insecure channel in such a way that their opponent, Eve, cannot discover their content.

4.2 Terminologies

- **Plaintext:** The message you want to send, like "HELLO". The plaintext is written in some alphabet consisting of a certain number N of letters. The term "letter" (or "character") can refer not only to the familiar $A-Z$, but also to numerals, blanks, punctuation marks, or any other symbols that we allow ourselves to use when writing the messages. (If we don't include a blank, for example, then all of the words are run together, and the messages are harder to read).
- **Encryption:** The process of disguising a message in such a way as to hide its substance is encryption.
- **Ciphertext:** The disguised message, like XQABE.
- **Message unit:**The plaintext and ciphertext are broken up into message units. A message unit might be a single letter, a pair of letters (digraph), a triple of letters (trigraph), or a block of 50 letters
- **Decryption:** The process of turning ciphertext back into plaintext is decryption.
- **Encode:** The processes of converting plaintext into a number, numbers is called encloding.The first step is to "label" all possible plaintext message units and all possible ciphertext message units by means of mathematical objects from which functions can be easily constructed. These objects are

often simply the integers in some range. For example, if our plaintext and ciphertext message units are single letters from the 26-letter alphabet A-Z, then we can label the letters using the integers $0, 1, 2, \ldots, 25$, which we call their "numerical equivalents." Thus, in place of A we write 0, in place of S we write 18, in place of X we write 23, and so on. As another example, if our message units are digraphs in the 27-letter alphabet consisting of A-Z and a blank, we might first let the blank have numerical equivalent 26 (one beyond Z), and then label the digraph whose two letters correspond to $x, y \in \{0, 1, 2, \ldots, 26\}$ by the integer

$$27x + y \in \{0, 1, ..., 728\}.$$

- **Decode:** Turn number or numbers back into plaintext. There is nothing secretive about encoding and decoding.
- **Block Cipher** operates on blocks of symbols. Examples: Digraph is a pair of letters, Trigraph is a triple of letters.
- **Cryptosystem:** A pair of enciphering and deciphering algorithms. We associate the process of encryption with a one-to-one function f from plaintext message to ciphertext message, and the reverse decryption process function f^{-1} is the map from ciphering text to plain text. We can represent the situation schematically by the diagram

$$\mathbf{P} \overset{f}{\to} \mathbf{C} \overset{f^{-1}}{\to} \mathbf{P}$$

  Any such set-up is called a cryptosystem.
- **Cryptanalysis** is the process by which the enemy tries to turn cipher text into plain text.

4.3 Types of Cryptography

4.3.1 Symmetric Key Cryptography

Symmetric Key Cryptography is an encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. The Algorithm use is also known as a secret key algorithm or sometimes called a symmetric algorithm

The key for encrypting and decrypting the message had to be known to all the recipients. Else, the message could not be decrypted by conventional means.

Symmetric-key systems are simpler and faster; their main drawback is that the two parties must somehow exchange the key in a secure way and keep it secure after that. The following is one of the simplest forms of symmetric key cryptography, called the Caesar cipher. Both the sender and recipient have the "symmetric" key b.

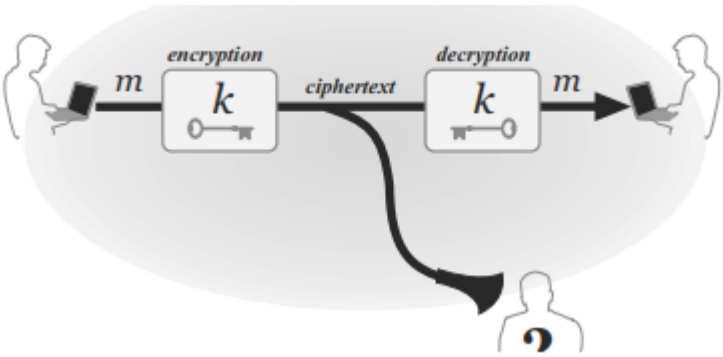


Figure 4.1: Symmetric Cryptosystem (see [11]).

We encrypt the message P by

$$C = f(P) \equiv P + b(\text{mod } N),$$

we can compute

$$P = f^{-1}(C) = C - b(\text{mod } N).$$

. For example, say we take $P = 18$ to $C = 26$, in modular $N = 32$, so we substitute P and C in the forms of $C \equiv P + b(\text{mod } N)$ and get

$$26 \equiv 18 + b(\text{mod } 32).$$

By solving for key of b, and $b = 8$ and both sender and recipient know this key. Now, when the recipient only gets the ciphertext C from the sender, he can eventually decipher the message by$P = C - b = 26 - 8 \equiv 18(\text{mod } 32)$. 2). This is correct.

4.3.2 Affine enciphering transformation

An **affine enciphering transformation** is of the form

$$C \equiv aP + b(\text{mod } N)$$

where the pair (a, b) is the encrypting key, $\gcd(a, N) = 1$.
Example: $C \equiv 13P+3(\text{mod } 26)$. Encrypt $B = 1$ or $D = 3$ and get $13\times1+3 \equiv 16$ and $13\times3+3 \equiv 16(\text{mod } 26)$. $C \equiv 3P+4(\text{mod } 26)$ is OK since $\gcd(3, 26) = 1$. In this case $F = 5$ goes to $3 \times 5 + 4 \equiv 19(\text{mod}26)$ and $19 = T$.
Decryption: Solve for P.

$$C - 4 \equiv 3P(\text{mod } 26)$$

and

$$3^{-1}(C - 4) \equiv P(mod26)$$

. Now

$$3^{-1} \equiv 9(\text{mod } 26)$$

(since $3.9 \equiv 1(\text{mod } 26)$). So $P \equiv 9(C-4) \equiv 9C - 36 \equiv 9C + 16(\text{mod } 26)$. In general encryption:

$$C \equiv aP + b(\text{mod}N)$$

and decryption:

$$P \equiv a^{-1}(C-b)(\text{mod}N)$$

. Here $(a^{-1}, -a^{-1}b)$ is the decryption key.

4.3.3 Asymmetric Key Cryptography

Asymmetric cryptography , also known as Public-key cryptography, refers to a cryptographic algorithm which requires two separate keys, one of which is private and one of which is public. The public key is used to encrypt the message and the private one is used to decrypt the message.

4.3.4 RSA cryptosystem.

The RSA cryptosystem, which was invented by Rivest, Sharmir and Adleman in 1978. RSA works based on tremendous prime numbers. The steps are shown in the following:

1. Choose large prime numbers p and q and calculate $n = pq$.
2. Recall $\varphi(n) = (p-1)(q-1)$ when $n = pq$ because p, q are primes.
3. Randomly pick e satisfying the property of $1 < e < \varphi(n)$ with $\gcd(e, \varphi(n)) = 1$.
4. Find d such that $de \equiv 1(\text{mod } \varphi(n))$ through the Euclidean algorithm.
5. At the end of the process, the public enciphering key is $k_E = (n; e)$ and private deciphering key is $k_D = (n; d)$.

Example 1:

1. Say we pick two prime numbers $p = 3863$, $q = 83$, so $n = pq = 320629$.
2. Calculate $\varphi(n) = (p-1)(q-1) = 316684$.
3. Pick $e = 997$, which satisfies gcd $(e; \varphi(n)) = 1$.
4. We need to find d such that $de \equiv 1(\text{mod}\varphi(n))$. By applying the extended Euclidean algorithm, we obtain $d = 263321$.
5. So the public enciphering key is $k_E = (320629; 997)$ and the private deciphering key is $k_D = (320629; 263321)$.

- Suppose a person A wants to send the plaintext message $P = 5$ to the person B.
- First, A encrypts the message with B's public key $k_E = (320629; 997)$ and gets the cipher text $C = 5^{997} = 145463(\text{mod } 320629)$, and only sends the ciphertext $C = 145463$ to B.
- Once B receives the ciphertext C from A.
- He applies his own private key $k_D = (320629; 263321)$ to the ciphertext $C = 145463$ and gets $145463^{263321}(\text{mod } 320629)$.
- After calculation, at the end, he gets the plaintext message $P = 5$, which is the correct plaintext.

Example 2:

- Bob choose two secrete primes $p = 7$ and $q = 17$
- Bob computes $n = p.q = 7 \times 17 = 119$.
- Bob computes $\varphi(n) = (p-1)(q-1) = 96$
- Bob chooses a public encrypition exponent e with the property that

$$gcd(e, (p-1)(q-1)) = gcd(e, 96) = 1$$

  Take $e = 5$.

- Find $d \equiv e^{-1}(\text{mod } 96)$. Then $d = 77$
- Public Key: (119, 5), Private Key: (119, 77)

RSA Encryption

- Alice converts her plaintext into an integer

$$m = 19 \text{ satisfying } 1 \leq m \leq 119.$$

- Alice uses Bob's public key $(n, e) = (119, 5)$ to compute

$$c \equiv m^e (mod\ N), c \equiv 19^5 \equiv 66(\text{mod } 119)$$

- Alice sends the ciphertext $c = 66$ to Bob.

RSA Decryption

- Bob takes the ciphertext $c = 66$ and computes

$$c^d \equiv (\text{mod } n), 66^{77} \equiv 19(mod\ 119)$$

- The value that he compute is Alice message $m = 19$.

4.3.5 Hash Functions

The ideal cryptographic hash function has four main properties

- it is easy to compute the hash value for any given message
- it is infeasible to generate a message that has a given hash
- it is infeasible to modify a message without changing the hash
- it is infeasible to find two different messages with the same hash.

4.3.6 Signatures

Authentication when people send the message, we often need to verify the identity of the sender. We often call this the signature. We can construct a digital signature similar to a physical signature while communicating the message. Suppose Alice wants to send message P to Bob. She sends her signature SA along with her message. Let f_A be the enciphering transformation for Alice and f_B be the same for Bob and make them public. First, Alice composes Bob's f_B with her own private key f_A^{-1} to obtain $f_B f_A^{-1}(SA)$. When Bob gets the message, he first applies his own private key f_B^{-1} to obtain $f_A^{-1}(SA)$. Then he applies Alice's public enciphering transformation f_A, and obtains SA. Since he can decipher the signature, he concludes this message was indeed sent by Alice.

4.3.7 One way functions

The main idea behind asymmetric-key cryptography is the concept of the trapdoor one-way function.

- f is easy to compute($y = f(x)$).
- f^{-1} is very difficult to compute($y = f^{-1}(x)$)

When n is large, $n \to p \times q$ is a one-way function. Given p and q it is always easy to calculate n; given n, it is very difficult to compute p and q. This is the factorization problem.

4.3.8 Trapdoor One-Way Function

Suppose $y = f(x)$ be a one way function. Given y and a trapdoor, x can be computed easily.
When n is large, the function $y = x^k (\text{mod } n)$ is a trapdoor one-way function. Given x, k, and n, it is easy to calculate y. Given y, k, and n, it is very difficult to calculate x. This is the discrete logarithm problem. However, if we know the trapdoor, k' such that $kk' \equiv 1 (\text{mod } \varphi(n))$, we can use $x \equiv y^{k'} (\text{mod } n)$ to find x.

4.4 Problems

Problem 5. *In the* 27 *letter alphabet(with blank =26), use affine enciphering transformation with key* $a = 13, b = 9$ *to encipher the message "HELP ME".*

The affine enciphering transformation is

$$c(P) = aP + b(mod\ 27)$$

P	$c(P) = 13P + 9$	**C**
H	$13 \times 7 + 9 = 100 \equiv 19(mod\ 27)$	T
E	$13 \times 4 + 9 = 61 \equiv 7(mod\ 27)$	H
L	$13 \times 11 + 9 = 152 \equiv 17(mod\ 27)$	R
P	$13 \times 15 + 9 = 204 \equiv 15(mod\ 27)$	P
blank	$13 \times 26 + 9 = 347 \equiv 23(mod\ 27)$	X
M	$13 \times 12 + 9 = 165 \equiv 3(mod\ 27)$	R

The required message is " THRPXDH".

Problem 6. *In a long string of ciphertext which was encrypted by means of an affine map on single-letter message units in the 26-letter alphabet, you observe that the most frequently occurring letters are "Y" and "V", in that order. Assuming that those ciphertext message units are the encryption of "E" and "T", respectively, read the message "QAOOYQQEVHEQV".*

The affine deciphering transformation is

$$P \equiv a'C + b'(mod\ 26)$$

Given that "Y" and "V" are encryptions of "E" and "T" respectively. So we have the following equations:

$$4 \equiv 24a' + b'(mod\ 26) \tag{4.1}$$

$$19 \equiv 21a' + b'(mod\ 26) \tag{4.2}$$

Subtracting equation (2) from equation (1), we obtain

$$-15 \equiv 3a'(mod\ 26)$$

This implies that

$$\begin{aligned} 11 \equiv 3a'(mod\ 26) &\Rightarrow 99 \equiv 27a'(mod\ 26) \\ &\Rightarrow 99 \equiv a'(mod\ 26) \\ &\Rightarrow 21 \equiv a'(mod\ 26) \end{aligned}$$

Putting $a' \equiv 21(mod\ 26)$ in Eqn(2), we obtain

$$4 \equiv 504 + b'(mod\ 26) \Rightarrow b' \equiv 20(mod\ 26)$$

Hence the affine deciphering transformation is

$$P \equiv 21C + 20(mod\ 26)$$

C	$P \equiv 21x + 20(mod\ 26)$	**P**
Q	$21 \times 16 + 20 = 356 \equiv 18(mod\ 26)$	S
A	$21 \times 0 + 20 = 20 \equiv 20(mod\ 26)$	U
O	$21 \times 14 + 20 = 314 \equiv 2(mod\ 26)$	C
Y	$21 \times 24 + 20 = 524 \equiv 4(mod\ 26)$	E
E	$21 \times 4 + 20 = 104 \equiv 0(mod\ 26)$	A
V	$21 \times 21 + 20 = 461 \equiv 19(mod\ 26)$	T
H	$21 \times 7 + 20 = 167 \equiv 11(mod\ 26)$	L

So the required message is

"QAOOYQQEVHEQV" $\rightarrow$ SUCEESSATLAST

Problem 7. *You are trying to cryptanalyze an affine enciphering transformation of single-letter message units in a 37-letter alphabet. This alphabet includes the numerals 0–9, which are labeled by themselves (i.e. , by the integers 0–9) . The letters A-Z have numerical equivalents 10–35, respectively, and blank=36. You intercept the ciphertext "OH7F86BB46R36270266BB9" (here the O's are the letter "oh", not the numeral zero). You know that the plaintext ends with the signature "007" (zero zero seven) . What is the message?*

The deciphering transformation is

$$P \equiv a'C + b'(mod\ 37)$$

Given that "0(zero)" and "7" are encryptions of "B" and "9" respectively. So we have the following equations:

$$0 \equiv 11a' + b'(mod\ 37) \tag{4.3}$$

$$7 \equiv 9a' + b'(mod\ 37) \tag{4.4}$$

Eqn(3)-Eqn(4) gives:

$$\begin{aligned} -7 \equiv 2a'(mod\ 37) &\Rightarrow 30 \equiv 2a'(mod\ 37) \\ &\Rightarrow 570 \equiv a'(mod\ 37) \\ &\Rightarrow 15 \equiv a'(mod\ 37) \end{aligned}$$

Putting $a' \equiv 15(mod\ 37)$ in Eqn(3), we obtain:

$$\begin{aligned} 0 \equiv 11 \times 15 + b'(mod\ 37) &\Rightarrow 0 \equiv 165 + b'(mod\ 37) \\ &\Rightarrow 0 \equiv 17 + b'(mod\ 37) \\ &\Rightarrow -17 \equiv b'(mod\ 37) \\ &\Rightarrow 20 \equiv b'(mod\ 37) \end{aligned}$$

Hence the deciphering transformation is

$$P \equiv 15C + 20(mod\ 37)$$

C	$P \equiv 21x + 20(mod\ 26)$	**P**
O	$15 \times 24 + 20 = 380 \equiv 10(mod\ 26)$	H
H	$15 \times 17 + 20 = 275 \equiv 16(mod\ 26)$	G
7	$15 \times 17 + 20 = 314 \equiv 2(mod\ 26)$	C
F	$15 \times 15 + 20 = 245 \equiv 23(mod\ 26)$	N
8	$15 \times 8 + 20 = 140 \equiv 29(mod\ 26)$	T
6	$15 \times 6 + 20 = 110 \equiv 36(mod\ 26)$	BLANK
B	$15 \times 11 + 20 = 185 \equiv 0(mod\ 26)$	L
4	$15 \times 4 + 20 = 80 \equiv 6(mod\ 26)$	A
R	$15 \times 27 + 20 = 425 \equiv 18(mod\ 26)$	1
3	$15 \times 3 + 20 = 65 \equiv 28(mod\ 26)$	S
2	$15 \times 2 + 20 = 50 \equiv 13(mod\ 26)$	D
9	$15 \times 9 + 20 = 155 \equiv 7(mod\ 26)$	7

The required message is " AGENT 006 IS DEAD 007"

Problem 8. *Suppose there is a cryptosystem with 27-letter alphabets in which A–Z have numeral equivalents* $0 - -25$*,a blank=26. Suppose a study of a large sample of ciphertexts revals that the most common diagraphs are (in order) "ZA", "IA" and "IW". Suppose that the most common digraphs in the English language (for text written in our 27-letter alphabet) are "E " (i.e. , "E blank") , "S "; " T". You know that the cryptosystem uses an affine enciphering transformation modulo 729. Find the deciphering key, and read the message "NDXBHO". Also find the enciphering key.*

We know that plaintexts are enciphered by means of the rule

$$C \equiv aP + b(mod\ 729)$$

, and that ciphertexts can be deciphered by means of the rule

$$P \equiv a'C + b'(mod\ 729)$$

, here a, b form the enciphering key, and a', b' form the deciphering key.

digraph	Numerical equivalent$(27x + y(mod\ 729))$
"ZA "	$27 \times 25 + 0 = 675(mod\ 729)$
"E "	$27 \times 4 + 26 = 134(mod\ 729)$
"IA"	$27 \times 8 + 0 = 216(mod\ 729)$
"S "	$27 \times 18 + 26 = 512(mod\ 729)$
"IW"	$27 \times 8 + 22 = 238(mod\ 729)$
" T"	$27 \times 26 + 19 = 721(mod\ 729)$

By hypothesis we have the following equations:

$$675a' + b' \equiv 134(mod\ 729) \tag{4.5}$$

$$216a' + b' \equiv 512(mod\ 729) \tag{4.6}$$

$$238a' + b' \equiv 721(mod\ 729) \tag{4.7}$$

Eqn(5)-Eqn(6) gives:

$$459a' \equiv -378(mod\ 729) \tag{4.8}$$

Note that $(459, 729) \neq 1$. So (4.8) has no solutions. Eqn(5)-Eqn(7) gives:

$$437a' \equiv -587(mod\ 729) \equiv 142(mod\ 729) \tag{4.9}$$

To find the inverse of 437 in $\mathbb{Z}_{729}$.

$$\begin{aligned}
729 &= 437 \times 1 + 292 \\
437 &= 292 \times 2 + 145 \\
292 &= 145 \times 2 + 2 \\
145 &= 2 \times 72 + 1 \\
1 &= 145 - 2 \times 72 \\
&= 145 - 72(292 - 145 \times 2) \\
&= -72 \times 292 + 145 \times 145 \\
&= -72 \times 292 + 145(437 - 1 \times 292) \\
&= 145 \times 437 - 217(729 - 1 \times 437) \\
&= 145 \times 437 - 217 \times 729 + 217 \times 437 \\
&\equiv 362 \times 437(mod\ 729)
\end{aligned}$$

Multiplying both sides of equation (9) by 362, we obtain:

$$\begin{aligned}
a' &\equiv 362 \times 142(mod\ 729) \\
&\equiv 51404(mod\ 729) \\
&\equiv 374(mod\ 729)
\end{aligned}$$

Putting $a' \equiv 374(mod\ 729)$ in equation(5), we get:

$$\begin{aligned}
b' &\equiv 134 - 675 \times 374 \\
&- 252316 = -383 \equiv 647(mod\ 729)
\end{aligned}$$

digraph	Numerical equivalents$(27x + y(mod\ 729))$
"ND "	$27 \times 13 + 3 = 354(mod\ 729)$
"XB"	$27 \times 23 + 1 = 622(mod\ 729)$
"HO"	$27 \times 7 + 14 = 203(mod\ 729)$

We have

$$P \equiv a'C + b'(mod\ 729)$$

Therefore,

$$P \equiv 374C + 647(mod\ 729)$$

$$\begin{aligned}
&\equiv 374 \times ND + 647(mod\ 729)\\
&\equiv 374 \times 354 + 647(mod\ 729)\\
&\equiv 133043(mod\ 729) \equiv 365(mod\ 729)\\
&\equiv 27 \times 13 + 14(mod\ 729) = \text{“}NO''
\end{aligned}$$

$$\begin{aligned}
P &\equiv 374C + 647(mod\ 729)\\
&\equiv 374 \times XB + 647(mod\ 729)\\
&\equiv 374 \times 662 + 647(mod\ 729)\\
&\equiv 233275(mod\ 729) \equiv 724(mod\ 729)\\
&\equiv 27 \times 26 + 22(mod\ 729) = \text{“}\ \ W''
\end{aligned}$$

$$\begin{aligned}
P &\equiv 374C + 647(mod\ 729)\\
&\equiv 374 \times HO + 647(mod\ 729)\\
&\equiv 374 \times 203 + 647(mod\ 729)\\
&\equiv 76569(mod\ 729) \equiv 724(mod\ 729)\\
&\equiv 27 \times 0 + 24(mod\ 729) = \text{“}AY''
\end{aligned}$$

The required message is “ NO WAY”. Note that $a = a'^{-1}$ and $b = -ab'$. We have

$$374 \equiv a'(mod\ 729)$$

$$\begin{aligned}
729 &= 374 \times 1 + 355\\
374 &= 355 \times 1 + 19\\
355 &= 19 \times 18 + 13\\
13 &= 6 \times 2 + 1
\end{aligned}$$

Note that $a = a'^{-1}$ and $b = -ab'$. We have $374 \equiv a'(mod\ 729)$

$$\begin{aligned}
1 &= 13 - 2 \times 6\\
&= 13 - 2(19 - 1 \times 13)\\
&= -2 \times 19 + 3 \times 13\\
&= -2 \times 19 - 3(355 - 18 \times 19)\\
&= 3 \times 355 - 56 \times 19\\
&= 3 \times 355 - 56(374 - 1 \times 355)\\
&= -56 \times 374 + 59 \times 355\\
&= -56 \times 374 - 115 \times 374\\
&= -155 \times 374(mod\ 729)
\end{aligned}$$

So $a \equiv -115(mod\ 729) \equiv 614(mod\ 729)$. Also $b = -614 \times 647 \equiv 4(mod\ 729)$.

1. Alphabet $\Rightarrow$ 27-letter Alphabet(For example A–Z, blank)
2. Plaintext $\Rightarrow$ digraphs. For example

digraph	Numerical equivalent($27x + y(mod\ 729)$)
"ZA "	$27 \times 25 + 0 = 675(mod\ 729)$
"E "	$27 \times 4 + 26 = 134(mod\ 729)$
"IA"	$27 \times 8 + 0 = 216(mod\ 729)$
"S "	$27 \times 18 + 26 = 512(mod\ 729)$
"IW"	$27 \times 8 + 22 = 238(mod\ 729)$
" T"	$27 \times 26 + 19 = 721(mod\ 729)$

Consider an N-letter alphabet.

1. Note each digraph has numerical equivalents in $\mathbb{Z}_{N^2}$
2. Instead of associating eqach digraph to element in $\mathbb{Z}_{N^2}$ we associate each digraph with a veector $[x, y]^T$ where x is the numerical equivalent of the first letter and y is the numerical equivalent of the second alphabet. For example, consider the alphabet $\mathbf{A} = \{A - -Z, blank\}$.

$$"ZA'' \Rightarrow (25, 0)^T$$
$$"E\ \ '' \Rightarrow (4, 26)^T$$
$$"IA'' \Rightarrow (8, 0)^T$$

Problem 9. *Find the inverse of the matrix* $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$ *in* $\mathbb{Z}_{26}$.

$$det(A) = D = 2 \times 8 - 3 \times 7 = -5 = 21(mod\ 26)$$

Note that $(21, 26) = 1$ *so* D *has inverse in* $\mathbb{Z}_{26}$ *and* $D^{-1} = 21^{-1} = 5$. *Therefore*

$$\begin{aligned} A^{-1} &= \begin{pmatrix} D^{-1}d & -D^{-1}b \\ -D^{-1}c & D^{-1}a \end{pmatrix} \\ &= \begin{pmatrix} 5 \times 8 & -5 \times 3 \\ -5 \times 7 & 5 \times 2 \end{pmatrix} \\ &= \begin{pmatrix} 40 & -15 \\ -35 & 10 \end{pmatrix} = \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \end{aligned}$$

Problem 10. *Solve the following system of simultaneous congruences:*

$$2x + 3y \equiv 1 mod\ 26$$
$$7x + 8y \equiv 2 mod\ 26$$

The given system is equivalent to matrix:

$$\begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 2 \end{pmatrix} (mod\ 26)$$

Therefore

$$\begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$
$$\equiv \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \end{pmatrix} \equiv \begin{pmatrix} 10 \\ 11 \end{pmatrix}$$

Problem 11. *Suppose we are working in the 26-letter alphabet, use the matrix* $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$ *to encipher the message "NO".*

Note that the matrix corresponding to the digraph unit "NO" is

$$P = \begin{pmatrix} 13 \\ 14 \end{pmatrix}$$

Therefore

$$C = AP = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} 13 \\ 14 \end{pmatrix} = \begin{pmatrix} 16 \\ 21 \end{pmatrix} \rightarrow \text{"}QV\text{"}$$

Problem 12. *Suppose we are working in the 26-letter alphabet, use the matrix* $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$ *to encipher the message "NOANSWER".*

The matrix corresponding to "NOANSWER" is

$$P = \begin{pmatrix} 13 & 0 & 18 & 4 \\ 14 & 13 & 22 & 17 \end{pmatrix}$$

Therefore

$$C = AP = \begin{pmatrix} 68 & 39 & 102 & 59 \\ 203 & 104 & 302 & 164 \end{pmatrix} = \begin{pmatrix} 16 & 13 & 24 & 7 \\ 21 & 0 & 16 & 6 \end{pmatrix}$$

The coded message is "QVNAYQHI"

Problem 13. *Suppose we are working in the 26-letter alphabet, use the matrix* $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix}$ *to decipher the message "FWMDIQ".*

The matrix corresponding to "FWMDIQ" is

$$C = \begin{pmatrix} 5 & 12 & 8 \\ 22 & 3 & 16 \end{pmatrix}$$

We have

$$C = AP$$

Therefore

$$P = A^{-1}C = \begin{pmatrix} 14 & 11 \\ 17 & 10 \end{pmatrix} \begin{pmatrix} 5 & 12 & 8 \\ 22 & 3 & 16 \end{pmatrix} = \begin{pmatrix} 0 & 19 & 2 \\ 19 & 0 & 10 \end{pmatrix}$$

The decoded message is "ATTACK"

Problem 14. *Suppose that we know that our adversary is using a 2×2 enciphering matrix with a 29-letter alphabet, where A–Z have the usual numerical equivalents, blank=26, ?=27, ! =28. We receive the message*

"GFPYJP X?UYXSTLADPLW, "

and we suppose that we know that the last five letters of plaintext are our adversary's signature "KARLA." Decipher the message

"GFPYJP X?UYXSTLADPLW "

Problem 15. *Note that*

$$\text{“}AR\text{”} = \begin{pmatrix} 0 \\ 17 \end{pmatrix} \to \text{“}DP\text{”} = \begin{pmatrix} 3 \\ 15 \end{pmatrix}$$

$$\text{“}LA\text{”} = \begin{pmatrix} 11 \\ 0 \end{pmatrix} \to \text{“}LW\text{”} = \begin{pmatrix} 11 \\ 22 \end{pmatrix}$$

We have

$$C = AP$$

Therefore

$$\begin{pmatrix} 3 & 11 \\ 15 & 22 \end{pmatrix} = A \begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix}$$

So

$$A^{-1} = \begin{pmatrix} 0 & 11 \\ 17 & 0 \end{pmatrix} \begin{pmatrix} 3 & 11 \\ 15 & 22 \end{pmatrix}^{-1} = \begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix}$$

Now

$$C = AP$$

Therefore

$$\begin{aligned} P &= A^{-1}P \\ &= \begin{pmatrix} 21 & 19 \\ 22 & 18 \end{pmatrix} \begin{pmatrix} 6 & 15 & 9 & 26 & 27 & 24 & 18 & 11 & 3 & 11 \\ 5 & 24 & 15 & 23 & 20 & 23 & 19 & 0 & 15 & 22 \end{pmatrix} \\ &= \begin{pmatrix} 18 & 17 & 10 & 26 & 19 & 13 & 14 & 28 & 0 & 11 \\ 19 & 8 & 4 & 0 & 26 & 14 & 13 & 10 & 17 & 0 \end{pmatrix} \\ &= \text{“}STRIKE \quad AT \quad NOON!KARLA.\text{”} \end{aligned}$$

Bibliography

[1] Apostol T.M., Introduction to Analytic Number Theory, Narosa Publishing House, New Delhi, 1990.

[2] **G. H. Hardy and E.M. Wright**: Introduction to the theory of numbers; Oxford International Edn; 1985

[3] **A. Hurwitz & N. Kritiko**: Lectures on Number Theory; Springer Verlag ,Universitext; 1986

[4] **T. Koshy**: Elementary Number Theory with Applications; Harcourt / Academic Press; 2002

[5] **D. Redmond**: Number Theory; Monographs & Texts in Mathematics No: 220; Marcel Dekker Inc.; 1994

[6] **P. Ribenboim**: The little book of Big Primes; Springer-Verlag, New York; 1991

[7] **K.H. Rosen**: Elementary Number Theory and its applications(3rd Edn.); Addison Wesley Pub Co.; 1993

[8] **W. Stallings**: Cryptography and Network Security-Principles and Practices; PHI; 2004

[9] **D.R. Stinson**: Cryptography- Theory and Practice(2nd Edn.); Chapman & Hall / CRC (214. Simon Sing : The Code Book The Fourth Estate London); 1999

[10] **S.Y. Yan**: Number Theroy for Computing(2nd Edn.); Springer-Verlag; 2002

[11] Jonathan Katz and Yehuda, Introduction to Modern Cryptography, CRC Press.

4.5 Syllabus

Semester 1

MTH1CO5: NUMBER THEORY
No. of Credits: 4
No. of hours of Lectures/week: 5

TEXT 1 : APOSTOL T.M., INTRODUCTION TO ANALYTIC NUMBER THEORY, Narosa Publishing House, New Delhi, 1990.

TEXT 2: KOBLITZ NEAL A., COURSE IN NUMBER THEROY AND CRYPTOGRAPHY, SpringerVerlag, NewYork, 1987.

Module 1

Arithmetical functions and Dirichlet multiplication; Averages of arithmetical functions [Chapter 2: sections 2.1 to 2.14, 2.18, 2.19; Chapter 3: sections 3.1 to 3.4, 3.9 to 3.12 of Text 1]

Module 2

Some elementary theorems on the distribution of prime numbers [Chapter 4: Sections 4.1 to 4.10 of Text 1]

Module 3

Quadratic residues and quadratic reciprocity law [Chapter 9: sections 9.1 to 9.8 of Text 1] Cryptography, Public key [Chapters 3 ; Chapter 4 sections 1 and 2 of Text 2.]

4.6 Notations

$\mathbb{N}$ = the set of natural numbers

$\mathbb{C}$ = the set of complex numbers

$[x]$ = the greatest integer less than or equal to x

$\{x\} = x - [x]$

$d|n$ = d divides n

$\sum_{d|n}$ = summation over all divisors of n

$\sum_{p|n}$ = summation over all prime divisors of n

$\#(A)$ = the cardinality of the set A

(c, d) = the greatest common divisor of c and d