To

My brother Sagar

Contents

Preface

These are the class notes for the first-semester undergraduate students of our college. These notes help students to acquire the basic knowledge of Number Theory. The pre-requisitions for reading these notes are the basic knowledge in set theory.

It contains three chapters. In Chapter-I, we tried to discuss the construction of natural numbers and integers as well as the algebraic operations, ordering properties of them. Moreover, division algorithm, greatest integer functions are discussed briefly.

In Chapter-II, Number theoretic functions are discussed with some well-known examples of number theoretic functions.

In Chapter-III, we introduced the idea of congruences. Also, we discussed Euler's Theorem, Fermat's little theorem, Chinese remainder theorem etc. As an application of Euler's theorem, public-key cryptosystems (RSA model) are also briefly introduced here.

Ramakrishna Mission
Vivekananda Centenary College.

Bikash Chakraborty
08th May, 2019.

Chapter 1

Introduction

1.1 The set of Natural numbers

The ability to count things are known to us from our childhood. That's why in common language, natural numbers are called counting numbers. Also, natural numbers are seem to be the God gifted numbers.

In set theoretic notations (Zermelo-Fraenkel set theory), the **natural numbers** are defined recursively by letting $0 = \{\}$ be the empty set and $n + 1 = n \cup \{n\}$ for each n. So we can formulate a natural numbers as below:

$$\begin{aligned} 0 &= \{\} = \varphi, \\ 1 &= \{0\} = \{\varphi\}, \\ 2 &= \{0, 1\} = \{\varphi, \{\varphi\}\}, \\ 3 &= \{0, 1, 2\} = \{\varphi, \{\varphi\}, \{\varphi, \{\varphi\}\}\}, \\ &\dots \end{aligned}$$

Peano's axioms, also known as Peano's postulates, in number theory, five axioms introduced in 1889 by Italian mathematician Giuseppe Peano. Like the axioms for geometry devised by Greek mathematician Euclid, the Peano's axioms were meant to provide a rigorous foundation for the natural numbers $\{0, 1, 2, 3, \dots\}$ used in arithmetic, number theory, and set theory. In particular, the Peano's axioms enable an infinite set to be generated by a finite set of symbols and rules.

We start with the axioms of Peano:

Peano's Axioms:

1. The set $\mathbb{N}$ has a distinguished element which we call "1", i.e., $\mathbb{N} \neq \varphi$.

2. There exists a distinguished set map $\sigma : \mathbb{N} \to \mathbb{N}$. The element $n' = \sigma(n)$ is called **successor of** n.

3. The map σ is injective. i.e., distinct elements has distinct successors.

4. There does not exist an element n such that $\sigma(n) = 1$, i.e., σ is not a surjective map.

5. Let $S \subseteq \mathbb{N}$ such that $1 \in \mathbb{N}$ and $k \in S$ implies $k+1 \in S$. Then $S = \mathbb{N}$.

   (This property is known as **Principle of Mathematical Induction**).

Theorem 1.1.1. If $n \in \mathbb{N} \setminus \{1\}$. Then there exists $m \in \mathbb{N}$ such that $\sigma(m) = n$.

Proof. Let us construct the following set

$$S := \{n \in \mathbb{N} \quad : \quad n = 1 \ \text{ or, } \ n = \sigma(m) \ \text{ for some } \ m \in \mathbb{N}\}.$$

Then

i. $1 \in S$.

ii. Let $k \in S$ with $k \geq 2$. Then there exists $m \in \mathbb{N}$ such that $\sigma(m) = k$.

   Now, $\sigma(k) = \sigma(\sigma(m))$. Since, $\sigma(m) \in \mathbb{N}$, so $\sigma(k) \in S$. Thus by Principle of Mathematical Induction, $S = \mathbb{N}$.

This completes the proof. □

Algebraic operations on $\mathbb{N}$

Let us define a binary operation, namely "**addition**" on $\mathbb{N}$ as follows:

i. For all $n \in \mathbb{N}$, $n + 1 := \sigma(n)$.

ii. For $n \in \mathbb{N}$ and $m \in \mathbb{N} \setminus \{1\}$, $n + m = n + \sigma(m') := \sigma(n + m')$.

   (By Theorem 1.1.1, there exists $m' \in \mathbb{N}$ such that $\sigma(m') = m$.)

Example 1.1.1. We denote

$$1 + 1 = \sigma(1) := 2.$$

Now, using definition of addition,

$$1 + 2 = 1 + \sigma(1) = \sigma(1 + 1) = \sigma(2). \ \text{ We denote } \ \sigma(2) := 3.$$

Again, by similar way,

$$1 + 3 = 1 + \sigma(2) = \sigma(1 + 2) = \sigma(3). \ \text{ We denote } \ \sigma(3) := 4.$$

And, so on.

Remark 1.1.1. Thus the set of naturals can be thought as

$$\mathbb{N} := \{1, \sigma(1), \sigma(\sigma(1)), \ldots\},$$

or, in notations,

$$\mathbb{N} := \{1, 2, 3, 4, \ldots\}.$$

Exercise 1.1.1. Using "principle of mathematical induction", Show that

i. $x + y = y + x$ for all $x, y \in \mathbb{N}$.

ii. $x + (y + z) = (x + y) + z$ for all $x, y, z \in \mathbb{N}$.

iii. For all $x, y, z \in \mathbb{N}$, if $x + y = x + z$, then $y = z$.

Next, we define another binary operation, namely "**multiplication**" on $\mathbb{N}$ recursively as follows:

i. For all $n \in \mathbb{N}$, $n \cdot 1 := n$.

ii. For $n \in \mathbb{N}$ and $m \in \mathbb{N} \setminus \{1\}$, $n \cdot m = n \cdot \sigma(m') = n + n \cdot m'$.
(By Theorem 1.1.1, there exists $m' \in \mathbb{N}$ such that $\sigma(m') = m$.)

Example 1.1.2. Clearly, $n \cdot 2 = n \cdot \sigma(1) = n + n \cdot 1 = n + n$.
Again, $n \cdot 3 = n \cdot \sigma(2) = n + n \cdot 2 = n + (n + n)$.

Exercise 1.1.2. Using "principle of mathematical induction", Show that

i. For all $x, y, z \in \mathbb{N}$, $x \cdot (y + z) = x \cdot y + x \cdot z$.

ii. $x \cdot y = y \cdot x$ for all $x, y \in \mathbb{N}$.

ii. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all $x, y, z \in \mathbb{N}$.

Ordering properties of natural numbers

Let $n, m \in \mathbb{N}$. We say that n is less than m, written $n < m$, if there exists a $k \in \mathbb{N}$ such that $m = n + k$.
We also write $n \leq m$ to mean that either $n = m$ or $n < m$.

Exercise 1.1.3. Show that for $x, y, z \in \mathbb{N}$,

i. $x \leq y$ and $y \leq x$ implies $x = y$.

ii. $x \leq y$ and $y \leq z$ implies $x \leq z$.

Principle of Mathematical Induction

Let $S \subseteq \mathbb{N}$ such that

i. $1 \in S$,

ii. $k \in S \Rightarrow k + 1 \in S$.

Then $S = \mathbb{N}$.

Well-ordering principle

Every non-empty subset of $\mathbb{N}$ has a least element, i.e., Let $S \neq \varphi$ and $S \subseteq \mathbb{N}$. Then there exist $m \in S$ such that $m \leq s$ for every $s \in S$.

Theorem 1.1.2. "Principle of Mathematical Induction" is equivalent to "Well-ordering principle".

Proof. **Principle of Mathematical Induction $\Rightarrow$ Well-ordering principle**.

Let $S \neq \varphi$ and $S \subseteq \mathbb{N}$. Assume that S has no least element. Then $1 \notin S$. Now, we define

$$T := \{x \in \mathbb{N} \ : \ x < s \ \text{ for each } \ s \in S\}.$$

Then $T \cap S = \varphi$ and $T \neq \varphi$, as $1 \in T$.

Let $p \in T$. Then $p < s$ for every $s \in S$. That is any element of S is greater than or equal to $p + 1$.

If $p + 1 \in S$, then S has a least element, which is not possible. Thus $p + 1 \in T$.

Since $1 \in T$ and $p \in T \Rightarrow p + 1 \in T$, so by principle of mathematical induction, $T = \mathbb{N}$. Hence, $S = \varphi$. Thus our assumption is wrong.

Well-ordering principle $\Rightarrow$ Principle of Mathematical Induction.

Let us define

$$T := \mathbb{N} \setminus S.$$

If $T \neq \varphi$, then by well-ordering principle, T has a minimum element, say m.

Since $1 \in S$, so $1 \notin T$. Thus $m > 1$, i.e., $m - 1 \in S$. Thus by the given property of S, $m = (m - 1) + 1 \in S$, which is a contradiction. Thus $T = \varphi$. Hence $S = \mathbb{N}$. □

Theorem 1.1.3. Let $n \in \mathbb{N}$ and $P(n)$ be a statement. If

i. $P(1)$ is true and

ii. $P(k)$ is true implies $P(k + 1)$ is true,

then $P(n)$ is true for all $n \in \mathbb{N}$.

Proof. Let

$$S = \{n \in \mathbb{N} \ : \ P(n) \ \text{ is } \ \text{true}\}.$$

Then

i. $1 \in S$ is true and

ii. $k \in S$ is implies $k + 1 \in S$.

Thus by principle of mathematical induction, $S = \mathbb{N}$. This proves that $P(n)$ is true for all $n \in \mathbb{N}$. □

Example 1.1.3. Using principle of mathematical induction, show that

$$n < 2^n \quad \text{for} \quad n \in \mathbb{N}.$$

Solution:
Here the statement is

$$P(n) \ : \ n < 2^n \quad \text{for} \quad n \in \mathbb{N}.$$

Clearly, $P(1)$ is true. Assume that $P(k)$ is true for any natural number k. Now,

$$\begin{aligned} 2^{k+1} &= 2^k \cdot 2, \\ &\geq 2 \cdot k, \ \text{ since } \ P(k) \ \text{ is } \ \text{true}, \\ &\geq k+1. \end{aligned}$$

Thus $P(k+1)$ is true. Hence, by principle of mathematical induction, $P(n)$ is true for every $n \in \mathbb{N}$.

Exercise 1.1.4. Using principle of mathematical induction, show that

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}.$$

Exercise 1.1.5. Using principle of mathematical induction, show that

$$1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Exercise 1.1.6. Using principle of mathematical induction, show that

$$1^3 + 2^3 + 3^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2.$$

Exercise 1.1.7. Using principle of mathematical induction, show that $3^{2n} - 8n - 1$ is divisible by 64.

Theorem 1.1.4. Let $n \in \mathbb{N}$ and $P(n)$ be a statement. Given that

i. $P(n_0)$ is true for $n_0 \in \mathbb{N}$ and $P(n)$ is false for $n < n_0$.

ii. $P(k)$ is true implies $P(k+1)$ is true for all $k \geq n_0$.

Then $P(n)$ is true for all $n \geq n_0$.

Proof. Let

$$S = \{n \in \mathbb{N} \quad : \quad P(n) \ \text{ is } \ \text{true}\},$$

and

$$T = \{n_0, n_0 + 1, n_0 + 2, \ldots\}.$$

It is clear that $S \subseteq T$. If possible, let $T \setminus S \neq \varphi$. Then by well-ordering principle of natural numbers, we have a least element of $T \setminus S$, say m.

Since $n_0 \notin T \setminus S$, so, $m > n_0$. Thus $m - 1 \geq n_0$. Hence, $m - 1 \in T$. As m is the least member of $T \setminus S$, so $m - 1 \notin T \setminus S$. Thus $m - 1 \in S$.

Thus by the given property of S, we have $m = (m-1) + 1 \in S$, which is impossible. Thus $S = T$. This completes the proof. □

Example 1.1.4. Show that

$$2^n < n! \quad \text{for} \quad n \geq 4 \quad \text{and} \quad n \in \mathbb{N}.$$

Remark 1.1.2. Here, the statement is

$$P(n) \quad : \quad 2^n < n! \quad \text{for} \quad n \geq 4 \quad \text{and} \quad n \in \mathbb{N}.$$

Clearly, the statements $P(1)$, $P(2)$, and $P(3)$ are wrong.

Solution:

Clearly, $P(4)$ is true. Assume that $P(k)$ is true for any natural number $k \geq 4$. Now,

$$\begin{aligned} 2^{k+1} &= 2^k \cdot 2, \\ &< (k!) \cdot 2, \quad \text{since} \quad P(k) \quad \text{is} \quad \text{true}, \\ &< (k!) \cdot (k+1) = (k+1)!. \end{aligned}$$

Thus $P(k+1)$ is true. Hence, by Theorem 1.1.4, $P(n)$ is true for every $n \in \mathbb{N}$ and $n \geq 4$.

Theorem 1.1.5 (Principle of strong mathematical induction). Let $S \subseteq \mathbb{N}$ such that

i. $1 \in S$,

ii. For every $k \in \mathbb{N}$, if $\{1, 2, 3, \ldots, k\} \subseteq S$, then $k + 1 \in S$.

Then $S = \mathbb{N}$.

Proof. Let us define

$$T := \mathbb{N} \setminus S.$$

If $T \neq \varphi$, then by well-ordering principle, T has a minimum element, say m.

Since $1 \in S$, so $1 \notin T$. Thus $m > 1$, i.e., $\{1, 2, 3, \ldots, m-1\} \subseteq S$. Thus by the given property of S, $m = (m-1) + 1 \in S$, which is a contradiction. Thus $T = \varphi$. Hence $S = \mathbb{N}$. □

Remark 1.1.3. We have already seen that "Principle of Mathematical Induction (in short, PMI)" is equivalent to "Well-ordering principle". Now, we have to see that "Principle of Mathematical Induction" is equivalent to "Principle of strong Mathematical Induction".

Principle of Mathematical Induction ⇒ Principle of strong Mathematical Induction

Let S be a subset of natural numbers satisfying the hypothesis of "Principle of strong Mathematical Induction". Now, we construct a set

$$T := \{n \in \mathbb{N} \quad : \quad 1, 2, 3, \ldots, n \in S\}$$

Then $1 \in T$ as $1 \in S$.

Assume that $k \in T$. Then $\{1, 2, 3, \ldots, k\} \subseteq S$. But S satisfies the hypothesis of Principle of strong Mathematical Induction. Thus $(k+1) \in S$. Hence, $(k+1) \in T$.

Thus T satisfies the hypothesis of Principle of Mathematical Induction. Thus $T = \mathbb{N}$, i.e., $S = \mathbb{N}$.

Principle of strong Mathematical Induction $\Rightarrow$ Well ordering principle (hence, PMI)

Let $S \subseteq \mathbb{N}$ and S has no least element.

Claim: $S = \varphi$.

For this, we construct a set

$$T := \mathbb{N} \setminus S.$$

Since S has no least element, so $1 \in T$. Assume that $\{1, 2, 3, \ldots, k\} \subseteq T$. Then $i \notin S$ for $1 \leq i \leq k$. Thus $(k+1) \notin S$, otherwise, it will be the least element of S. Thus $(k+1) \in T$.

Thus T satisfies the Principle of strong Mathematical Induction. Hence, $T = \mathbb{N}$, i.e., $S = \varphi$.

Example 1.1.5. Let $x_1 = 1, x_2 = 2$ and

$$x_{n+2} = \frac{1}{2}(x_n + x_{n+1}) \ \text{ for all } \ n \in \mathbb{N}.$$

Show that $1 \leq x_n \leq 2$ for all $n \in \mathbb{N}$.

Solution:

Let

$$S = \{n \in \mathbb{N} \ : \ 1 \leq x_n \leq 2\}.$$

Then $1 \in S$. Also, assume that for every $k \in \mathbb{N}$, $\{1, 2, 3, \ldots, k\} \subseteq S$.

That is, $1 \leq x_i \leq 2$ for $1 \leq i \leq k$. Thus

$$\frac{1}{2}(1+1) \leq \frac{1}{2}(x_k + x_{k-1}) \leq \frac{1}{2}(2+2).$$

Hence $1 \leq x_{k+1} \leq 2$, i.e., $k+1 \in S$. Thus by, principle of mathematical induction, we obtain $S = \mathbb{N}$.

Exercise 1.1.8 (Backward mathematical induction). Let $S \subseteq \mathbb{N}$ such that

i. S is not a finite set.

ii. For every $k \in \mathbb{N}$, $k \in S$ implies $k - 1 \in S$.

Then $S = \mathbb{N}$.

A fallacy!

All horses have the same color!!!!

We prove(!!) this argument by principle of mathematical induction.

For the case $n = 1$, let us take any one horse from the all horses. Thus $P(1)$ is true.

Assume that $P(k)$ is true, i.e, k-horses have the same colour.

Now, we take $k+1$ horses $\{h_1, h_2, \ldots, h_{k+1}\}$. Since $\{h_1, h_2, \ldots, h_k\}$ (k-horses) have same colour and $\{h_2, \ldots, h_{k+1}\}$ (k-horses) have same colour, so the $(k+1)$ horses $\{h_1, h_2, \ldots, h_{k+1}\}$ have same colour, because $\{h_2, \ldots, h_{k+1}\} \cap \{h_1, h_2, \ldots, h_k\} \neq \varphi$.

If k- horses have the same color, then $k+1$-horses will also have the same color. Thus, by the principle of mathematical induction, in any group of horses, all horses must be the same color.

But it is not true that all horses are of the same color, so where did we go wrong in our induction proof?

Think!!!!: For $n = 2$, $\{h_2\} \cap \{h_1\} = \varphi$. Thus $P(1) \nRightarrow P(2)$.

1.2 The set of Integers

Let us consider a set $S = \mathbb{N} \times \mathbb{N}$. We define a binary relation $\sim$ on S with the following rule:

$$(a, b) \sim (c, d) \text{ if and only if } a + d = b + c.$$

We can easily verify that $\sim$ is an equivalence relation on S. Thus $\sim$ gives a partition on S.

Let $\mathbb{Z}$ be the set of all equivalence classes under this relation. Next, we define addition and multiplication on $\mathbb{Z}$ as

$$[(a, b)] + [(c, d)] = [(a + c, b + d)],$$

$$[(a, b)] \cdot [(c, d)] = [(ac, bd)].$$

Also, the negation (or additive inverse) of an integer is obtained by reversing the order of the pair:

$$-[(a, b)] := [(b, a)].$$

The standard ordering on the integers is given by:

$$[(a, b)] < [(c, d)] \text{ if and only if } a + d < b + c.$$

Example 1.2.1. 1. $[(0, 0)] = [(1, 1)] = \ldots = [(n, n)]$,

2. $[(1, 0)] = [(2, 1)] = \ldots = [(n + 1, n)]$,

3. $[(0, 1)] = [(1, 2)] = \ldots = [(n, n + 1)]$.

Every equivalence class has a unique member that is of the form $(n, 0)$ or $(0, n)$ or $(0, 0)$. The natural number n is identified with the class $[(n, 0)]$, and the class $[(0, n)]$ is denoted by the symbol $-n$. Thus $-0 = 0$.

Thus, $[(a, b)]$ is denoted by

$$\begin{aligned} [(a, b)] &= a - b \text{ if } b \leq a, \\ &= b - a \text{ if } a < b. \end{aligned}$$

Example 1.2.2. 1. $0 = [(0, 0)] = [(1, 1)] = \ldots = [(n, n)]$,

2. $1 = [(1, 0)] = [(2, 1)] = \ldots = [(n + 1, n)]$,

3. $-1 = [(0, 1)] = [(1, 2)] = \ldots = [(n, n + 1)]$.

This notation recovers the familiar representation of the integers as $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

Absolute values of integers

Let us denote by $\mathbb{N}_0 = \mathbb{N} \cup \{0\} \subseteq \mathbb{Z}$. Next, we define a map $|\cdot|: \mathbb{Z} \to \mathbb{N} \cup \{0\}$ as

$$\begin{aligned} | a | &= a \text{ if } a \text{ non-negative}, \\ &= -a \text{ if } a \text{ negative}. \end{aligned}$$

Example 1.2.3. Let $m, n \in \mathbb{Z}$. Then

i. $| n | \geq 0$. Moreover, $| n |= 0$ if and only if $n = 0$.

ii. [Symmetric Property] $| m - n |=| n - m |$.

iii. [Triangle Inequality] $| m + n | \leq | m | + | n |$.

This function is known as the **absolute value**.

1.3 Division algorithm

We begin this section with a statement of the Division Algorithm:

Theorem 1.3.1. Given two integers a and b with $b > 0$, then there exists unique pair of integers q and r such that

$$a = bq + r, \quad \text{with } 0 \leq r < b.$$

Proof. Let

$$S = \{a - bx \ : \ x \in \mathbb{Z} \ \text{ and } \ a - bx \geq 0\}.$$

Then $S \neq \varphi$ as $[a - b(- \mid a \mid)] = \mid a \mid (b \pm 1) \in \mathbb{N} \cup \{0\}$. Moreover, $S \subseteq \mathbb{N} \cup \{0\}$. Thus by Well-Ordering principle, S has a least element, say, $a - bq$. Let

$$r = a - bq$$

Thus $r \geq 0$. Moreover, we have to show that $r < b$.

If not, assume $r \geq b$, then $[a - b(q + 1)] = [r - b] \geq 0$ and $[a - b(q + 1)] = (a - bq) - b \leq (a - bq)$, which contradicts the fact that $a - bq$ is the least element of S.

Thus $0 \leq r < b$.

Uniqueness part:

If possible, there exist another pair q' and r' such that $a = bq' + r'$. Then $(r - r') = b(q - q')$ and $0 \leq r < b$, $0 \leq r' < b$. Thus $b \mid (\mid r' - r \mid)$ and $0 \leq \mid r' - r \mid < b$. Hence, $r - r' = 0$, consequently, $q' - q = 0$. □

Corollary 1.3.1. Given two integers a and b with $b \neq 0$,then there exists unique pair of integers q and r such that

$$a = bq + r, \quad \text{with } \ 0 \leq r < \mid b \mid .$$

Proof. Here $\mid b \mid > 0$. Thus we apply division algorithm for a and $\mid b$. □

Definition 1.3.1. We say that q is **the quotient** and r is **the remainder** in the division of a by b.

Definition 1.3.2. If $r = 0$, then we say that b divides a, or, a is divisible by b. In this case, we write $b \mid a$.

Remark 1.3.1. We know that $0 = 0 \times n$, where n is any integers. Thus, if we divide 0 by 0, we obtain any integer as a quotient. Thus the uniqueness of quotient is violated. So, we can't determine the quotient "exactly" when 0 is divided by 0.

Theorem 1.3.2. If $a \mid b$ and $a \mid c$, then $a \mid bx + cy$, for any integers $x, y \in \mathbb{Z}$.

Proof. Given that $b = aq$ and $c = aq'$ for some integers $q, q' \in \mathbb{Z}$. Then $bx + cy = a(qx + q'y)$. This completes the proof. □

Example 1.3.1. Prove that product of any m consecutive integers is divisible by m.

Proof. Let $c, c+1, c+2, \ldots, c+(m-1)$ be m consecutive integers. Then by Division Algorithm, we obtain

$$c = qm + r$$

for some integers $q, m \in \mathbb{Z}$ with $0 \leq r < m$. Thus

$$c + (m - r) = m(q + 1).$$

Thus $m \mid c + (m - r)$. This completes the proof. □

Definition 1.3.3. Let $a, b \in \mathbb{Z}$, both not zero. We define the greatest common divisor of a, b, denoted by, $d = \gcd(a, b)$ as

i. $d > 0$,

ii. $d \mid a$ and $d \mid b$,

iii. if $c \mid a$ and $c \mid b$, then $c \mid d$.

Example 1.3.2. $\gcd(-8, 12) = \gcd(-8, -12) = \gcd(8, 12) = 4$.

Example 1.3.3. $\gcd(0, n) = n$, where $n \in \mathbb{Z} \setminus \{0\}$.

Theorem 1.3.3. Let $a, b \in \mathbb{Z}$, both not zero. Then $\gcd(a, b)$ can be expressed as a integer combination of a and b, i.e., there exist integers (not unique), $u, v \in \mathbb{Z}$ such that

$$\gcd(a, b) = au + bv.$$

Proof. Since $\gcd(\mid a \mid, \mid b \mid) = \gcd(a, b)$, so without loss of generality, we assume that $a \geq 0$ and $b \geq 0$. Let

$$S = \{ax + by \quad : \quad x, y \in \mathbb{Z} \;\text{ and }\; ax + by > 0\}.$$

Clearly, $(\mid a \mid + \mid b \mid) = \{a(\pm 1) + b(\pm)\} \in S$. (We choose $x = 1$ if $a \geq 0$ and $x = -1$ if $a < 0$. Similarly, we choose y.) Thus $S \neq \varphi$ and $S \subseteq \mathbb{N}$.

Thus by Well-ordering property, S has least element, say d. Thus there exists integers $u, v \in \mathbb{Z}$ such that

$$d = au + bv.$$

Claim: $d = \gcd\{a, b\}$.

i. Clearly $d > 0$.

ii. Now, by division algorithm, we have $a = dq + r$, where $0 \leq r < d$.

$$\begin{aligned} r &= a - dq \\ &= a - (au + bv)q \\ &= a(1 - uq) + b(-vq), \end{aligned}$$

which implies $r \in S$. Since $0 \leq r < d$ and d is the minimum element of S, so $r = 0$. Thus $d \mid a$. Similarly, we can check that $d \mid b$.

iii. If $c \mid a$ and $c \mid b$, then $c \mid au + bv = d$ (by Theorem 1.3.2).

Thus $d = \gcd(a, b)$. □

Remark 1.3.2. Let $a = 12$, $b = 18$, $u = 3$ and $v = -2$. Here, $au + bv = 0$, but 0 is not the $\gcd(a, b)$.

Thus the converse part of Theorem 1.3.3 is not true always.

Theorem 1.3.4. Let $a, b \in \mathbb{Z}$, both not zero. Then $\gcd(a, b) = 1$ if and only if there exist integers (not unique), $u, v \in \mathbb{Z}$ such that

$$au + bv = 1.$$

Proof. If $\gcd(a, b) = 1$, then by Theorem 1.3.3, there exist integers (not unique), $u, v \in \mathbb{Z}$ such that $au + bv = 1$.

Next, we assume that there exist integers (not unique), $u, v \in \mathbb{Z}$ such that $au + bv = 1$. Now, our claim is to show that $\gcd(a, b) = 1$.

Let $\gcd(a, b) = d$, then $d \mid a$ and $d \mid b$. Thus $d \mid au + bv$, i.e., $d \mid 1$. Since $d > 0$, so $d = 1$. □

Theorem 1.3.5. Let $a, b \in \mathbb{Z} \setminus \{0\}$ such that $a = bq + r$ for some integers q and r with $0 \leq r <\mid b \mid$. Then $\gcd(a, b) = \gcd(b, r)$.

Proof. Let $d = \gcd(a, b)$ and $d' = \gcd(b, r)$. Then $d \mid a$ and $d \mid b$. Thus $d \mid (a - bq) = r$. As $d \mid r$ and $d \mid b$, so $d \mid d'$. Similarly, we can check that $d' \mid d$. Thus $d = d'$, as d, d' is positive. □

Euclidean algorithm

The Theorem 1.3.5 help us to find the gcd of two (hence finite) given numbers. This process is known as the Euclidean algorithm.

Theorem 1.3.6 (Euclidean algorithm). Given two positive integers a and b with $b \nmid a$. Let $a = r_0$ and $b = r_1$ and applying the division algorithm repeatedly to obtain a set of remainders defined successively by the relations

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2, && 0 < r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3, && 0 < r_3 < r_2, \\
&\vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, && 0 < r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n + r_{n+1}, && r_{n+1} = 0.
\end{aligned}$$

Then $\gcd\{a, b\} = r_n$.

Proof. Division algorithm ensures that the sequence of non-negative real numbers $\{r_n\}$ exists and strictly decreasing. Since $r_n \geq 0$ and strictly decreasing, so there exist a stage where $r_{n+1} = 0$.

Thus applying the Theorem 1.3.5, we obtain,

$$\gcd\{a, b\} = \gcd\{r_0, r_1\} = \gcd\{r_1, r_2\} = \ldots = \gcd\{r_{n-2}, r_{n-1}\} = \gcd\{r_{n-1}, r_n\} = r_n$$

□

Example 1.3.4. Find $\gcd\{15, 40\}$.

Solution:
By division algorithm, we have

$$\begin{aligned} 40 &= 2 \times 15 + 10, \\ 15 &= 1 \times 10 + 5, \\ 10 &= 2 \times 5 + 0. \end{aligned}$$

Thus $\gcd\{15, 40\} = 5$.
Again,

$$\begin{aligned} 5 &= 15 - 1 \times 10, \\ &= 15 - 1 \times (40 - 2 \times 15), \\ &= 3 \times 15 - 1 \times 40. \end{aligned}$$

Thus $\gcd\{15, 40\} = 15u + 40v$, where $u = 3$ and $v = -1$.

Exercise 1.3.1. Find the integers u and v satisfying

$$20u + 37v = 1.$$

Exercise 1.3.2. Find $\gcd\{250, 39\}$.

Exercise 1.3.3. Show that $\gcd\{a, a + 2\} = 1$, or, 2 where $n \in \mathbb{N}$.

1.4 Prime numbers

An integer $p(> 1)$ is said to be a **prime number** if its only positive divisors are 1 and p.

An integer which is not a prime number is called a **composite number**.

Remark 1.4.1. The number 1 is regarded as neither prime nor composite.

Theorem 1.4.1. Every integer $n > 1$ is either prime or a product of prime numbers.

Proof. Let

$$S = \{n \in \mathbb{N} \ : \ n > 1 \ \text{ and } \ n \ \text{ has no prime divisor}\}.$$

If $S = \varphi$, then there is nothing to prove. So, we assume that $S \neq \varphi$. Since $S \subseteq \mathbb{N}$, so by Well-Ordering principle, S has a least element, say m. Thus $m > 1$. Since, $m \in S$, so m is not prime. Hence m is a composite number. Thus it has a positive divisor other than 1 and m, say d. Then $1 < d < m$.Now we consider two cases:
Case:-I
If d is a prime, then m has a prime divisor, a contradiction.
Case:-II
If d is not a prime, then $d \in S$. which contradicts that m is the least element of S.

Thus $S = \varphi$, i.e., every integer $n > 1$ is either prime or has a prime divisors. □

Theorem 1.4.2. Let p be a prime number and a be an integer with $1 \leq a < p$, then

$$\gcd\{a, p\} = 1.$$

Proof. Left as an exercise. □

Theorem 1.4.3. Let p be a prime number and a be an integer with $a \geq p$, then either $p \mid a$, or $\gcd\{a, p\} = 1$.

Proof. Left as an exercise. □

Theorem 1.4.4. Let p be a prime number and a, b be two integers with $p \mid ab$, then either $p \mid a$, or $p \mid b$.

Proof. Given that $p \mid ab$. That is $ab = kp$, for some integer k.

If $p \nmid a$, then $\gcd\{p, a\} = 1$. Thus there exists integers u and v such that $pu + va = 1$.

Now, $b = p(bu) + v(ab) = p(bu) + p(kv)$, i.e, $p \mid b$. □

Theorem 1.4.5 (Euclid's Theorem). The number of primes are infinite.

Proof. On contrary, we assume that there are only finitely many primes, say $p_1, p_2, p_3, \ldots, p_k$. Let

$$N = 1 + p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k.$$

Then $N > p_i$ for all i. Now, we consider two cases:

Case:-I

If N is a prime, then N is new prime as $N > p_i$ for all i. Thus the list of primes $p_1, p_2, p_3, \ldots, p_k$ is incomplete, a contradiction.

Case:-II

If N is a composite number, then by Theorem 1.4.1, it must have a prime factor. Since $p_i \mid (N-1)$, so $p_i \nmid N$. Thus the prime factor is not in the list of primes $p_1, p_2, p_3, \ldots, p_k$. So, the list is again incomplete, which is again contradiction.

Thus the number of primes are infinite. □

We know that the sum $\sum\limits_{n \in \mathbb{N}} \frac{1}{n}$ diverges. Now, we take the sum of reciprocals of all primes and see that the sum again diverges.

Theorem 1.4.6 (Euler)**.** The infinite series $\sum\limits_{n=1}^{\infty} \frac{1}{p_n}$ diverges.

Proof. See ([1]) □

Next we state fundamental theorem of arithmetic without proof.

Theorem 1.4.7 (Fundamental theorem of arithmetic)**.** Every integer $n > 1$ can be represented as a product of prime factors in only one way, apart from the order of the factors.

That is, if the prime factors of n are $p_1, p_2, \ldots, p_r$ and if p_i occurs as a factor a_i times, then

$$n = p_1^{a_1} p_2^{a2} \ldots p_r^{a_r}.$$

[This form is known as **canonical form**.]

Exercise 1.4.1. Show that if $2^n - 1$ is prime, then n is prime.

Exercise 1.4.2. Show that if $2^n + 1$ is prime, then n is a power of 2.

Exercise 1.4.3. Show that $n^4 + 4$ is composite if $n > 1$.

1.5 Greatest integer function

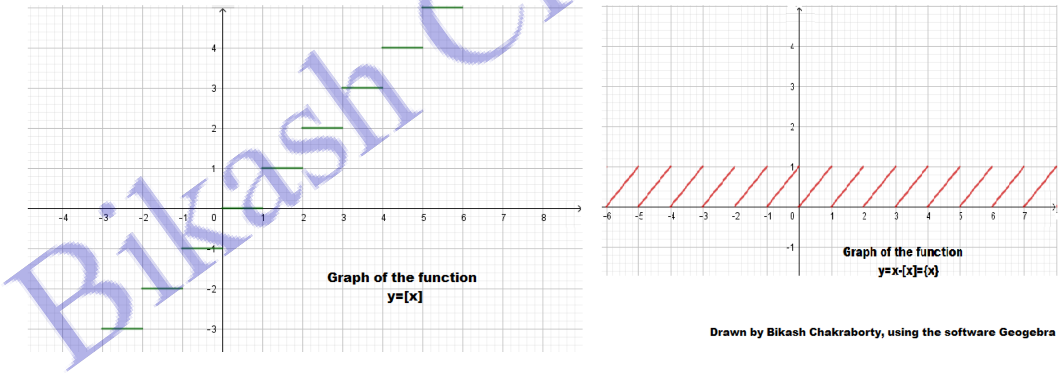
Let x be any real number, then by Archimedean property, there exists an integer n such that

$$n \leq x < n + 1.$$

Thus x can be expressed as

$$x = n + f,$$

where $0 \leq f < 1$. The "integral part of x" is denoted by $[x]$ and "fractional part of x" is denoted by $\{x\}$. Thus the fractional part is the sawtooth function and a periodic function with period 1.



Graph of the function y=[x]

Graph of the function y=x-[x]={x}

Drawn by Bikash Chakraborty, using the software Geogebra

Example 1.5.1. i. If $x = 3.4$, then $[x] = 3$ and $\{x\} = 0.4$.

ii. If $x = 0.4$, then $[x] = 0$ and $\{x\} = 0.4$.

iii. If $x = -0.4$, then $x = -1 + 0.6$, i.e., $[x] = -1$ and $\{x\} = 0.6$.

iv. If $x = -3.4$, then $x = -4 + 0.6$, i.e., $[x] = -4$ and $\{x\} = 0.6$.

Example 1.5.2. i. If $-2 \leq x < -1$, then $[x] = -2$.

ii. If $-1 \leq x < 0$, then $[x] = -1$.

iii. If $0 \leq x < 1$, then $[x] = 0$.

iv. If $1 \leq x < 2$, then $[x] = 1$.

Remark 1.5.1. For two real numbers, x and y,

$$[x + y] \geq [x] + [y].$$

Solution:
Let $x = n_1 + f_1$ and $y = n_2 + f_2$, where $0 \leq f_1, f_2 < 1$. Thus $[x] + [y] = n_1 + n_2$, but $[x + y] \geq n_1 + n_2$ as $f_1 + f_2$ may be greater than 1. Thus equality occurs if $0 \leq f_1 + f_2 < 1$ and $[x] + [y] + 1 = [x + y]$ if $1 \leq f_1 + f_2 < 2$.

Definition 1.5.1. Let p be a prime and $x \in \mathbb{Z}, x \neq 0$. The p-**adic valuation of** x, denoted by $v_p(x)$ is defined as the largest non-negative integer e such that p^e divides x. In other words, $v_p(x)$ is the exact exponent of p in the prime factorization of x.

Also, by definition, $v_p(0) = +\infty$.

Theorem 1.5.1 (Legendre's theorem). The largest exponent e of a prime p such that $p^e \mid n!$ is given by

$$e = v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$$

Remark 1.5.2. We have seen that the formula on the right side is an infinite sum, but for any particular values of n and p, it has only finitely many nonzero terms. Because, for every i large enough that $p^i > n$, one has $[\frac{n}{p^i}] = 0$.

Proof of the Legendre's theorem: Given

$$n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n.$$

Let $p, 2p, 3p, \ldots, mp$ are the all positive integral multiple of p not exceeding n. Then $mp \leq n < (m + 1)p$, i.e., $[\frac{n}{p}] = m$. Thus there are $\left[\frac{n}{p}\right]$ integers below n that contribute a factor of p.

Out of these $\left[\frac{n}{p}\right]$ integers, $\left[\frac{n}{p^2}\right]$ contribute a second factor; and among those $[\frac{n}{p^3}]$ contribute a third factor p, and so on.

Thus the total number of times p divides $n!$ is

$$e = v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots.$$

□

Example 1.5.3. Find the highest power of 3 contained in $20!$.

Solution:
There are $[\frac{20}{3}] = 6$ integers, namely, $3, 6, 9, 12, 15, 18$ which are divisible by 3. Out of these 6 integers, $[\frac{20}{3^2}] = 2$ integers, namely, $9, 18$ which are divisible by 3^2. Out of these integers, $[\frac{20}{3^3}] = 0$ integers which are divisible by 3^3.

Thus the highest power of 3 contained in $20!$ is $6 + 2 + 0 = 8$.

Example 1.5.4. Show that $v_p(n!) = \frac{n-1}{p-1}$, where $n = p^r$.

Solution:

$$\begin{aligned} v_p(n!) &= \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^{r-1}}\right] + \left[\frac{n}{p^r}\right] \\ &= p^{r-1} + p^{r-2} + \ldots + p + 1 \\ &= \frac{p^r - 1}{p-1} \\ &= \frac{n-1}{p-1}. \end{aligned}$$

Example 1.5.5. The product of n consecutive positive integers is divisible by $n!$.

Solution:
Let the product be

$$(m+1)(m+2)\ldots(m+n) = \frac{(m+n)!}{m!}.$$

Claim: $\frac{(m+n)!}{m!n!}$ is an integer.

Let p be any prime factor of $m!n!$. Then p must be a factor of $(m+n)!$.

Let r, s and t be the largest exponents of the prime p in $m!$, $n!$ and $(m+n)!$ respectively. Now using the fact that $[x+y] \geq [x] + [y]$, we have

$$\begin{aligned} t &= \left[\frac{m+n}{p}\right] + \left[\frac{m+n}{p^2}\right] + \left[\frac{m+n}{p^3}\right] + \ldots, \\ &\geq \left(\left[\frac{m}{p}\right] + \left[\frac{n}{p}\right]\right) + \left(\left[\frac{m}{p^2}\right] + \left[\frac{n}{p^2}\right]\right) + \left(\left[\frac{m}{p^3}\right] + \left[\frac{n}{p^3}\right]\right)\ldots, \\ &= r + s. \end{aligned}$$

Thus $m!n!$ must be a divisor of $(m+n)!$. Hence the proof.

Exercise 1.5.1. For a real number x

$$\begin{aligned} [x] + [-x] &= 0, \text{if } x \text{ is an integer} \\ &= -1, \text{otherwise.} \end{aligned}$$

Exercise 1.5.2. For a real number x

$$[x] + [x + \frac{1}{2}] = [2x].$$

Exercise 1.5.3. For a real number x

$$[x] + \left[x + \frac{1}{3}\right] + \left[x + \frac{2}{3}\right] = [3x].$$

Exercise 1.5.4. Find the highest power of 5 contained in $140!$.

Exercise 1.5.5. Show that $6 \mid n(n+1)(n+2)$ where $\in \mathbb{Z}$.

Exercise 1.5.6. If $n > 1$, then show that the sum $\sum\limits_{k=1}^{n} \frac{1}{k}$ is not an integer.

Chapter 2

Number theoretic functions

2.1 Introduction

The **fundamental theorem of arithmetic** tells us that "every integer $n > 1$ can be expressed as a product of prime factors in only one way, apart from the order of the factors."

If the distinct prime factors of n are $p_1, p_2, \ldots p_r$ and if p_i occurs as a factor a_i times, then

$$n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}.$$

Definition 2.1.1. A function $f : \mathbb{N} \to \Phi$, where $\Phi \subseteq \mathbb{R}$, or $\Phi \subseteq \mathbb{C}$, is called a **number theoretic function**, i.e., the domain of the function is the set of natural numbers.

A number theoretic function f is called **multiplicative** if it is not identically zero and if

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

A multiplicative function f is called **completely multiplicative** if

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

Example 2.1.1. Let $f_\alpha = n^\alpha$, where α is a fixed real or complex number. Clearly f_α is a completely multiplicative function.

2.2 The Möbius function $\mu(n)$

Definition 2.2.1. The Möbius function $\mu : \mathbb{N} \to \mathbb{R}$ is defined as follows:

$$\begin{aligned} \mu(n) &= 1 && \text{if } n = 1, \\ &= (-1)^r && \text{if } a_1 = a_2 = \ldots = a_r = 1, \\ &= 0 && \text{otherwise} \end{aligned}$$

Definition 2.2.2. The identity function $I(n)$ is defined as

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

Theorem 2.2.1. If $n \geq 1$, then $\sum\limits_{d|n} \mu(d) = I(n)$.

Proof. For $n = 1$, the result is true. Let $n > 1$ and $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$. If d is factor of n and $p_i^2 \mid d$, then $\mu(d) = 0$. Thus

$$\begin{aligned} &\sum_{d|n} \mu(d) \\ =\ & \mu(1) + \sum_{i=1}^{r} \mu(p_i) + \sum \mu(p_i p_j) + \sum \mu(p_i p_j p_k) + \ldots + \mu(p_1 p_2 \ldots p_k) \\ =\ & 1 + \binom{k}{1}(-1)^k + \binom{k}{2}(-1)^2 + \ldots + \binom{k}{k}(-1)^k \\ =\ & (1-1)^k \\ =\ & 0. \end{aligned}$$

□

2.3 The Euler totient function $\varphi(n)$

Definition 2.3.1. The Euler totient function $\varphi : \mathbb{N} \to \mathbb{R}$ is defined to be the number of positive integers not exceeding n which are relatively prime to n.

Now, we state the relationship between the Möbius function $\mu(n)$ and the Euler totient function $\varphi(n)$ without proof:

Theorem 2.3.1. If $n \geq 1$, we have

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

Theorem 2.3.2. If $n \geq 1$, then

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

Proof. For $n = 1$, there is nothing prove. Let $n > 1$ and $p_1, p_2, \ldots, p_r$ be the distinct prime divisors of n. Now, if d is a divisor of n, then d can expressed as product of some primes p_i for $1 \leq i \leq r$, and

$$\begin{aligned} \mu(d) &= 0 \text{ if } p_i^2 \mid d \text{ for some } i, \\ &= \pm 1, \text{ otherwise.} \end{aligned}$$

Now,

$$\begin{aligned}
\prod_{p|n}(1-\frac{1}{p}) &= \prod_{i=1}^{r}(1-\frac{1}{p_i}) \\
&= 1-\sum\frac{1}{p_i}+\sum\frac{1}{p_ip_j}-\sum\frac{1}{p_ip_jp_k}+\ldots+\sum\frac{(-1)^r}{p_1p_2\ldots p_r} \\
&= \frac{1}{1}+\sum\frac{(-1)}{p_i}+\sum\frac{(-1)^2}{p_ip_j}+\sum\frac{(-1)^3}{p_ip_jp_k}+\ldots+\sum\frac{(-1)^r}{p_1p_2\ldots p_r} \\
&= \sum_{d|n}\frac{\mu(d)}{d} \\
&= \frac{\varphi(n)}{n}, \quad \text{by} \quad \text{Theorem} \quad 2.3.1.
\end{aligned}$$

This completes the proof. □

Theorem 2.3.3. If $m, n \in \mathbb{N}$ and $\gcd\{m, n\} = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.

Proof. Let $m = p_1^{a_1}p_2^{a_2}\ldots p_r^{a_r}$ and $n = q_1^{b_1}q_2^{b_2}\ldots q_s^{b_s}$. Since $\gcd\{m, n\} = 1$, so

$$mn = p_1^{a_1}p_2^{a_2}\ldots p_r^{a_r}q_1^{b_1}q_2^{b_2}\ldots q_s^{b_s}, \qquad \gcd\{p_i, q_j\} = 1.$$

Now, the result follows from Theorem 2.3.2. □

Remark 2.3.1. Thus the Euler totient function $\varphi(n)$ is multiplicative, but not completely multiplicative, as $\varphi(8) \neq \varphi(2)\varphi(4)$.

Theorem 2.3.4. If p be a prime and k be natural number, then

$$\varphi(p^k) = p^k - p^{k-1}.$$

Proof. The proof follows from Theorem 2.3.2. But, here we give another tricky proof.

Clearly, $\varphi(p^k)$ counts those natural numbers which are $\leq p^k$ and prime to p^k, i.e, $\varphi(p^k)$ counts those natural numbers which are $\leq p^k$ and not of the form $t \cdot p$, where $p \leq t \cdot p \leq p^k$, (i.e., $1 \leq t \leq p^{k-1}$). Thus

$$\varphi(p^k) = p^k - p^{k-1}.$$

□

Theorem 2.3.5. $\varphi(n)$ is even for $n \geq 3$.

Proof. If $n = 2^p$ with $p \geq 2$, then $\varphi(n) = 2^{p-1}$, which is even.

If n has at least one odd prime factor, then n can be written as $n = p^\alpha q$ with $\gcd\{p, q\} = 1$. Then $\varphi(n) = \varphi(p^\alpha)\varphi(q) = p^{\alpha-1}(p-1)\varphi(q)$, which is even. □

Theorem 2.3.6. Let $n \geq 2$. Then the sum of all positive integers less than n and prime to n is $\frac{1}{2}n\varphi(n)$.

Proof. Let those integers be

$$a_1, a_2, \ldots, a_{\varphi(n)}.$$

Claim: If $\gcd\{b, n\} = 1$, then $\gcd\{b, n-b\} = 1$.

If $\gcd\{b, n\} = 1$, then there exists integers u, v such that $ub + nv = 1$, i.e, $(u+v)b + v(n-b) = 1$. Thus $\gcd\{b, n-b\} = 1$.

Hence, $n - a_1, n - a_2, \ldots, n - a_{\varphi(n)}$ are the complete list of integers less than n and prime to n. Thus

$$\begin{aligned} S &= a_1 + a_2 + \ldots + a_{\varphi(n)} \\ &= (n - a_1) + (n - a_2) + \ldots + (n - a_{\varphi(n)}) \\ &= n\varphi(n) - S. \end{aligned}$$

Thus $S = \frac{1}{2}n\varphi(n)$. □

Exercise 2.3.1. Let $n \geq 2$. Then the average of all positive integers less than n and prime to n is $\frac{n}{2}$.

2.4 The Dirichlet product

Definition 2.4.1. Let f and g be two number theoretic functions. We define the Dirichlet product of them as a new number theoretic function h as follows:

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

We write $f * g$ for h.

Remark 2.4.1. We have seen in Theorem 2.3.1, that

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

Thus $\varphi = \mu * N$, where N is defined as $N(n) = n$ for all $n \in \mathbb{N}$.

Theorem 2.4.1 (Commutative Law)**.** For any two number theoretic functions f and g, we have

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

Proof. $(f * g)(n) = \sum\limits_{d|n} f(d)g(\frac{n}{d}) = \sum\limits_{d'|n} f(\frac{n}{d'})g(d') = (g * f)(n).$ □

Theorem 2.4.2 (Associative Law)**.** For any three number theoretic functions f, g and k, we have

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

Proof. Let $f * g = B$. Then

$$\begin{aligned}
(B * k)(n) &= \sum_{dd'=n} B(d)k(d') \\
&= \sum_{dd'=n} \left(\sum_{d_1 d_2 = d} f(d_1)g(d_2) \right) k(d') \\
&= \sum_{d_1 d_2 d' = n} f(d_1)g(d_2)k(d').
\end{aligned}$$

Similarly, we can compute $f * (g * k)(n)$ and observe the associativity of Dirichlet product. □

Theorem 2.4.3 (Existence of identity element)**.** For any number theoretic function f, we have

$$f * I = I * f = f.$$

Proof. Clearly, $(f * I)(n) = \sum\limits_{d|n} f(d)I(\frac{n}{d}) = f(n)I(1) = f(n)$.
This completes the proof. □

Theorem 2.4.4. If f is a number theoretic function with$f(1) \neq 0$, then there exist a unique number theoretic function f^{-1}, called the Dirichlet inverse of f, such that

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

Proof. Since Dirichlet product is commutative, so we shall prove that $(f * f^{-1})(n) = I(n)$ has unique solution for the function values $f^{-1}(n)$. We will establish this by mathematical induction.

For $n = 1$, we obtain $f(1)f^{-1}(1) = 1$. As $f(1) \neq 0$, so $f^{-1}(1) = \frac{1}{f(1)}$.

Next we assume that $f^{-1}(k)$ can be determined for all $k < n$. Now,

$$\sum_{d|n} f(\frac{n}{d})f^{-1}(d) = I(n),$$

gives

$$f(1)f^{-1}(n) + \sum_{d|n, d<n} f(\frac{n}{d})f^{-1}(d) = I(n) = 0,$$

Since all the values of $f^{-1}(d)$ for $d \mid n, d < n$ are known and $f(1) \neq 0$, so we can determine $f^{-1}(n)$. □

Remark 2.4.2. Thus f^{-1} is given by

$$f^{-1}(1) = \frac{1}{f(1)}, \quad f^{-1}(n) = \frac{-1}{f(1)} \sum_{d|n, d<n} f(\frac{n}{d})f^{-1}(d) \text{ for } n > 1.$$

Remark 2.4.3. The set of all number theoretic functions f with $f(1) \neq 0$ forms an abelian group with respect to the binary operation $*$.

Theorem 2.4.5 (Möbius inversion formula). The equation

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

gives

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

Proof. Let us first define unit function $u(n)$ as

$$u(n) = 1 \quad \text{for all} \quad n.$$

Given that $f = g * u$. Also, from Theorem 2.2.1, we obtain $\sum_{d|n} \mu(d) = I(n)$, i.e., $\mu * u = I$.

Now,

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

This completes the proof. □

Theorem 2.4.6 (Converse part of Möbius inversion formula). If

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

then

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

Proof. Given that $g = f * \mu$. Also, from Theorem 2.2.1, we obtain $\sum_{d|n} \mu(d) = I(n)$, i.e., $\mu * u = I$.

Now,

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

This completes the proof. □

Exercise 2.4.1. For any positive integer n, show that

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

Exercise 2.4.2. Using Möbius inversion formula, show that

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

Exercise 2.4.3. If f and g be two number theoretic functions with $f(1) \neq 0$ and $g(1) \neq 0$, then

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

Theorem 2.4.7. If f and g are multiplicative, then their Dirichlet product $f * g$ is also multiplicative.

Proof. Let $h = f * g$ and $m, n \in \mathbb{N}$ with $\gcd\{m, n\} = 1$. If $c \mid mn$, then there exist a, b such that $c = ab$ and $a \mid m$, $b \mid n$. Also, $\gcd\{a, b\} = 1$. Now,

$$\begin{aligned} h(mn) &= \sum_{c|mn} f(c)g(\frac{mn}{c}) \\ &= \sum_{a|m, b|n} f(ab)g(\frac{mn}{ab}) \\ &= \sum_{a|m, b|n} f(a)f(b)g(\frac{m}{a})g(\frac{n}{b}) \\ &= \sum_{a|m} f(a)g(\frac{m}{a}) \sum_{b|n} f(b)g(\frac{n}{b}) \\ &= h(m)h(n). \end{aligned}$$

This completes the proof. □

2.5 The divisor functions $\sigma_\alpha(n)$

Definition 2.5.1. For real or complex number α and any integer $n \geq 1$, we define

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

This function is known as **divisor function**.

Theorem 2.5.1. The divisor function $\sigma_\alpha(n)$ is multiplicative.

Proof. Let us first define unit function $u(n)$ as

$$u(n) = 1 \quad \text{for all} \quad n.$$

Clearly, $u(n)$ is multiplicative function. Also,

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha = u * N^\alpha.$$

Since Dirichlet product of two multiplicative functions is multiplicative, so the divisor function $\sigma_\alpha(n)$ is multiplicative. □

Example 2.5.1. Compute $\sigma_\alpha(p^a)$, where $a \geq 0$ and p is a prime.

Solution:
Since the positive divisors of p^a are $1, p, p^2, \ldots, p^a$, so

$$\begin{aligned}\sigma_\alpha(p^a) = 1^a + p^a + p^{2a} + \ldots + p^{a\alpha} &= \frac{p^{\alpha(a+1)-1}}{p^\alpha - 1} \text{ if } \alpha \neq 0 \\ &= a + 1 \text{ if } \alpha = 0.\end{aligned}$$

Example 2.5.2. Compute $\sigma_\alpha(n)$, where $n \geq 1$.

Solution:
If the distinct prime factors of n are $p_1, p_2, \ldots p_r$ and if p_i occurs as a factor a_i times, then

$$n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}.$$

Since the divisor function $\sigma_\alpha(n$ is multiplicative, so

$$\sigma_\alpha(n) = \sigma_\alpha(p_1^{a_1})\sigma_\alpha(p_2^{a_2}) \ldots \sigma_\alpha(p_r^{a_r}).$$

Rest part is left as an exercise for the reader.

Definition 2.5.2. If $\alpha = 0$, then $\sigma_0(n)$ is the number of divisors of n, and this is denoted by $\tau(n)$.

Definition 2.5.3. If $\alpha = 1$, then $\sigma_1(n)$ is the sum of divisors of n, and this is denoted by $\sigma(n)$.

Theorem 2.5.2. If $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$, then $\tau(n) = (1 + a_1)(1 + a_2) \ldots (1 + a_r)$.

Theorem 2.5.3. If $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$, then

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_r^{a_r+1} - 1}{p_r - 1}.$$

Example 2.5.3. Show that the product of all positive divisors of a positive integer $n > 1$ is $n^{\frac{\tau(n)}{2}}$.

Solution:
If d is a positive integer of n, then there exist a positive integer d' such that $dd' = n$. Now

$$\begin{aligned} n^{\tau(n)} &= \prod_{d|n} n \\ &= \prod_{d|n} dd' \\ &= \prod_{d|n} d \prod_{d'|n} d' \\ &= (\prod_{d|n} d)^2. \end{aligned}$$

Thus $\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$.

Exercise 2.5.1. Show that $\tau(n)$ is a odd number if and only if n is a perfect square.

Exercise 2.5.2. If $d_1, d_2, \dots, d_k$ be the list of all positive divisors of n, then

$$\frac{1}{d_1} + \frac{1}{d_2} + \dots + \frac{1}{d_k} = 2.$$

Definition 2.5.4. A positive integer n is said to be a **perfect number** if $\sigma(2n) = 2n$.

If n is a perfect number and $n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$, then

$$\begin{aligned} & 2n \\ = & (1 + p_1 + \dots + p_1^{a_1}) \cdot (1 + p_2 + \dots + p_2^{a_2}) \cdot \dots \cdot (1 + p_r + \dots + p_r^{a_r}) \\ = & \sum_{i_1, i_2, \dots, i_r} p_1^{i_1} p_2^{i_2} \dots p_r^{i_r}, \quad \text{where } 0 \le i_1 \le a_1, \dots, 0 \le i_r \le a_r \end{aligned}$$

Thus

$$\begin{aligned} & n \\ = & 2n - p_1^{a_1} p_2^{a_2} \dots p_r^{a_r} \\ = & \left(\sum_{i_1, i_2, \dots, i_r} p_1^{i_1} p_2^{i_2} \dots p_r^{i_r} \right) - p_1^{a_1} p_2^{a_2} \dots p_r^{a_r} \end{aligned}$$

That is, n is the sum of all positive divisors excluding itself.

The first perfect number is 6, as $1 + 2 + 3 = 6$. The next perfect number is 28, as $28 = 1 + 2 + 4 + 7 + 14$.

Exercise 2.5.3. If n be an odd positive integer, then

$$\varphi(2n) = \varphi(n).$$

Exercise 2.5.4. If n be an even positive integer, then

$$\varphi(2n) = 2\varphi(n).$$

Exercise 2.5.5. If n be the product of two successive odd primes, then

$$\varphi(n)\sigma(n) = (n+1)(n-3).$$

Exercise 2.5.6. Let $k > 1$ be¡ a integer. If $2^k - 1$ is a prime, then $2^{k-1}(2^k - 1)$ is a perfect number.

Chapter 3

Congruences

3.1 Introduction

Gauss introduced the notation of Congruence. Congruence is an equivalence relation on the set of integers.

Definition 3.1.1. Let $a, b \in \mathbb{Z}$ and m be a natural number. By "a is congruent to b modulo m", we mean that $m \mid a - b$. In this case, we write $a \equiv b \pmod{m}$ or, $a \equiv_m b$.

Example 3.1.1. Let $n \in \mathbb{N}$.

i) n is even if and only if $n \equiv 0 \pmod{2}$.

ii) n is odd if and only if $n \equiv 1 \pmod{2}$.

Theorem 3.1.1. Congruence is an equivalence relation on $\mathbb{Z}$.

Proof. Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$. Let us define a relation $\equiv_m$ on $\mathbb{Z}$ by $a \equiv_m b$ if and only if $m \mid a - b$.

Then $\equiv_m$ is reflexive as $m \mid a - a$.

Let $a \equiv_m b$ holds. Then $m \mid a - b$, i.e., $m \mid b - a$. Thus $b \equiv_m a$ holds. So $\equiv_m$ is symmetric.

Now let $a \equiv_m b$ and $b \equiv_m c$ hold for some integers $a, b, c \in \mathbb{Z}$. Then $m \mid a - b$ and $m \mid b - c$. That is, $m \mid (a - b) + (b - c)$. So, $\equiv_m$ is transitive.
Thus "$\equiv_m$" is an equivalence relation on $\mathbb{Z}$. □

Theorem 3.1.2. If $a \equiv b \pmod{m}$ and $\alpha \equiv \beta \pmod{m}$, then

i) $ax + \alpha y \equiv bx + \beta y \pmod{m}$ for all integers x and y.

ii) $a\alpha \equiv b\beta \pmod{m}$.

iii) $a^n \equiv b^n \pmod{m}$ for all natural number n.

iv) $f(a) \equiv f(b) \pmod{m}$ for every polynomial f with integer coefficients.

Proof. i) Since $m \mid (a-b)$ and $m \mid (\alpha - \beta)$, so for any two integers x and y, $m \mid x(a-b) + y(\alpha - \beta)$. Thus $ax + \alpha y \equiv bx + \beta y \pmod{m}$ for all integers x and y.

ii) Putting $x = \alpha$ and $y = b$ in (i), we have $a\alpha \equiv b\beta \pmod{m}$.

iii) Let $P(n)$ be a statement that $a^n \equiv b^n \pmod{m}$ for all natural number n.

It is given that $P(1)$ is true. Assume that $P(k)$ is true for a positive integer $k \geq 1$. Thus $a \equiv b \pmod{m}$ and $a^k \equiv b^k \pmod{m}$. Thus by (ii), $a^{k+1} \equiv b^{k+1} \pmod{m}$, i.e., $P(k+1)$ is true. So by mathematical induction, the claim is true.

iv) Let $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_lx^l$ be a polynomial of degree l with integer coefficients. Then by (ii) and (iii), we have

$$\begin{aligned}
a_0 &\equiv a_0 \pmod{m},\\
a_1a &\equiv a_1b \pmod{m},\\
a_2a^2 &\equiv a_2b^2 \pmod{m},\\
\ldots &\ldots \ldots\\
a_{l-1}a^{l-1} &\equiv a_{l-1}b^{l-1} \pmod{m},\\
a_la^l &\equiv a_lb^l \pmod{m}.
\end{aligned}$$

Now applying (i), we have $f(a) \equiv f(b) \pmod{m}$.

□

Example 3.1.2. The numbers of the form $F_n = 2^{2^n}$ are called Fermat's Numbers. It is easy to check that F_0, F_1, F_2, F_3 and F_4 are primes. Moreover, Fermat thought that F_n is prime for every $n \in \mathbb{N}$, but, in 1732, Euler found that F_5 is composite.

Since $2^{16} = 65536 \equiv 154 \pmod{641}$, so

$$\begin{aligned}
2^{32} &\equiv (154)^2 \pmod{641}\\
&\equiv 23716 \pmod{641}\\
&\equiv 640 \pmod{641}\\
&\equiv -1 \pmod{641}.
\end{aligned}$$

That is, $641 \mid F_5$.

Example 3.1.3. Let

$$n = a_m(10)^m + a_{m-1}(10)^{m-1} + \ldots + a_2(10)^2 + a_1(10)^1 + a_0,$$

where $0 \leq a_i \leq 9$. Let

$$S = a_0 + a_1 + \ldots + a_m.$$

Show that

i. $2 \mid n$ if and only if $2 \mid a_0$.

ii. $9 \mid n$ if and only if $9 \mid S$.

Solutions:
Let $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_0$ be a polynomial with integer coefficients.

i. Now,

$$\begin{aligned} 10 &\equiv 0 \pmod{2} \\ i.e., \quad f(10) &= f(0) \pmod{2} \\ i.e., \quad n &= a_0 \pmod{2} \end{aligned}$$

Thus $2 \mid (n - a_0)$. Hence, $2 \mid n$ if and only if $2 \mid a_0$.

ii. Again,

$$\begin{aligned} 10 &\equiv 1 \pmod{9} \\ i.e., \quad f(10) &= f(1) \pmod{9} \\ i.e., \quad n &= S \pmod{9} \end{aligned}$$

Thus $9 \mid (n - S)$. Hence, $9 \mid n$ if and only if $9 \mid S$.

Exercise 3.1.1. Let

$$n = a_m(1000)^m + a_{m-1}(1000)^{m-1} + \ldots + a_2(1000)^2 + a_1(1000)^1 + a_0,$$

where $0 \leq a_i \leq 9$. Let

$$T = a_0 - a_1 + \ldots + (-1)^m a_m.$$

Show that

i. $7 \mid n$ if and only if $7 \mid T$.

ii. $11 \mid n$ if and only if $11 \mid T$.

iii. $13 \mid n$ if and only if $13 \mid T$

Example 3.1.4. Show that $17 \mid (2^{3n+1} + 3 \cdot 5^{2n+1})$ for every natural number n.
Solutions:
Clearly,

$$\begin{aligned} & 2^{3n+1} + 3 \cdot 5^{2n+1} \\ = \quad & 2 \cdot 8^n + 15 \cdot 25^n \end{aligned}$$

And,

$$\begin{aligned} 25 &\equiv 8 \pmod{17} \\ So, \quad 25^n &= 8^n \pmod{17} \\ i.e., \quad 15 \cdot (25)^n &= 15 \cdot (8)^n \pmod{17} \\ i.e., \quad 15 \cdot (25)^n &= (-2) \cdot (8)^n \pmod{17}. \end{aligned}$$

Thus $17 \mid (2^{3n+1} + 3 \cdot 5^{2n+1})$ for every natural number n.

Exercise 3.1.2. Show that $3(4^{n+1}-1)$ is divisible by 9.

Theorem 3.1.3 (Wilson's Theorem). If p be a prime, then $p \mid (p-1)!+1$.

Proof. First we show that 1 and $p-1$ are only elements which has self-inverse in $\mathbb{Z}_p$. Let $1 \leq a \leq p-1$ and $a^2 \equiv 1 \pmod{p}$. Then

$$p \mid a-1, \text{ or, } p \mid a+1.$$

Since $0 \leq a-1 \leq p-2$ and $2 \leq a+1 \leq p$, so $a=1$ or, $a=p-1$.

Next, we show that every element $b \in \{2,\dots,p-2\}$ has unique inverse mod p in $\{2,\dots,p-2\}$.

Since $\gcd\{b,p\}=1$, then there exists integers u and v such that

$$bu+pv=1.$$

Again, by division algorithm, there exist integers t and c such that

$$u=pt+c, \quad 0 \leq c \leq p-1.$$

Since $\gcd\{b,p\}=1$, so $c \neq 0$. Now, $bc+p(bt+v)=1$, i.e., $bc \equiv 1 \pmod{p}$. Also, $c \neq 1, p-1$, as $1, p-1$ are self inverse elements (mod p).

Thus c is the inverse element of b with respect to (mod p).

Now we have to show that each $b \in \{2,\dots,p-2\}$ has unique inverse with respect to (mod p). If not, assume that $bc \equiv 1 \pmod{p}$ and $bc' \equiv 1 \pmod{p}$ for some $c, c' \in \{2,3,\dots,p-2\}$. Then

$$b(c-c') \equiv 0 \pmod{p}.$$

But $\gcd\{b,p\}=1$ and $0 \leq \mid c-c' \mid < p$, so $p \mid (c-c')$, so $c=c'$.

From the above discussion, it is clear that

$$\begin{aligned}
2\cdot 3 \cdot \cdot 4 \cdot \ldots \cdot (p-2) &\equiv 1 \pmod{p},\\
\text{i.e., } (p-2)! &\equiv 1 \pmod{p},\\
\text{i.e., } (p-1)! &\equiv 1 \times (p-1) \pmod{p},\\
\text{i.e., } (p-1)!+1 &\equiv (p-1)+1 \pmod{p},\\
\text{i.e., } (p-1)!+1 &\equiv p \pmod{p},\\
\text{i.e., } (p-1)!+1 &\equiv 0 \pmod{p}.
\end{aligned}$$

□

Next, we show that the converse part of the Wilson's Theorem is also true.

Theorem 3.1.4. Let $n(>1)$ be a natural number such that $n \mid (n-1)!+1$. Then n is a prime number.

Proof. For a contradiction, we assume that $n = uv$ and $1 \lneqq u,\ v \lneqq n$. Since $u \mid n$ and $n \mid (n-1)! + 1$, so

$$u \mid (n-1)! + 1. \tag{3.1.1}$$

As $(n-1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot u \cdot \ldots \cdot (n-1)$, so

$$u \mid (n-1)!. \tag{3.1.2}$$

Thus from equations (3.1.1) and (3.1.2), we obtain $u \mid 1$, i.e., $u = 1$, a contradiction. Thus n must be a prime. □

Example 3.1.5. Find the remainder of $97!$ when divided by 101.

Solution:
First we will apply Wilson's theorem to note that $100! \equiv -1 \pmod{101}$. When we decompose the factorial, we get that

$$(100)(99)(98)(97!) \equiv -1(\text{mod}\ \ 101).$$

Now, we note that $100 \equiv -1(\text{ mod }\ 101)$, $99 \equiv -2 \pmod{101}$, and $98 \equiv -3(\text{ mod }\ 101)$. Hence

$$(-1)(-2)(-3)(97!) \equiv -1(\text{mod}\ \ 101).$$

Now, we want to the inverse of 6 in $(\text{mod} 101)$. Using the division algorithm, we get that

$$\begin{aligned} 101 &= 6(16) + 5, \\ 6 &= 5(1) + 1, \\ 5 &= 5(1) + 0. \end{aligned}$$

Thus $1 = 6 + [101 + 6(-16)](-1)$, i.e., $1 = 101(-1) + 6(17)$. Hence, 17 can be used as an inverse for $6 \pmod{101}$. Thus

$$\begin{aligned} 6(97!) &\equiv 1(\text{mod}\ \ 101), \\ (17)(6)(97!) &\equiv (17)1 \pmod{101}, \\ 97! &\equiv 17 \pmod{101} \end{aligned}$$

Hence, $97!$ has a remainder of 17 when divided by 101.

Exercise 3.1.3. Find the remainder of $67!$ when divided by 71.

3.2 Residue classes

Let $a, b \in \mathbb{Z}$ and m be a natural number. We have already defined a congruent relation on $\mathbb{Z}$ by a is related to b if and only if "a is congruent to b modulo m". Since this relation is an equivalence relation on $\mathbb{Z}$, so it gives a partition on $\mathbb{Z}$. Each "equivalence classes" are known as **Residue classes**.

Definition 3.2.1. Let $a \in \mathbb{Z}$ and m be a natural number. Then **Residue class** of a modulo m is denoed by $\overline{a}$ and defined by

$$\overline{a} := \{x \ : \ x \equiv a \pmod{m}\}.$$

That is, $x = a + qm$, for some $q \in \mathbb{Z}$

Example 3.2.1. Let $n \in \mathbb{Z}$. Then by Division Algorithm, $n = 5q + r$, where $q \in \mathbb{Z}$ and $r = 0, 1, \dots, 4$. Thus $\overline{0}$ contains all those integers which are divisible by 5. Similarly, $\overline{1}$ contains all those integers which gives remainder one after division by 5. and so on.

Thus $\mathbb{Z} = \overline{0} \cup \overline{1} \cup \dots \cup \overline{4}$.

Also, we observed that if $x \in \overline{3}$, then x gives remainder 3 when it is divided by 5, i.e, $5 \mid (x - 3)$, i.e., $x \equiv 3 \pmod{5}$.

Now, the following results are immediate from the discussion of elementary set theory.

Theorem 3.2.1. Let $a, b \in \mathbb{Z}$ and m be a natural number.

i. $\overline{a} = \overline{b}$ if and only if $a \equiv b \pmod{m}$.

ii. Two integers x and y are in same residue class if and only if $x \equiv y \pmod{m}$.

iii. The m residue classes $\overline{1}, \overline{2}, \dots, \overline{m}$ are disjoint and their union is $\mathbb{Z}$.

Proof. Proofs are left as exercises. □

Exercise 3.2.1. Let $a, b \in \mathbb{Z}$ and m be a natural number. We denote by $\mathbb{Z}_m := \{\overline{1}, \overline{2}, \dots, \overline{m}\}$ and we also define two binary operations on $\mathbb{Z}_m$ as

$$\overline{a} \oplus \overline{b} = \overline{(a + b)},$$

and

$$\overline{a} \odot \overline{b} = \overline{(a \cdot b)}.$$

Check that these two binary operations are well-defined.

Exercise 3.2.2. Let m be a natural number. Then prove that $(\mathbb{Z}_m, \oplus)$ is a cyclic group.

Remark 3.2.1. In $\mathbb{Z}_4$, we can check that $\overline{2}\odot\overline{0}=\overline{0}$, $\overline{2}\odot\overline{1}=\overline{2}$, $\overline{2}\odot\overline{2}=\overline{0}$, $\overline{2}\odot\overline{3}=\overline{2}$. So, there is no element $\overline{x}\in\mathbb{Z}_4$ such that $\overline{2}\odot\overline{x}=\overline{1}$. Thus not all elements in $\mathbb{Z}_m$ has multiplicative inverses.

Let $\overline{n}\in\mathbb{Z}_m$ with $\gcd\{n,m\}=1$. Then there exist integers n' and m' such that $nn'+mm'=1$, i.e., $\overline{n}\odot\overline{n'}\equiv 1$ (mod m).

Conversely, if for some $\overline{n}\in\mathbb{Z}_m$, there exist integers n' such that $\overline{n}\odot\overline{n'}\equiv 1$ (mod m) holds, then $\gcd\{n,m\}=1$.

Thus we can easily sort out the elements of $\mathbb{Z}_m$ which has multiplicative inverses in $\mathbb{Z}_m$. The set of all elements which has multiplicative inverses is denoted by $\mathbb{Z}_m^*$.

Exercise 3.2.3. Let m be a natural number. Then prove that $(\mathbb{Z}_m^*,\odot)$ is an abelian group.

3.3 Linear congruences

Let $f(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_0$ be a polynomial of degree n with integer coefficients and $a_0\not\equiv 0\ (mod\, m)$. Then $f(x)\equiv 0$ (mod m) is said to be a polynomial congruence (mod m) of degree n.

Definition 3.3.1. A polynomial congruence of degree 1 is called a linear congruence.

Thus the general form of a linear congruence modulo m is $ax\equiv b$ (mod m), where $a\not\equiv 0$ (mod m).

An integer α is said to be a solution of $ax\equiv b$ (mod m), if $a\alpha\equiv b$ (mod m). If α is a solution to $ax\equiv b$ (mod m), then $\alpha+qm$ are also solutions of $ax\equiv b$ (mod m), where $q\in\mathbb{Z}$.

Thus two solutions α and β (if exists) of $ax\equiv b$ (mod m), are said to be **distinct** if $(\alpha-\beta)$ is not divisible by m.

Example 3.3.1. The congruence equation $2x\equiv 3$ (mod 4) has no solution as $(2x-3)$ is an odd number for every integer x.

Example 3.3.2. The congruence equation $x^2\equiv 1$ (mod 8) has a solution 1. Thus another solutions are $1+8q$, but they are not “distinct” from 1. Thus residue class 1 with respect to modulo 8 is a solution of the given congruent equation, i.e., $\overline{1}$ (mod 8) is a solution.

Example 3.3.3. It can be shown that the congruence equation $x^2\equiv 1$ (mod 8) has four “distinct” solutions. They are $1,3,5,7$. More generally, solutions are $\overline{1}$ (mod 8), $\overline{3}$ (mod 8), $\overline{5}$ (mod 8), $\overline{7}$ (mod 8).

Theorem 3.3.1. Assume $a,m\in\mathbb{N}$ and $\gcd(a,m)=1$. Then the linear congruence $ax\equiv b$ (mod m) has exactly one solution modulo m.

Proof. Since $\gcd(a, m) = 1$, so there exist integers u and v such that $au + mv = 1$. Thus $a(bu) - b$ is divisible by m. Hence

$$a(bu) \equiv b \text{ (mod } m).$$

Thus bu is a solution to the linear congruence $ax \equiv b$ (mod m).

Now, we have to show that this solution is unique up to modulo m. If not, then assume that x_1 and x_2 be two solutions to the linear congruence $ax \equiv b$ (mod m). Then

$$ax_1 \equiv b \pmod{m} \text{ and } b \equiv ax_2 \pmod{m}.$$

Since congruence relation is transitive, so $ax_1 \equiv ax_2 \pmod{m}$, i.e., m divides $a(x_1 - x_2)$. But $\gcd(a, m) = 1$ (i.e., a and m has no common factor other than ± 1). Thus m divides $(x_1 - x_2)$, i.e., $x_1 \equiv x_2 \pmod{m}$. This completes the proof. □

Example 3.3.4. Find all integer x such that $5x \equiv 2$ (mod 3).

Solution:
Here $\gcd(5, 3) = 1$, so there exist integers u and v such that

$$5u + 3v = 1. \tag{3.3.1}$$

Now, by the Division Algorithm, we have

$$\begin{aligned} 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Thus

$$1 = 3 - 2 = 3 - (5 - 3) = 5 \cdot (-1) + 3 \cdot (2). \tag{3.3.2}$$

Now, subtracting (3.3.2) from (3.3.1), we obtain

$$5(u + 1) = -3(v - 2).$$

Thus $3 \mid (u+1)$, i.e., $u = -1+3t$, where $t \in \mathbb{Z}$. Hence all solutions are $u = -1+3t$, where $t \in \mathbb{Z}$.

Theorem 3.3.2. Assume $a, m \in \mathbb{N}$ and $\gcd(a, m) = d$. Then the linear congruence $ax \equiv b$ (mod m) has solutions if and only if $d \mid b$.

Proof. Assume that the linear congruence $ax \equiv b$ (mod m) has a solution, say x_0. Then $ax_0 = mq + b$ for some $q \in \mathbb{Z}$. Again, since $\gcd(a, m) = d$, so there exist integers u and v such that $a = du$ and $m = dv$. Thus

$$b = ax_0 - mq = d(ux_0 - vq),$$

which implies $d \mid b$.
Conversely, assume that $d \mid b$. Since $\gcd(a, m) = d$, so there exist integers r, s and t such that $b = rd$ and $as + mt = d$. Thus

$$\begin{aligned} b &= rd \\ &= r(as + mt). \end{aligned}$$

Thus $m \mid (a(rs) - b)$, i.e., $a(rs) \equiv b \pmod{m}$. This completes the proof. □

Theorem 3.3.3. Assume $a, m \in \mathbb{N}$, $\gcd(a, m) = d$ and $d \mid b$. Then the linear congruence $ax \equiv b \pmod{m}$ has exactly d solutions modulo m.

Moreover, the solutions are given by

$$t, t + \frac{m}{d}, t + \frac{2m}{d}, \ldots, t + (d-1)\frac{m}{d}.$$

Proof. Since $d \mid b$, so by our previous result, the linear congruence $ax \equiv b \pmod{m}$ has a solution, say t. Thus $m \mid (at - b)$.

Now, we establish that $x_i = t + i \cdot \frac{m}{d}$ is a solution to the linear congruence $ax \equiv b \pmod{m}$ where $0 \leq i \leq (d-1)$. Now,

$$\begin{aligned} ax_i - b &= a(t + i \cdot \frac{m}{d}) - b \\ &= m\left(\frac{at - b}{m} + \frac{a \cdot i}{d}\right) \\ &\equiv 0 \pmod{m}. \end{aligned}$$

Next, we show that all x_i's are distinct up to modulo m. If possible, let $x_i \equiv x_j \pmod{m}$, where $0 \leq i, j \leq (d-1)$. Then $m \mid \frac{(i-j)m}{d}$, but $\gcd(a, m) = d$. So, $m \mid (i - j)$. Again, as $d \mid m$ and $0 \leq\mid i - j \mid< d$, so $i = j$.

Lastly, we have to show that if y is a solution to the linear congruence $ax \equiv b \pmod{m}$, then $y \equiv x_r \pmod{m}$ for some r with $0 \leq r < d$. Since y is a solution to the linear congruence $ax \equiv b \pmod{m}$, so

$$ay \equiv b \pmod{m}.$$

Also, t is a solution to the linear congruence $ax \equiv b \pmod{m}$,i.e.,

$$at \equiv b \pmod{m}.$$

Thus

$$ay \equiv at \pmod{m}.$$

Hence $m \mid a(y - t)$, but as $\gcd(a, m) = d$, so $\frac{m}{d} \mid (y - t)$, i.e., $y = t + r' \cdot \frac{m}{d}$ for some integer r'. Now, by the division algorithm, $r' = q \cdot d + r$ where $0 \leq r < d$. Thus $y = t + q \cdot m + r \cdot \frac{m}{d} \equiv t + r \cdot \frac{m}{d} \pmod{m}$. This completes the proof. □

Exercise 3.3.1. If $d = \gcd\{a, m\}$, then $ax \equiv ay \pmod{m} \Leftrightarrow x \equiv y \pmod{\frac{m}{d}}$.

Exercise 3.3.2. Solve in integers:

$$20x \equiv 10 \pmod{35}.$$

Exercise 3.3.3. Solve in integers:

$$x \equiv 3 \pmod{17}.$$

Exercise 3.3.4. Solve in integers:

$$7x \equiv 3 \pmod{15}.$$

3.4 Linear Diophantine equation

An equation in one or more unknowns which is to be solved in integers is said to be a "Diophantine equation". In our present discussion, we will discuss on the Diophantine equation of the type $ax + by = c$, where a, b, c are integers.

Theorem 3.4.1. The equation $ax + by = c$, where a, b, c are integers and a, b are not both zeros, has solutions in integers if and only if $d \mid c$, where $d = \gcd\{a, b\}$.

Proof. Given $d = \gcd\{a, b\}$. Now, the equation $ax + by = c$ can be written as

$$ax \equiv c \pmod{b}.$$

. Thus by Theorem 3.3.2, the equation $ax + by = c$ has an integral solution if and only if $\gcd\{a, b\}$ divides c. This completes the proof. □

Moreover, if (x_0, y_0) is a solution of the equation $ax + by = c$, then

$$\begin{aligned} a(x - x_0) &= -b(y - y_0) \\ i.e., \quad \frac{(x - x_0)}{\frac{b}{d}} &= -\frac{(y - y_0)}{\frac{a}{d}} \\ i.e., \quad \frac{(x - x_0)}{\frac{b}{d}} &= -\frac{(y - y_0)}{\frac{a}{d}} = t, (say) \end{aligned}$$

for some integer t. That is,

$$x = x_0 + t \cdot \frac{b}{d}, \quad \text{and} \quad y = y_0 - t \cdot \frac{a}{d},$$

for all integer t.

Example 3.4.1. Find the integral solutions of the equation $13x + 4y = 115$.

Solution:

Since $\gcd\{13, 4\} = 1$, so there are integers u and v such that $13u + 4v = 1$. Now, by Division Algorithm, we obtain

$$\begin{aligned} 13 &= 3 \cdot 4 + 1 \\ so,\ 115 &= 13(115) + 4(-3 \cdot 115) \end{aligned}$$

Thus $x = 115$ and $y = -345$ is a solution to the given equation. Moreover,

$$13(x - 115) + 4(y + 345) = 0.$$

Thus $u = 115 + 4t$ and $v = -345 - 13t$ ($t \in \mathbb{Z}$) is the general solution of the given equation.

Exercise 3.4.1. Find the integral solutions of the equation $7x + 11y = 1$.

3.5 Euler's theorem and its applications

We have already introduced the Euler's totient function $\varphi : \mathbb{N} \to \mathbb{R}$. If $n \geq 1$, the the Euler's totient function $\varphi(n)$ is defined to be the number of positive integers not exceeding n and relatively prime to n.

Theorem 3.5.1 (Euler's Theorem). If $n \in \mathbb{N}$ and $\gcd\{a, n\} = 1$, then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Proof. Since $\gcd\{a, n\} = 1$, so by our previous discussion, $\overline{a} \in \mathbb{Z}_n^*$. Since $(\mathbb{Z}_n^*, \odot)$ is a group of order $\varphi(n)$, so by Lagrange's Theorem, the order of $\overline{a}$ divides $\varphi(n)$. Thus $\overline{a}^{\varphi(n)} = \overline{1}$. Hence,

$$a^{\varphi(n)} - 1 \equiv \ (\text{mod } n).$$

□

Corollary 3.5.1. If a prime number p does not divide a, then

$$a^{p^2 - p} \equiv 1 \pmod{p^2}.$$

Proof. Since $\gcd\{a, p\} = 1$, so $\gcd\{a, p^2\} = 1$. Thus by Euler's Theorem,

$$a^{p(p-1)} = a^{\varphi(p^2)} \equiv 1 \pmod{p^2}.$$

□

If n is a prime number, then the following result is an immediate consequence of Euler's Theorem.

Corollary 3.5.2 (Fermat's Theorem). If a prime number p does not divide a, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Corollary 3.5.3. If a prime number p does not divide a, then

$$a^p \equiv a \ (\text{mod} \ \ p).$$

Example 3.5.1. Find the last digit of 3^{100}.

Solution:
Let $n \in \mathbb{N}$, then n can be written as $n = a_1 + a_2 10 + a_3 10^2 + \ldots + a_k 10^{k-1}$. Thus a_1 is the last digit of n if and only if $10 \mid (n - a_1)$, i.e., if and only if $n \equiv a_1 \pmod{10}$.

Now, using Euler's Theorem, we obtain,

$$3^4 = 3^{\varphi(10)} \equiv 1 \pmod{10}$$

Thus $(3^4)^{25} \equiv 1 \ (\text{mod} \ \ 10)$. So the last digit is 1.

Example 3.5.2. Find the last two digits of 3^{100}.

Solution:
Let $n \in \mathbb{N}$, then n can be written as $n = a_1 + a_2 10 + a_3 10^2 + \ldots + a_k 10^{k-1}$. Thus $a_1 + a_2 10$ is the last two digits of n if and only if $100 \mid (n - a_1 - a_2 10)$, i.e., if and only if $n \equiv a_1 + a_2 10 \pmod{100}$.

Now, using Euler's Theorem, we obtain,

$$\begin{aligned} 3^{40} = 3^{\varphi(100)} &\equiv 1 \ (\text{mod } 100), \\ \text{i.e. } 3^{80} &\equiv 1 \ (\text{mod } 100), \\ \text{i.e. } 3^{100} &\equiv 3^{20} \ \ (\text{mod } 100). \end{aligned}$$

Again,

$$\begin{aligned} 3^{20} &= (81)^5, \\ &= (81 \times 81)^2 \times 81, \\ &= (6561)^2 \times 81, \\ &\equiv (61)^2 \times 81, \ \ (\text{mod } 100), \\ &= 3721 \times 81, \\ &\equiv 21 \times 81, \ \ (\text{mod } 100), \\ &= 1701, \\ &\equiv 01, \ \ (\text{mod } 100). \end{aligned}$$

Thus $3^{100} \equiv 01 \ (\text{mod} \ \ 100)$. So the last two digits are 01.

Example 3.5.3. If p be a prime, then show that $1^p + 2^p + \ldots + (p-1)^p$ is divisible by p.

Solution:
Using Fermat's Theorem, we obtain

$$a^p \equiv a \pmod{p}, \quad \gcd\{a, p\} = 1.$$

Thus for $1 \leq i \leq p-1$, we have $i^p \equiv i \pmod{p}$. Thus

$$\begin{aligned} \sum_{i=1}^{p-1} i^p &\equiv \sum_{i=1}^{p-1} i \pmod{p} \\ &= \frac{p(p-1)}{2} \\ &\equiv 0 \pmod{p}. \end{aligned}$$

3.6 System of linear congruences

A system of two or more linear congruences was first found in Chinese literature. For this reason, these types of problems are known as "Chinese remainder theorem".

"There are certain number of things whose number is unknown. If we count them by the multiple of three, we have two left over; by the multiple of five, we have three left over, and by the multiple of seven, we have two left over. How ,many things are there?"

If We translated this problem in terms of congruence, the problem becomes: Find the integer solution of the following system of linear equations:

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

Theorem 3.6.1 (Chinese remainder theorem). Assume $m_1, m_2, \ldots, m_r$ are positive integers and $\gcd\{m_i, m_j\} = 1$ if $i \neq j$.

Let $b_1, b_2, \ldots, b_r$ be arbitrary integers. Then the system of congruences

$$\begin{aligned} x &\equiv b_1 \ (\text{mod } m_1) \\ x &\equiv b_2 \ (\text{mod } m_2) \\ &\vdots \\ x &\equiv b_r (\text{mod } m_r) \end{aligned}$$

has exactly one solution modulo $m_1 m_2 \ldots m_r$, i.e., if x_0 be a solution, then $x = x_0 + t(m_1 m_2 \ldots m_r)$ is also solution for any integer t.

Proof. Let us construct two natural numbers as

$$M = m_1 m_2 \ldots m_r, \quad \text{and}$$

$$M_k = \frac{M}{m_k}.$$

Then for any $k \in \{1, 2, \ldots, r\}$, we have $\gcd\{M_k, m_k\} = 1$. Thus there exist integers $M_k^{'} \in \mathbb{Z}$ and $m_k^{'} \in \mathbb{Z}$ such that $M_k M_k^{'} + m_k m_k^{'} = 1$. That is, for $1 \leq k \leq r$,

$$M_k M_k^{'} \equiv 1 \pmod{m_k} \tag{3.6.1}$$

and, for $1 \leq i \leq r$ with $i \neq k$,

$$m_i \mid M_k \tag{3.6.2}$$

Now, we construct the following integer

$$x_0 = b_1 M_1 M_1^{'} + b_2 M_2 M_2^{'} + \ldots + b_r M_r M_r^{'}$$

Thus for $1 \leq i \leq r$, and using (3.6.2) and (3.6.1), we have

$$\begin{aligned} & x_0 - b_i \\ = \; & b_1 M_1 M_1^{'} + b_2 M_2 M_2^{'} + \ldots + b_{i-1} M_{i-1} M_{i-1}^{'} + b_i (M_i M_i^{'} - 1) \\ & + b_{i+1} M_{i+1} M_{i+1}^{'} + \ldots + b_r M_r M_r^{'} \\ \equiv \; & b_i (M_i M_i^{'} - 1) \pmod{m_i} \\ \equiv \; & 0 \pmod{m_i}. \end{aligned}$$

Thus x_0 satisfies every congruences in the system.

If possible, assume that y be another solution to the system of the congruences. Then $y \equiv b_i \pmod{m_i}$ for every $i \in \{1, 2, \ldots, r\}$. Thus $y \equiv x_0 \pmod{m_i}$ for every $i \in \{1, 2, \ldots, r\}$, i.e., $m_i | (y - x_0)$ for every $i \in \{1, 2, \ldots, r\}$. Since $\gcd\{m_i, m_j\} = 1$ if $i \neq j$, so

$$m_1 m_2 \ldots m_r | (y - x_0).$$

Thus $y \equiv x_0 \pmod{M}$, i.e., the solution is unique upto congruence modulo M. □

Remark 3.6.1. We have seen in (3.6.1), that

$$M_k M_k^{'} \equiv 1 \pmod{m_k}, \tag{3.6.3}$$

That is, $M_k^{'}$ is the multiplicative inverse of M_k in $\mathbb{Z}_{m_k}$

Example 3.6.1. Solve the following system of linear congruences

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

Solution: Here $M = 105$, $M_1 = 35$, $M_2 = 21$ and $M_3 = 15$.

Now, we try to find the multiplicative inverse of M_1 in $\mathbb{Z}_3$, multiplicative inverse of M_2 in $\mathbb{Z}_5$ and multiplicative inverse of M_3 in $\mathbb{Z}_7$, i.e.,

$$\begin{aligned} 35 M_1^{'} &\equiv 1 \pmod{3} \\ 21 M_2^{'} &\equiv 1 \pmod{5} \\ 15 M_3^{'} &\equiv 1 \pmod{7}. \end{aligned}$$

By Euler's Theorem, we obtain, $35^{\varphi(3)} (= 35^2) \equiv 1 \pmod{3}$. Thus

$$\begin{aligned} 35 M_1^{'} &\equiv 1 \pmod{3} \\ \text{i.e., } 35^2 M_1^{'} &\equiv 35 \pmod{3} \\ \text{i.e., } M_1^{'} &\equiv 35 \pmod{3} \\ \text{i.e., } M_1^{'} &\equiv 2 \pmod{3}. \end{aligned}$$

Again by Euler's Theorem, we obtain, $21^{\varphi(5)}(=21^4)\equiv 1 \pmod 5$. Thus

$$\begin{aligned} 21M_2^{'} &\equiv 1 \pmod{5} \\ \text{i.e., } 21^4M_2^{'} &\equiv 21^3 \pmod{5} \\ \text{i.e., } M_2^{'} &\equiv 1 \pmod{5}, \text{since } 21^3\equiv 1 \pmod{5}. \end{aligned}$$

Similarly,

$$\begin{aligned} M_3^{'} &\equiv 15^{\varphi(7)-1} \pmod{7} \\ \text{i.e., } M_3^{'} &\equiv 15^5 \pmod{7} \\ \text{i.e., } M_3^{'} &\equiv 1 \pmod{7}, \text{since } 15^5\equiv 1 \pmod{7}. \end{aligned}$$

Thus $x_0 = 2\times 35\times 2 + 3\times 21\times 1 + 2\times 15\times 1 = 233$ is a solution to the given congruences, and the general solutions are $233+105t$, $t\in\mathbb{Z}$.

Example 3.6.2. Assume $m_1, m_2, \ldots, m_r$ are positive integers and $\gcd\{m_i, m_j\} = 1$ if $i\neq j$.

Let $b_1, b_2, \ldots, b_r$ be arbitrary integers and $a_1, a_2, \ldots, a_r$ satisfy $\gcd\{a_i, m_i\} = 1$ for $i = 1, 2, \ldots, r$. Then the system of congruences

$$\begin{aligned} a_1x &\equiv b_1 \pmod{m_1} \\ a_2x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_rx &\equiv b_r (\text{mod } m_r) \end{aligned}$$

has exactly one solution modulo $m_{_1}m_{_2}\ldots m_{_r}$.

Solution: Since $\gcd\{a_i, m_i\} = 1$, so there exist integers $a_i^{'}$ and $m_i^{'}$ such that $a_ia_i^{'} + m_im_i^{'} = 1$, i.e., $a_ia_i^{'}\equiv 1 \pmod{m_i}$. Let $c_i = a_i^{'}b_i$. Then the system of congruences changed to the following system of congruences:

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_r (\text{mod } m_r) \end{aligned}$$

Rest part of the proofs are follows from the Chinese remainder theorem.

Exercise 3.6.1. Solve the following system of linear congruences

$$\begin{aligned} x &\equiv 2 \pmod{5} \\ x &\equiv 3 \pmod{7} \\ x &\equiv 5 \pmod{8} \end{aligned}$$

Exercise 3.6.2. Solve the following system of linear congruences

$$\begin{aligned} 3x &\equiv 2 \pmod{5} \\ 4x &\equiv 3 \pmod{7} \\ 3x &\equiv 5 \pmod{8} \end{aligned}$$

3.7 Public Key Encryptions

Public key cryptography(PKC) is an encryption technique that uses a paired public and private key algorithm for secure data communication. A message sender uses a recipient's public key to encrypt a message. To decrypt the sender's message, only the recipient's private key may be used.

The **RSA** (Rivest-Shamir-Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret (private). Before going to discuss the RSA method, we introduce some terminologies:

Definition 3.7.1. **Encryption** is the process of converting data to an unrecognizable or "encrypted" form. It is commonly used to protect sensitive information so that only authorized parties can view it,i.e., **Encryption** allows information to be hidden so that it cannot be read without special knowledge (such as a password).

Definition 3.7.2. A **Plaintext** is un-encrypted information, i.e., the messages before encryption, or, the raw data.

Definition 3.7.3. A **Ciphertext** refers to the output of the encryption process, i.e., encrypted data.

Definition 3.7.4. **Decryption** is the process of decoding encrypted information so that is can be accessed again by authorized users, i.e., decryption is the reverse process of encryption "plaintext".

To make the data confidential, the "plaintext" is encrypted using a particular algorithm and a public key. After encryption process, "plaintext" gets converted into "ciphertext". To decrypt the "ciphertext", similar algorithm is used and at the end the original data is obtained again.

Based on encryption and decryption, there are three types of cryptographic algorithms:

i) **Secret Key (Symmetric) Cryptography (SKC)**: This algorithm needs only one single key for both encryption and decryption.

ii) **Public Key (Asymmetric) Cryptography (PKC):** This algorithm needs one key for encryption and another one key for decryption.

iii) **Hash Functions (One way cryptography):** It is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size (known as hash value) and is designed to be a one-way function, that is, a function which is infeasible to invert. The only way to re-create the input data from an ideal cryptographic hash function's output is to attempt a brute-force search of possible inputs to see if they produce a match, or use a rainbow table of matched hashes.

    Hash function has no key since the "plaintext" is not recoverable from the "ciphertext".

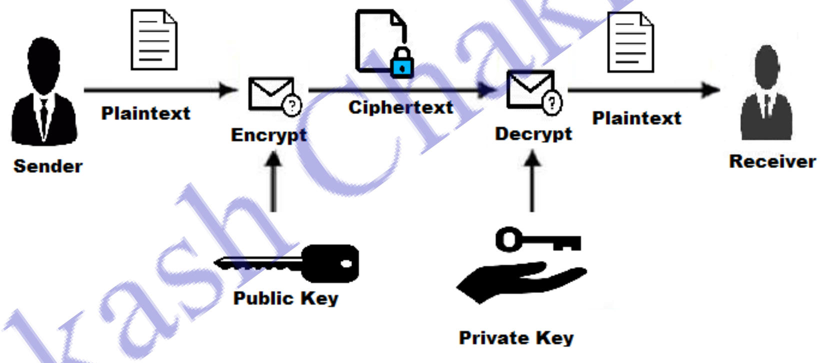
We only discuss the RSA "public key cryptography"(PKC) algorithm. The RSA algorithm is named after the famous mathematicians Ron Rivest, Adi Shamir and Leonard Adleman, who invented this algorithm in 1977. This algorithm is used in many software products, digital signatures, or encryption of small blocks of data etc.

RSA uses two different but mathematically linked keys. One key can be shared with everyone, known as **public key**, whereas the key must be kept secret, known as **private key**.

RSA Algorithm

The RSA algorithm involves four steps: **key generation**, **key distribution**, **encryption** and **decryption**. Now, we describe the method with an example.

Example 3.7.1. Suppose **client A**("Receiver") sends its "public key" to the **client B**("Sender") and requests him for some data. The client B "encrypts the data using public key" of client A and sends the encrypted data to client A, then client A receives this data and "decrypts it by his private key".



The process of encryption and decryption

Drawn by Bikash Chakraborty, using Paint

The mathematics behind the RSA algorithm

Step-I: Key generation:
The two keys for the RSA algorithm are generated by the following way:

i. First, we consider two different **large prime numbers** p and q and calculate $n = pq$.

ii. Next, we calculate Euler's totient function $\phi(n) = \phi(pq) = (p-1)(q-1)$.

iii. Then we choose an integer e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$.

iv. Finally, we find the inverse d of e in modulo $\mathbb{Z}_{\varphi(n)}$, i.e., $de \equiv 1 \pmod{\phi(n)}$.

Here, the Public Key is $\{e, n\}$ and Private Key is $\{d, n\}$.

Step-II: Encrypting message

Now, client A sends his public key $\{e, n\}$ to the client B and he must kept the private key $\{d, n\}$ to him secretely. Client B wants to send message M to client A.

i. First he turns M into a number m smaller than n.

ii. Then he computes the "ciphertext" c corresponding to "plaintext" m as follows:

$$m^e \equiv c \pmod{n},$$

and send it to client A.

Step-III: Decrypting message

Client A received the encrypted data c and he recovers the data m from c by using his private key $\{d, n\}$ as follows:

$$c^d \equiv m^{de} \pmod{n}.$$

If $m \equiv 0 \pmod{p}$, then $m^{de} \equiv 0 \equiv m \pmod{p}$. Otherwise, by Fermat's theorem, we obtain

$$m^{p-1} \equiv 1 \pmod{p}.$$

Thus $m^{\varphi(n)} \equiv 1 \pmod{p}$.

As, $de \equiv 1 \pmod{\phi(n)}$, i.e., $de = 1 + k \cdot \varphi(n).$, so $m^{de} \equiv m \pmod{p}$.

Hence, for any m,

$$m^{de} \equiv m \pmod{p}.$$

Similarly,

$$m^{de} \equiv m \pmod{q}.$$

Thus

$$\begin{aligned} c^d &\equiv m^{de} \pmod{n} \\ &\equiv m \pmod{n}, \end{aligned}$$

Now, from m, he gets the original message M.

One numerical example

Step-I: Key generation:

i. Let us consider two prime numbers $p = 11$ and $q = 17$.

ii. Now we compute $n = pq = 187$.

iii. Thus $\phi(n) = \phi(pq) = (p-1)(q-1) = 160$.

iv. Next, we choose an integer e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$, i.e., $1 < e < 160$ and $\gcd(e, 160) = 1$. Therefore, we choose $e = 7$.

v. Finally, we compute d such that $de \equiv 1 \pmod{\phi(n)}$, i.e, $7d \equiv 1 \pmod{160}$. Thus $d = 23$.

Therefore the public key is $\{7, 187\}$ and the private key is $\{23, 187\}$.

Step-II: Encrypting message

Suppose client B want to send the message "E" to client A. So, Client B turns "E" into a number $m = 5$ (accordingly alphabetical positions), and obtain the "ciphertext" c corresponding to "plaintext" m as follows:

$$\begin{aligned} c &\equiv m^e \pmod{n} \\ &= 5^7 \pmod{187} \\ &\equiv 146 \pmod{187}. \end{aligned}$$

Thus client B send $c = 146$ to client A.

Step-III: Decrypting message

Now, client A, decrypt the "ciphertext" $c = 146$ to "plaintext" as follows:

$$\begin{aligned} m &\equiv c^d \pmod{n} \\ &= 146^{23} \pmod{187} \\ &= \left[(146)^2\right]^{11} \times 146 \pmod{187} \\ &\equiv (185)^{11} \times 146 \pmod{187} \\ &= \left[(185)^2\right]^5 \times 185 \times 146 \pmod{187} \\ &\equiv 4^5 \times 82 \pmod{187} \\ &\equiv 5 \pmod{187}. \end{aligned}$$

Thus client A got the "plaintext" $m = 5$ and can get the original message "E".

Bibliography

[1] T. M. Apostol, Introduction to Analytic Number Theory, Springer.

[2] A. Baker, A Comprehensive course in Number Theory, Cambridge University Press.

[3] J. Katz and Y. Lindell, Introduction to Modern Cryptography, CRC Press, New Delhi.

[4] S. K Mapa, Higher Algebra (Classical), Sarat Book Distributors, 2007.

[5] I. Niven, H. S. Zuckerman, H. L. Montgomery, An Introduction to the Theory of Numbers, Wiley.

[6] D. Mihet, Legendre's and Kummer's theorems again, Resonance, 15 (12), 1111-1121, 2010.

[7] B. Schneier, Applied cryptography, Wiley, New Delhi, 2006.

[8] https://en.wikipedia.org/wiki/Integer.

[9] https://en.wikipedia.org/wiki/Peano_axioms.