

# Elementary Number Theory

Hamjak Debbarma

April 19, 2022

## Notations

$$\mathbb{Z} = \{\dots - 3, -2, -1, 0, 1, 2, 3\dots\}$$

$$\mathbb{Z}^+ = \{1, 2, 3\dots\}$$

$$\mathbb{Z}^- = \{\dots - 3, -2, -1\}$$

$$\mathbb{Z}^{0+} = \{0, 1, 2, 3\dots\}$$

$$\mathbb{Z}^{0-} = \{\dots - 2, -1, 0\}$$

## 1 Introduction: Divisibility, Prime, GCD

Let  $a, b \in \mathbb{Z}$  and  $a > 0$  we say  $a$  divides  $b$ ,  $a|b$  if  $b = ac$  for some  $c \in \mathbb{Z}$ . Here,  $a$  is the divisor or factor of  $b$  and  $b$  is the multiple of  $a$ .

**Note:**

- Sign has no effects:  $6|12, -5|53, 9|-81$
- Divisibility is a statement not an operator like divide  $/$
- Divisibility is mostly deals with Positive Integers.

### Properties of Divisibility

Let  $a, b, c \in \mathbb{Z}$ , then

- If  $a|b$  and  $a|c$  then  $a|b + c$
- If  $a|b$  and  $b|c$  then  $a|c$
- If  $a|b$  then  $a|mb$  for some integer  $m$
- If  $a|b$  and  $a|c$  then  $a|bm + cn$  for some integer  $m, n$

**Definition 1** (Prime). Let  $p > 0$  and  $p \in \mathbb{Z}^+$ ,  $p$  is prime iff the divisor of  $p$  is 1 and  $p$ .

**Definition 2** (Composite). Let  $M > 1$  which is not prime is composite.

**Remark 1.** 0 and 1 are neither prime nor composite.

**Theorem 1** (Fundamental Theorem of Arithmetic). Any integer greater than 1 can be written as a unique product of primes. Here, the primes ordering does not matter.

**Definition 3** (Common Divisor). The integer  $c$  is the common divisor of  $a$  and  $b$  if  $a = cn$  and  $b = cm$  for some integer  $n, m$  or if  $c|a$  and  $c|b$ .

**Definition 4** (GCD).  $\gcd(a, b)$  is the largest common divisor of  $a$  and  $b$ ,  $\gcd(a, b) > 1$  and by convention  $a, b \neq 0$ .

**Definition 5** (Co-primes). If  $\gcd(a, b) = 1$  then  $a, b$  are relatively prime or coprime though  $a, b$  needs not be prime.

**Lemma 1** (Bézout's Identity). If  $\gcd(a, b) = d$  then  $\exists x, y \in \mathbb{Z}$  s.t  $ax + by = d$

**Lemma 2.** if  $a = bq + r$  then  $\gcd(a, b) = \gcd(b, r)$

**Lemma 3.** if  $a|c$  and  $b|c$  and  $\gcd(a, b) = 1$  then  $ab|c$

**Theorem 2** (Division). Let  $a, b \in \mathbb{Z}$ ,  $b > 0$  then  $\exists q, r \in \mathbb{Z}$  s.t  $a = bq + r$  where,  $0 \leq r < b$

**Definition 6** (Linear Diophantine Eqn). Given  $a, b, c \in \mathbb{N}$  the eqn.  $ax + by = c$  has a solution for  $x, y \in \mathbb{Z}$  iff  $\gcd(a, b)|c$

Note: To solve Diophantine we can use Extended Euclid's Algorithm.

## 2 Congruences

**Definition 7.** Let  $n$  be fixed positive integer,  $a, b \in \mathbb{Z}$  are said to be congruent modulo  $n$ ,  $a \equiv b \pmod{n}$  if  $n|(a - b)$  i.e,  $a - b = nk$  for some  $k \in \mathbb{Z}$ .

**Example 1.**  $n = 7$ ,  $3 \equiv 24 \pmod{7} \implies 7|(3 - 24) \implies 7|-21$

**Example 2.**  $6 \not\equiv 1 \pmod{3} \implies 3 \nmid (6 - 1)$

Note

- Any two integers are congruent modulo 1,  $a \equiv b \pmod{1} \iff 1|(a - b)$
- Two integers are congruent modulo 2 if either both even or both odd.

**Definition 8** (Equivalence Class). For  $x \in \mathbb{Z}$  define the equivalence class of  $x$  w.r.t  $\equiv \pmod{n}$  by  $[x] = \{a \in \mathbb{Z} | a \equiv x \pmod{n}\}$

**Fact:** There are exactly  $n$  equivalence classes modulo  $n$  i.e,  $[0], [1], \dots, [n-1]$  that is, every integer is in one of those classes.

**Lemma 4.** If  $n > 1$  and  $a$  be any integers and  $r$  be remainder when  $a/n$  then  $a \equiv r \pmod{n}$  or  $\forall a \in \mathbb{Z}$   $a$  is congruent to exactly one of those least residue modulo  $n$ .

*Proof.*  $a/n \implies a = qn + r$  where,  $q, r \in \mathbb{Z}$  and  $0 \leq r < n$   
 $a - r = qn \implies a \equiv r \pmod{n}$  □

**Corollary 1.** If  $a \equiv r \pmod{n}$  then  $r = \{0, 1, 2, \dots, n-1\}$

**Definition 9** (Complete System of Residue (CSR)). Given  $a \in \mathbb{Z}$  let  $q$  and  $r$  be its quotient and remainder upon division by  $n$  i.e,  $a = qn + r, 0 \leq r < n$ . Then by definition of congruences  $a \equiv r \pmod{n}$  and  $r = \{0, 1, 2, \dots, n-1\}$  called the least non negative residue (remainder) modulo  $n$ .

In general a collection of  $\{a_1, a_2, \dots, a_n\}$  is a **Complete System of Residue** modulo  $n$  if each  $a_i \equiv r_i \pmod{n}$  i.e,  $\{a_1, a_2, \dots, a_n\} \equiv \{0, 1, 2, \dots, n-1\} \pmod{n}$  and  $a_i \not\equiv a_j \pmod{n}$

**Example 3.** Consider  $n = 4$  and  $S = \{12, 11, 8, 3\}$  does  $S$  form CSR modulo 4.

*Soln.*  $r = \{0, 1, 2, 3\}$  and  $12 \equiv 0 \pmod{4}$  and  $8 \equiv 0 \pmod{4}$  implies,  $12 \equiv 8 \pmod{4}$ . So,  $S$  does not form CSR. □

**Theorem 3.** For arbitrary integers  $a$  and  $b$ ,  $a \equiv b \pmod{n}$  iff  $a$  and  $b$  leaves the same non-negative remainder when divided by  $n$ .

*Proof.*  $a \equiv b \pmod{n} \implies a - b = nk \implies a = b + nk$  for some  $k \in \mathbb{Z}$   
 $n|b \implies b = nq + r \implies a = nq + r + nk \implies a = (nq + nk) + r$   
Now, assume  $a = nq_1 + r$  and  $b = nq_2 + r$  then  $a - b = nq_1 + r - nq_2 - r \implies a - b = n(q_1 - q_2) \implies a \equiv b \pmod{n}$   $\square$

**Theorem 4.** Let  $n > 1$  and  $a, b, c, d \in \mathbb{Z}$  then the following properties hold :

1.  $a \equiv a \pmod{n}$
2. if  $a \equiv b \pmod{n}$  then  $b \equiv a \pmod{n}$
3. if  $a \equiv b \pmod{n}$  and  $b \equiv c \pmod{n}$  then  $a \equiv c \pmod{n}$
4. if  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n}$  then  $a + c \equiv b + d \pmod{n}$  and  $ac \equiv bd \pmod{n}$
5. if  $a \equiv b \pmod{n}$  then  $a + c \equiv b + c \pmod{n}$  and  $ac \equiv bc \pmod{n}$
6. if  $a \equiv b \pmod{n}$  then  $a^k \equiv b^k \pmod{n}$  for any  $k \in \mathbb{Z}^+$

*Proof.* (Prop5) Using prop1 and prop4  $a \equiv b \pmod{n}$  and  $c \equiv c \pmod{n}$  implies,  $a + c \equiv b + c \pmod{n}$  and  $ac \equiv bc \pmod{n}$   
(prop6) Using prop4 we can established the prove.  $\square$

### Divisibility Test for an Integer

- An integer is divisible by 2 iff it's unit digits is 0, 2, 4, 6, 8
- For 3 its digits sum should be divisible by 3
- For 4, the no. form by its last digits should be divisible by 4
- For 5, last digit should be 0 or 5.
- An integer  $N$  is divisible by 6 iff  $6|M$ , where  $M = a_0 + 4a_1 + \dots + 4a_m$
- For 8, the no. formed by last three digits should be divisible by 8.
- For 9 its digits sum should be divisible by 9
- For 10, the last digit should be 0
- For 11,  $11|N$  iff the altering sum of its digit is divisible by 11. E.g,  $N = 639162513 \implies 3 - 1 + 5 - 2 + 6 - 1 + 9 - 3 + 6 = 22$

## 3 Linear Congruences

**Definition 10.** An eqn, of the form  $ax \equiv b \pmod{n}$  is called the Linear congruences.

**Lemma 5.**  $ax \equiv b \pmod{n}$  has a solution iff  $d|b$ , where  $d = \gcd(a, n)$ . If  $d|b$  then it has  $d$  mutually incongruent solution modulo  $n$ .

**Note:**

1. if  $x_1$  is a soln of  $ax \equiv b \pmod{n}$  then any other  $x_2 \equiv x_1 \pmod{n}$  is congruent solution.
2. if  $x_1$  and  $x_2$  are both soln and  $x_1 \not\equiv x_2 \pmod{n}$  then it is called incongruent soln of  $ax \equiv b \pmod{n}$ .

**Definition 11** (Inverse of Modulo  $n$ ). Any value of  $x$  which is a solution of  $ax \equiv 1 \pmod{n}$  is called the inverse of modulo  $n$ . Thus if  $a^{-1}$  is the inverse then  $aa^{-1} \equiv 1 \pmod{n}$

**Strategy for solving:**  $ax \equiv b \pmod{n}$

1.  $a$  is invertible modulo  $n$  iff  $\gcd(a, n) = 1$ ,  $ax + ny = 1$  so,  $ax \equiv 1 \pmod{n}$
2. Reduction: if  $ca \equiv cb \pmod{n} \implies a \equiv b \pmod{\frac{n}{\gcd(c, n)}}$
3.  $ax \equiv b \pmod{n}$  has a soln iff  $\gcd(a, n) | b$
4. if  $ax \equiv b \pmod{n}$  has a soln then there are  $\frac{n}{\gcd(a, n)}$  number of soln separated by  $\frac{n}{\gcd(a, n)}$

## 4 Fermat's Little Theorem

**Theorem 5.** Let  $p$  be prime and  $\gcd(a, p) = 1$  then  $a^{p-1} \equiv 1 \pmod{p}$

**Corollary 2.** If  $p$  is prime then  $a^p \equiv a \pmod{p}$

*Proof.* From  $a^{p-1} \equiv 1 \pmod{p}$  we multiply by  $a$ . □

## 5 Wilson's Theorem

**Theorem 6.** If  $p$  is a prime then  $(p-1)! \equiv -1 \pmod{p}$

*Proof.* Consider,

$$\begin{aligned}
 (p-1)! &\equiv 1(2.3 \dots (p-2))p-1 \pmod{p} \\
 &\equiv 1(2.2^{-1} \dots (p-2)(p-2)^{-2})p-1 \pmod{p} \\
 &\equiv 1.1 \dots (p-1) \pmod{p} \\
 &\equiv p-1 \pmod{p} \qquad (p \equiv 0 \pmod{p}) \\
 &\equiv -1 \pmod{p}
 \end{aligned}$$

□

**Lemma 6.** If  $a^2 \equiv 1 \pmod{p}$  then  $a \equiv 1 \pmod{p}$  or  $a \equiv -1 \pmod{p}$

*Proof.* Suppose,  $a^2 \equiv 1 \pmod{p} \implies p | a^2 - 1 \implies p | (a+1)(a-1) \implies a \equiv 1 \pmod{p}$  or  $a \equiv -1 \pmod{p}$   
 (So, the only integer who are their own inverse  $\pmod{p}$  is  $\pm 1 \pmod{p}$ ) □

## 6 Chinese Remainder Theorem

## 7 Hensel's Lemma

## 8 Polynomial Congruences

## 9 Lagrange's Polynomial

## 10 Euler's Totient