Lecture 01

Theory of Congruences

↓

first introduced by German Mathematician 'Carl Friedrich Gauss' (1777-1855).

A famous Quote by Gauss

> Mathematics is the queen of sciences
> & Number theory is the queen of Mathematics

Gauss solved a problem to find sum of 1 to 100 in very easy way when he was only 3 years old.

like $1+2+3+\cdots+50+51+\cdots+98+99+100$

$1+100 = 101$
$2+99 = 101$
$3+98 = 101$
$\vdots$
$50+51 = 101$

such pairs $= 50$

$\therefore 1+2+3+\cdots+100 = 50\times 101 = \underline{5050}$

In this way, there is another technique to find the sum of first n natural numbers

$1+2+3+\cdots+(n-1)+n$
$n+(n-1)+(n-2)+\cdots+2+1$

adding horizonally (sum) = adding vertically (sum)

$2(1+2+3+\cdots+n) = (n+1)+(n+1)+\cdots+(n+1)$

$2(1+2+\cdots+n) = n(n+1)$

$\therefore \boxed{1+2+\cdots+n = \frac{n(n+1)}{2}}$

Basic Properties of Congruence

Gauss introduced the concept of congruence and symbol $\equiv$ because of close analogy with algebraic equality.

Definition Let n be a fixed positive integer.

Two integers a and b are said to be congruent modulo n say

$a \equiv b \bmod n$ iff n divides the difference $a-b$.

i.e $a \equiv b \bmod n$ iff $a-b = kn$ for some integer k

note: a is congruent to b modulo $n \Leftrightarrow a \equiv b \bmod n$

a is incongruent to b modulo $n \Leftrightarrow a \not\equiv b \bmod n$

To fix the idea, let us consider the following example

Q. Let $n=7$, check whether the following a and b are congruent modulo n.

(a) $a = 3$, $b = 24$

(b) $a = -31$, $b = 11$

(c) $a = 25$, $b = 12$

Soln: (a) $a-b = 3-24 = -21$, $7 \mid -21$ as $-21 = -3 \times 7$, $-3 \in \mathbb{Z}$

$\therefore a-b = kn \Rightarrow a \equiv b \bmod n$

(b) $a-b = -31-11 = -42 = -6 \times 7 = kn$, $k = -6 \in \mathbb{Z}$

$\therefore a \equiv b \bmod n$.

(c) $a-b = 25-12 = 13 \neq k7$ for any $k \in \mathbb{Z}$

$\therefore a-b \not\equiv 0 \bmod n$ or $a \not\equiv b \bmod n$

mark2. any two integers a and b are congruence modulo 2 if either both are even or both are odd integers.

usual practice is to assume that $n > 1$

Given an integer a, let q and r be its quotient and remainder upon division by n so that

$$a = qn + r \qquad 0 \le r < n$$

congruence def^n gives, $a \equiv r \pmod n$

$\downarrow$

a is congruent to r mod n

r has total n choices say $r = 0, 1, 2, \dots, n-1$

Every integer a is congruent to exactly one integer r under modulo n where $0 \le r < 1$.

In particular $a \equiv 0 \bmod n$ iff n/a

$S = \{0, 1, 2, \dots, n-1\}$ → set of least non negative residues modulo n.

Complete set/system of Residues modulo n :-

A collection of n integers $a_1, a_2, \dots, a_n$ is said form a complete set of residues modulo n if every integer is congruent modulo n to one and only one of a_k.