Chapter 8

Definition: Let a, b, m be integers. We say that <u>a is congruent to b modulo m</u> if:

$$m \mid (a-b)$$

Write: $a \equiv b \pmod{m}$

The number m is called the modulous of the congruence.

Example: $5 \mid (7-2) \Rightarrow 7 \equiv 2 \pmod{5}$

$6 \mid (47-35) \Rightarrow 47 \equiv 35 \pmod{6}$

Observation: Let a, m be two integers, by Euclidean algorithm, we can find q, r such that

$$a = qm + r \quad \text{with} \quad 0 \leq r < m.$$

This implies: $m \mid (a-r)$

In other words: $a \equiv r \pmod{m}$.

This means: every integer is congruent, modulo m, to a number between 0 and $m-1$.

Congruences with same modulus behave in many ways like numbers :

Proposition: Suppose that

$$a \equiv b \pmod{m}$$
$$b \equiv c \pmod{m}$$

Then: (1) $a \equiv a \pmod{m}$ (reflexive)

(2) $b \equiv a \pmod{m}$ (symmetric)

(3) $a \equiv c \pmod{m}$ (transitive)

Proof: (1) $m \mid 0 = (a-a) \Rightarrow a \equiv a \pmod{m}$

(2) $a \equiv b \pmod{m} \Rightarrow m \mid (a-b)$

$\Rightarrow a-b = rm \Rightarrow b-a = -rm$

$\Rightarrow m \mid (b-a) \Rightarrow b \equiv a \pmod{m}$

(3) $a \equiv b \pmod{m}$ $\quad a-b = rm$

$b \equiv c \pmod{m}$ $\quad b-c = sm$

$$a-c = a+(-b+b)-c = (a-b)+(b-c)$$

$$= rm + sm = (r+s)m$$

$$m \mid (a-c) \implies a \equiv c \pmod{m}$$ □

<u>Proposition:</u> Suppose that

$$a_1 \equiv b_1 \pmod{m}$$
$$a_2 \equiv b_2 \pmod{m}$$

Then: (1) $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$

(2) $a_1 - a_2 \equiv b_1 - b_2 \pmod{m}$

(3) $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

Proof: $a_1 \equiv b_1 \pmod{m}$ $\quad a_1 - b_1 = r_1 m$

$a_2 \equiv b_2 \pmod{m}$ $\quad a_2 - b_2 = r_2 m$

(1) $$(a_1 + a_2) - (b_1 + b_2) = a_1 + a_2 - b_1 - b_2$$
$$= (a_1 - b_1) + (a_2 - b_2)$$
$$= r_1 m + r_2 m = (r_1 + r_2) m$$

$$\implies m \mid (a_1 + a_2) - (b_1 + b_2)$$

$$\implies a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$$

(2) Similar

(3) $a_1b_1 - a_2b_2 = a_1b_1 + (-a_1b_2 + a_1b_2) - a_2b_2$

$$= a_1b_1 - a_1b_2 + a_1b_2 - a_2b_2$$

$$= a_1(b_1 - b_2) + (a_1 - a_2)b_2$$

$$= a_1 r_2 m + r_1 m b_2$$

$$= (a_1 r_2 + a_2 r_1) m$$

$$\Rightarrow m \mid (a_1a_2 - b_1b_2) \Rightarrow a_1a_2 \equiv b_1b_2 \pmod{m} \quad \square$$

However: $ac \equiv bc \pmod{m} \not\Rightarrow a \equiv b \pmod{m}$

(counter)example: $15 \cdot 2 = 30 \qquad 20 \cdot 2 = 40.$

$$15 \cdot 2 \equiv 20 \cdot 2 \pmod{10}$$

but $15 \not\equiv 20 \pmod{10}$

Congruent Equations:

A congruent equation (with one unknown) is of the form:

$$P(x) \equiv 0 \pmod{m}.$$

$P(x)$ is a polynomial.

A <u>linear</u> congruent equation (with one unknown)

$$ax + b \equiv 0 \pmod{m}.$$

We will study how to solve linear congruent equation.

Example: $x + 12 \equiv 5 \pmod{8}$

Solution: $x + 12 - 12 \equiv 5 - 12 \pmod{8}$

$$x \equiv -7 \pmod{8}$$

(This is okay for the solution, but we prefer a number between 0 and $8-1=7$)

Moreover, $8 \mid 8 = 1 - (-7) \Rightarrow -7 \equiv 1 \pmod{8}$

Therefore: $x \equiv 1 \pmod{8}$. $\square$