CONGRUENCE RELATION

Let m be a positive integer. We say that a is *congruent* to b *modulo* m. written

$$a \equiv b \text{ (modulo } m) \qquad \text{or simply} \qquad a \equiv b \pmod{m}$$

if m divides the difference $a - b$. The integer m is called the *modulus*. The negation of $a \equiv b \pmod{m}$ is written $a \not\equiv b \pmod{m}$. For example:

(i) $87 \equiv 23 \pmod 4$ since 4 divides $87 - 23 = 64$.

(ii) $67 \equiv 1 \pmod 6$ since 6 divides $67 - 1 = 66$.

(iii) $72 \equiv -5 \pmod 7$ since 7 divides $72 - (-5) = 77$.

(iv) $27 \not\equiv 8 \pmod 9$ since 9 does not divide $27 - 8 = 19$.

Theorem : Let m be a positive integer. Then:

(i) For any integer a, we have $a \equiv a \pmod{m}$.

(ii) If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

(iii) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Remark: Suppose m is positive, and a is any integer. By the Division Algorithm, there exist integers q and r with $0 = r \leq m$ such that $a = mq + r$. Hence

$$mq = a - r \quad \text{or} \quad m \mid (a - r) \quad \text{or} \quad a \equiv r \pmod{m}$$

Accordingly:

(1) Any integer a is congruent modulo m to a unique integer in the set

$$\{0,\ 1,\ 2, \ldots, m - 1\}$$

The uniqueness comes from the fact that m cannot divide the difference of two such integers.

(2) Any two integers a and b are congruent modulo m if and only if they have the same remainder when divided by m.

Residue Classes

Since congruence modulo m is an equivalence relation, it partitions the set $\mathbf{Z}$ of integers into disjoint equivalence classes called the *residue classes modulo m*. By the above remarks, a residue class consists of all those integers with the same remainder when divided by m. Therefore, there are m such residue classes and each residue class contains exactly one of the integers in the set of possible remainders, that is,

$$\{0,\ 1,\ 2,\ \ldots, m-1\}$$

Generally speaking, a set of m integers $\{a_1,\ a_2,\ \ldots, a_m\}$ is said to be a *complete residue system modulo m* if each a_i comes from a distinct residue class. (In such a case, each a_i is called a *representative* of its equivalence class.)

Thus the integers from 0 to $m-1$ form a complete residue system. In fact, any m consecutive integers form a complete residue system modulo m.

The notation $[x]_m$, or simply $[x]$ is used to denote the residue class (modulo m) containing an integer x, that is, those integers which are congruent to x. In other words,

$$[x] = \{a \in \mathbf{Z} \mid a \equiv x \pmod{m}\}$$

Accordingly, the residue classes can be denoted by

$$[0],\ [1],\ [2], \ldots, [m-1]$$

or by using any other choice of integers in a complete residue system.

EXAMPLE The residue classes modulo $m = 6$ follow:

$$[0] = \{\ldots, -18, -12, -6, 0, 6, 12, 18, \ldots\}, \quad |3| = \{\ldots, -15, -9, -3, 3, 9, 15, 21, \ldots\}$$
$$[1] = \{\ldots, -17, -11, -5, 1, 7, 13, 19, \ldots\}, \quad |4| = \{\ldots, -14, -8, -2, 4, 10, 16, 22, \ldots\}$$
$$[2] = \{\ldots, -16, -10, -4, 2, 8, 14, 20, \ldots\}, \quad |5| = \{\ldots, -13, -7, -1, 5, 11, 17, 23, \ldots\}$$

Note that $\{-2, -1, 0, 1, 2, 3\}$ is also a complete residue system modulo $m = 6$, and these representatives have minimal absolute values.

Congruence Arithmetic

The next theorem tells us that, under addition and multiplication, the congruence relation behaves very much like the relation of equality. Namely:

Theorem : Suppose $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$. Then:
(i) $a + b \equiv c + d \pmod{m}$; (ii) $a \cdot b \equiv c \cdot d \pmod{m}$

Remark: Suppose $p(x)$ is a polynomial with integral coefficients. If $s \equiv t \pmod{m}$, then using Theorem repeatedly we can show that $p(s) \equiv p(t) \pmod{m}$.

EXAMPLE Observe that $2 \equiv 8 \pmod{6}$ and $5 \equiv 41 \pmod{6}$. Then:

(a) $2 + 5 \equiv 8 + 41 \pmod{6}$ or $7 \equiv 49 \pmod{6}$

(b) $2 \cdot 5 \equiv 8 \cdot 41 \pmod{6}$ or $10 \equiv 328 \pmod{6}$

(c) Suppose $p(x) = 3x^2 - 7x + 5$. Then

$$p(2) = 12 - 14 + 5 = 3 \quad \text{and} \quad p(8) = 192 - 56 + 5 = 141$$

Hence $3 \equiv 141 \pmod{6}$.

Arithmetic of Residue Classes

Addition and multiplication are defined for our residue classes modulo m as follows:

$$[a] + [b] = [a + b] \quad \text{and} \quad [a] \cdot [b] = [ab]$$

For example, consider the residue classes modulo $m = 6$; that is,

$$[0], [1], [2], [3], [4], [5]$$

Then

$$[2] + [3] = [5], \quad [4] + [5] = [9] = [3], \quad [2]\cdot[2] = [4], \quad [2]\cdot[5] = [10] = [4]$$

The content of Theorem 11.22 tells us that the above definitions are well defined, that is, the sum and product of the residue classes do not depend on the choice of representative of the residue class.

There are only a finite number m of residue classes modulo m. Thus one can easily write down explicitly their addition and multiplication tables when m is small. Figure 11-4 shows the addition and multiplication tables for the residue classes modulo $m = 6$. For notational convenience, we have omitted brackets and simply denoted the residue classes by the numbers 0, 1, 2, 3, 4, 5.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1