LECTURE 11

Congruence and Congruence Classes

DEFINITION 11.1. *An **equivalence relation** $\tilde{}$ on a set S is a rule or test applicable to pairs of elements of S such that*

$$\begin{array}{ll} (i) & a \sim a \quad , \quad \forall\, a \in S \quad \textit{(reflexive property)} \\ (ii) & a \sim b \quad \Rightarrow \quad b \sim a \quad \textit{(symmetric property)} \\ (iii) & a \sim b \textit{ and } b \sim c \quad \Rightarrow \quad a \sim c \quad \textit{(transitive property)} \quad . \end{array}$$

You should think of an equivalence relation as a generalization of the notion of equality. Indeed, the usual notion of equality among the set of integers is an example of an equivalence relation. The next definition yields another example of an equivalence relation.

DEFINITION 11.2. *Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Then a is **congruent to** b **modulo** n;*

$$a \equiv b \pmod{n}$$

provided that n divides $a - b$.

Example.

$$17 \equiv 5 \pmod{6}$$

The following theorem tells us that the notion of congruence defined above is an equivalence relation on the set of integers.

THEOREM 11.3. *Let n be a positive integer. For all $a, b, c \in \mathbb{Z}$*

$$\begin{array}{ll} (i) & a \equiv a \,(mod\ n) \\ (ii) & a \equiv b \,(mod\ n) \quad \Rightarrow \quad b \equiv a \,(mod\ n) \\ (iii) & a \equiv b \,(mod\ n) \textit{ and } b \equiv c \,(mod\ n) \quad \Rightarrow \quad a \equiv c \,(mod\ n) \quad . \end{array}$$

Proof.

(i) $a - a = 0$ and $n \mid 0$, hence $a \equiv a \pmod{n}$.

(ii) $a \equiv b \pmod{n}$ means that $a - b = nk$ for some $k \in \mathbb{Z}$. Therefore, $b - a = -nk = n(-k)$; hence $b \equiv a \pmod{n}$.

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

$$\begin{array}{rcl} a - b & = & nk \\ b - c & = & nk' \quad . \end{array}$$

Adding these two equations yields

$$a - c = n(k + k') \quad ;$$

and so $a \equiv c \pmod{n}$. □

THEOREM 11.4. *If $a \equiv b \ (mod\ n)$ and $c \equiv d \ (mod\ n)$, then*

$$\begin{array}{ll} (i) & a + c \equiv b + d \ (mod\ n) \\ (ii) & ac \equiv bd \ (mod\ n) \quad . \end{array}$$

Proof.

(i) By the definition of congruence there are integers s and t such that $a - b = sn$ and $c - d = tn$. Therefore,

$$a - b + c - d = sn + tn = n(s + t)$$

or, adding $b + d$ to both sides of this equation,

$$a + c = b + d + n(s + t) \quad .$$

Hence, $a + c \equiv b + d \pmod{n}$.

(ii) Using the fact that $-bc + bc = 0$ we have

$$\begin{aligned} ac - bd &= ac + 0 - bd \\ &= ac + (-bc + bc) - bd \\ &= c(a - b) + b(c - d) \\ &= c(sn) + b(tn) \\ &= n(cs + bt) \end{aligned}$$

and so $n \mid (ac - bd)$. Hence, $ac \equiv bd \pmod{n}$.

□

DEFINITION 11.5. *Let a and n be integers with $n > 0$. The* ***congruence class of a modulo n****, denoted $[a]_n$, is the set of all integers that are congruent to a modulo n; i.e.,*

$$[a]_n = \{z \in \mathbb{Z} \mid a - z = kn \text{ for some } k \in \mathbb{Z}\} \quad .$$

Example:

In congruence modulo 2 we have

$$\begin{aligned} [0]_2 &= \{0, \pm 2, \pm 4, \pm 6, \cdots\} \\ [1]_2 &= \{\pm 1, \pm 3, \pm 5, \pm 7, \cdots\} \quad . \end{aligned}$$

Thus, the congruence classes of 0 and 1 are, respectively, the sets of even and odd integers.

In congruence modulo 5 we have

$$\begin{aligned} [3]_5 &= \{3, 3 \pm 5, 3 \pm 10, 3 \pm 15, \cdots\} \\ &= \{\cdots, -12, -7, -2, 3, 8, 13, 18, \cdots\} \quad . \end{aligned}$$

THEOREM 11.6. *$a \equiv c \ (mod\ n)$ if and only if $[a]_n = [c]_n$.*

Proof.

Assume $a \equiv c \pmod{n}$. Let $b \in [a]_n$. Then by definition $b \equiv a \pmod{n}$. By the transitivity property of congruence we then have

$$a \equiv b \pmod{n} \text{ and } a \equiv c \pmod{n} \Rightarrow \quad b \equiv c \pmod{n} \quad .$$

So $b \in [c]_n$. Thus, any element b of $[a]_n$ is also an element of $[c]_n$. Reversing the roles of a and c in the argument above we similarly conclude that any element of $[c]_n$ is also an element of $[a]_n$. Therefore

$$[a]_n = [c]_n \quad .$$

Conversely, suppose $[a] = [c]$. Since $a \equiv a \pmod{n}$, by the reflexive property of congruence, we have $a \in [a]$ and so, since by hypothesis $[a] = [c]$, $a \in [c]$. Hence,

$$a \equiv c \pmod{n} \quad .$$

□

Recall that if A and C are arbitrary sets, there are in general three possibilities:

$$\begin{array}{ll} (i) & A \cap C \neq \emptyset \quad \text{and } A = C \\ (ii) & A \cap C \neq \emptyset \quad \text{and } A \neq C \\ (iii) & A \cap C = \emptyset \quad . \end{array}$$

In the last case we say that the sets A and C are **disjoint**. The following corollary says that for congruence clases the immediary case (ii) does not exist.

COROLLARY 11.7. *Two congruence classes modulo n are either disjoint or identical.*

Proof.

If $[a]_n$ and $[b]_n$ are disjoint there is nothing to prove. Suppose then that $[a]_n \cap [b]_n \neq \emptyset$. Then there is an integer b such that $b \in [a]_n$ and $b \in [c]_n$. So $b \equiv a \pmod{n}$ and $b \equiv c \bmod n$). By the symmetry and transitivity properties of congruence we then have

$$a \equiv c \pmod{n} \quad .$$

Hence $[a]_n = [c]_n$ by Theorem 2.3. □

COROLLARY 11.8. *There are exactly n distinct congruence classes modulo n; namely,* $[0]_n$, $[1]_n$, $[2]_n$, …, $[n-1]_n$.

Proof.

We first show that no two of $0, 1, 2, \ldots, n-1$ are congruent modulo n. To see this, suppose that

$$0 \leq s < t < n \quad .$$

Then $t - s$ is a positive integer and $t - s < n$. Thus, n does not divide $t - s$ and so t is not congruent to s modulo n. Since no two of $0, 1, 2, \ldots, n-1$ are congruent, the classes $[0]_n, [1]_n, \ldots, [n-1]_n$ are all distinct, by Theorem 2.3.

To complete the proof we need to show that every congruence class is one of these classes. Let $a \in \mathbb{Z}$. By the Division Algorithm,

$$a = nq + r \tag{11.1}$$

or with $0 \leq r < n$. The condition on r implies $r \in \{0, 1, 2, \ldots, n-1\}$. If we rewrite (11.1) as

$$a - r = nq$$

it is clear that $a \equiv r \pmod{n}$. Thus, any integer a is congruent modulo n to some $r \in \{0, 1, 2, \ldots, n-1\}$. □

DEFINITION 11.9. *The set of all congruence classes modulo n is denoted* $\mathbb{Z}_n$ *(which is read "*$\mathbb{Z}$ *mod n").*

Thus,

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\} \quad .$$

Note that while the set

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

has an infinite number of elements, the set $\mathbb{Z}_n$ has only n elements. Note also that the individual elements of $\mathbb{Z}_n$ are not integers, but rather infinte sets of integers; e.g.,

$$[2] = \{\ldots, 2-3n, 2-2n, 2-n, 2, 2+n, 2+2n, 2+3n, \ldots.\} \quad .$$

We proved last time that congruence modulo n is an equivalence relation; i.e.,

$$\begin{array}{ll} (i) & a \equiv a \pmod{n} \\ (ii) & a \equiv b \pmod{n} \quad \Rightarrow \quad b \equiv a \pmod{n} \\ (iii) & a \equiv b \pmod{n} \text{ and } b \equiv c \pmod{n} \quad \Rightarrow \quad a \equiv c \pmod{n} \quad , \end{array}$$

and that congruence modulo n also is compatible with the addition and multiplication of integers

THEOREM 11.10. *If $a \equiv b$ (mod n) and $c \equiv d$ (mod n), then*

$$\begin{array}{ll} (i) & a + c \equiv b + d \pmod{n} \\ (ii) & ac \equiv bd \pmod{n} \quad . \end{array}$$

DEFINITION 11.11. *Let a and n be integers with $n > 0$. The **congruence class of** a **modulo** n, denoted $[a]$, is the set of all integers that are congruent to a modulo n; i.e.,*

$$[a] = \{z \in \mathbb{Z} \mid a - z = kn \text{ for some } k \in \mathbb{Z}\} \quad .$$

Example:

In congruence modulo 2 we have

$$\begin{array}{rcl} [0]_2 & = & \{0, \pm 2, \pm 4, \pm 6, \cdots\} \\ [1]_1 & = & \{\pm 1, \pm 3, \pm 5, \pm 7, \cdots\} \quad . \end{array}$$

Thus, the congruence classes of 0 and 1 are, respectively, the sets of even and odd integers.

In congruence modulo 5 we have

$$\begin{array}{rcl} [3] & = & \{3, 3 \pm 5, 3 \pm 10, 3 \pm 15, \cdots\} \\ & = & \{\cdots, -12, -7, -2, 3, 8, 13, 18, \cdots\} \quad . \end{array}$$

THEOREM 11.12. *$a \equiv c$ (mod n) if and only if $[a]_n = [c]_n$.*

Proof.

Assume $a \equiv c \pmod{n}$. Let $b \in [a]$. Then by definition $b \equiv a \pmod{n}$. By the transitivity property of congruence we then have

$$a \equiv b \pmod{n} \text{ and } a \equiv c \pmod{n} \Rightarrow \quad b \equiv c \pmod{n} \quad .$$

So $b \in [c]_n$. Thus, any element b of $[a]_n$ is also an element of $[c]$. Reversing the roles of a and c in the argument above we similarly conclude that any element of $[c]_n$ is also an element of $[a]_n$. Therefore

$$[a] = [c] \quad .$$

Conversely, suppose $[a] = [c]$. Since $a \equiv a \pmod{n}$, by the reflexive property of congruence, we have $a \in [a]$ and so, since by hypothesis $[a] = [c]$, $a \in [c]$. Hence,

$$a \equiv c \pmod{n} \quad .$$

□

Recall that if A and C are arbitrary sets, there are in general three possibilities:

$$\begin{array}{ll} (i) & A \cap C \neq \emptyset \quad \text{and } A = C \\ (ii) & A \cap C \neq \emptyset \quad \text{and } A \neq C \\ (iii) & A \cap C = \emptyset \quad . \end{array}$$

In the last case we say that the sets A and C are **disjoint**. The following corollary says that for congruence clases the immediary case (ii) does not exist.

COROLLARY 11.13. *Two congruence classes modulo n are either disjoint or identical.*

Proof.

If $[a]_n$ and $[b]_n$ are disjoint there is nothing to prove. Suppose then that $[a]_n \cap [b]_n \neq \emptyset$. Then there is an integer b such that $b \in [a]_n$ and $b \in [c]_n$. So $b \equiv a \pmod{n}$ and $b \equiv c \bmod n$). By the symmetry and transitivity properties of congruence we then have

$$a \equiv \text{c } (\text{mod } n) \quad .$$

Hence $[a]_n = [c]_n$ by Theorem 2.3. □

COROLLARY 11.14. *There are exactly n distinct congruence classes modulo n; namely, [0], [1], [2], . . . ,[n-1]*
.

Proof.

We first show that no two of $0, 1, 2, \ldots, n-1$ are congruent modulo n. To see this, suppose that

$$0 \leq s < t < n \quad .$$

Then $t - s$ is a positive integer and $t - s < n$. Thus, n does not divide $t - s$ and so t is not congruent to s modulo n. Since no two of $0, 1, 2, \ldots, n-1$ are congruent, the classes $[0]_n, [1]_n, \ldots, [n-1]_n$ are all distinct, by Theorem 2.3.

To complete the proof we need to show that every congruence class is one of these classes. Let $a \in \mathbb{Z}$. By the Division Algorithm,

$$a = nq + r \tag{11.2}$$

or with $0 \leq r < n$. The condition on r implies $r \in \{0, 1, 2, \ldots, n-1\}$. If we rewrite (11.2) as

$$a - r = nq$$

it is clear that $a \equiv r \pmod{n}$. Thus, any integer a is congruent modulo n to some $r \in \{0, 1, 2, \ldots, n-1\}$. □

DEFINITION 11.15. *The set of all congruence classes modulo n is denoted $\mathbb{Z}_n$ (which is read "$\mathbb{Z}$ mod n").*

Thus,

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\} \quad .$$

Note that while the set

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

has an infinite number of elements, the set $\mathbb{Z}_n$ has only n elements. Note also that the individual elements of $\mathbb{Z}_n$ are not integers, but rather infinte sets of integers; e.g.,

$$[2]_n = \{\ldots, 2-3n, 2-2n, 2-n, 2, 2+n, 2+2n, 2+3n, \ldots.\} \quad .$$