Math 214 Foundations of Higher Mathematics C.K. Li

§9.5/9.6 Congruence Modulo n

We study properties of the partition $\mathbf{Z}_n = \{[0], [1], \ldots, [n-1]\}$ of the set $\mathbf{Z}$.

Congruence Modulo n

Recall that for $n \in \mathbf{N}$ with $n > 1$, we have $\mathbf{Z}_n = \{[0], [1], \ldots, [n-1]\}$ with

$$[k] = \{nx + k : x \in \mathbf{Z}\}.$$

Two integers x, y lies in the same class if $x - y$ is divisible by n, and we write $x \equiv y \pmod{n}$.

Theorem Define a relation R on integers by xRy if $x \equiv y \pmod{n}$. Then

(a) For ANY $x \in \mathbf{Z}$, xRx. (Reflexive)

(b) If $x, y \in \mathbf{Z}$ satisfy xRy then yRx. (Symmetric)

(c) If $x, y, z \in \mathbf{Z}$ satisfy xRy, yRz, then xRz. (Transitive).

We say that R is an equivalence relation on $\mathbf{Z}$. Note that $[x_1] = [x_2]$ if $x_1 R x_2$.

Theorem Let $n > 1$ be an integer. For any $x, y \in \mathbf{Z}$, the following operations are well defined:

$$[x] + [y] = [x + y] \quad \text{and} \quad [x][y] = [xy].$$

Applications

(1) Find the last digit of 11^{2016}.

(2.a) Show that $10^{2n} - 1$ is divisible by 11 for any $n \in \mathbf{N}$.

(2.b) Show that $10^{2n+1} + 1$ is divisible by 11 for any $n \in \mathbf{N}$.

(2.c) Show that a number is divisible by 11 if the sum of its digits in even positions is the same as the sum of its digits in odd positions.

More about relations

Definition A relation R on a set S is an **equivalence relation** if it is

(R) reflexive: aRa for every $a \in S$.

(S) symmetric: If aRb, then bRa.

(T) transitive: If aRb and bRc, then aRc.

Examples

(1) Consider all relations on $\{1, 2\}$.

(2) Consider the relation on $\mathbf{Z}$ such that xRy if $x^2 = y^2$. Show that R is an equivalence relation on $\mathbf{Z}$.

(3) Consider the relation on $\mathbf{Z}$ such that xRy if $x > y$. Is R reflexive / symmetric / transitive?

Theorem Let R be an equivalence relation on a non-empty set S, and let $[a] = \{x \in S : (a, x) \in R\}$ be the equivalence class of $a \in S$.

(a) For $a, b \in S$, one and only one of the following holds.

(a.i) $(a, b) \in R$ and $[a] = [b]$, (a.ii) $(a, b) \notin R$ and $[a] \cap [b] = \emptyset$.

(b) The set $P = \{[a] : a \in S\}$ of equivalence classes forms a partition of S, i.e., S is a disjoint union of the nonempty subsets $[a]$.

Examples (a) Let $S = \mathbf{Z}$, and $(a, b) \in R$ if $a \equiv b \pmod{n}$. Then the equivalence classes are $[0], [1], \ldots, [n-1]$.

(b) Let $S = \mathbf{R} \times \mathbf{R} = \mathbf{R}^2$, and $((x_1, y_1), (x_2, y_2)) \in R$ if $x_1^2 + y_1^2 = x_2^2 + y_2^2$. Then the equivalence classes are $[(r, 0)] = \{(x, y) : x^2 + y^2 = r^2\}$, $r \geq 0$.

(c) Let $S = \mathbf{R}$, and $(a, b) \in R$ if $|a - b|$ is an even integer. Then the equivalence classes are $[r, r + 1)$, $r \in [0, 2)$.

Theorem Let $P = \{A_j : j \in J\}$ be a partition of a non-empty set A. Define R on A by xRy if $x, y \in A_j$ for some $j \in J$. Then P is the set of equivalence classes of A under R.

Example (a) The remainder classes $[0], \ldots, [n-1]$ forms a partition of $\mathbf{Z}$.

(b) The straight lines $L_r = \{(x, y) : x + y = r\}$, $r \in \mathbf{R}$, forms partition of $\mathbf{R} \times \mathbf{R}$.

§9.1 - 9.4

More generally, one can define a relation between two sets.

Definition, notation, and terminology Let A and B be sets.

A relation R from A to B is a subset of $A \times B$. We write xRy if $(x, y) \in R$.

The **domain** of R is $\text{dom}R = \{x \in A : (x, y) \in R \text{ for some } y \in B\}$.

The **range** of R is $\text{ran}R = \{y \in B : (x, y) \in R \text{ for some } x \in A\}$.

Examples (a) Relations from $A = \{a, b, c\}$ to $B = \{1, 2, 3, 4\}$.

(b) Relations from $\mathbf{Z}$ to $\{0, 1\}$.

(c) Relations from $\mathbf{R}$ to $\mathbf{Z}$.