基礎數學 MA-1015A

Chapter 3. Relations and Partitions

§3.1 Relations

Definition

Let A and B be sets. R is a ***relation*** from A to B if R is a subset of $A \times B$. A relation from A to A is called a relation on A. If $(a,b) \in R$, we say a is R-related (or simply related) to b and write aRb. If $(a,b) \notin R$, we write $a \not R b$.

Example

Let R be the relation "is older than" on the set of all people. If a is 32 yrs old, b is 25 yrs old, and c is 45 yrs old, then aRb, cRb, $a \not R c$. Similarly, the "less than" relation on $\mathbb{R}$ is the set $\{(x,y) \mid x < y\}$.

§3.1 Relations

Remark:

Let A and B be sets. Every subset of $A \times B$ is a relations from A to B; thus every collection of ordered pairs is a relation. In particular, the empty set $\varnothing$ and the set $A \times B$ are relations from A to B ($R = \varnothing$ is the relation that "nothing" is related, while $R = A \times B$ is the relation that "everything" is related).

§3.1 Relations

Definition

For any set A, the ***identity relation on*** A is the (diagonal) set

$$I_A = \{(a,a) \mid a \in A\}.$$

Definition

Let A and B be sets, and R be a relation from A to B. The ***domain*** of R is the set

$$\mathrm{Dom}(R) = \{x \in A \mid (\exists\, y \in B)(xRy)\},$$

and the ***range*** of R is the set

$$\mathrm{Rng}(R) = \{y \in B \mid (\exists\, x \in A)(xRy)\}.$$

In other words, the domain of a relation R from A to B is the collection of all first coordinate of ordered pairs in R, and the range of R is the collection of all second coordinates.

§3.1 Relations

Definition

Let A and B be sets, and R be a relation from A to B. The ***inverse*** of R, denoted by R^{-1}, is the relation

$$R^{-1} = \{(y,x) \in B \times A \mid (x,y) \in R \text{ (or equivalently, } xRy)\}.$$

In other words, xRy if and only if $yR^{-1}x$ or equivalently, $(x,y) \in R$ if and only if $(y,x) \in R^{-1}$.

Example

Let $T = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid y < 4x^2 - 7\}$. To find the inverse of T, we note that

$$\begin{aligned}(x,y) \in T^{-1} &\Leftrightarrow (y,x) \in T \Leftrightarrow x < 4y^2 - 7 \Leftrightarrow x + 7 < 4y^2 \\ &\Leftrightarrow (x,y) \in \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid x + 7 < 0\} \cup \\ &\qquad \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid 0 \leqslant \frac{x+7}{4} < y^2\}.\end{aligned}$$

§3.1 Relations

Theorem

Let A and B be sets, and R be a relation from A to B.

1. $\mathrm{Dom}(R^{-1}) = \mathrm{Rng}(R)$.
2. $\mathrm{Rng}(R^{-1}) = \mathrm{Dom}(R)$.

Proof.

The theorem is concluded by

$$\begin{aligned} b \in \mathrm{Dom}(R^{-1}) &\Leftrightarrow (\exists\, a \in A)\big[(b, a) \in R^{-1}\big] \Leftrightarrow (\exists\, a \in A)\big[(a, b) \in R\big] \\ &\Leftrightarrow b \in \mathrm{Rng}(R)\,, \end{aligned}$$

and

$$\begin{aligned} a \in \mathrm{Rng}(R^{-1}) &\Leftrightarrow (\exists\, b \in B)\big[(b, a) \in R^{-1}\big] \Leftrightarrow (\exists\, b \in B)\big[(a, b) \in R\big] \\ &\Leftrightarrow a \in \mathrm{Dom}(R)\,. \end{aligned}$$

□

§3.1 Relations

Definition

Let A, B, C be sets, and R be a relation from A to B, S be a relation from B to C. The ***composite*** of R and S is a relation from A to C, denoted by $S \circ R$, given by

$$S \circ R = \Big\{ (a, c) \in A \times C \,\Big|\, (\exists\, b \in B) \big[(aRb) \wedge (bSc) \big] \Big\} .$$

We note that $\mathrm{Dom}(S \circ R) \subseteq \mathrm{Dom}(R)$ and it may happen that $\mathrm{Dom}(S \circ R) \subsetneq \mathrm{Dom}(R)$.

§3.1 Relations

Example

Let $A = \{1, 2, 3, 4, 5\}$, $B = \{p, q, r, s, t\}$ and $C = \{x, y, z, w\}$. Let R be the relation from A to B:

$$R = \{(1, p), (1, q), (2, q), (3, r), (4, s)\}$$

and S be the relation from B to C:

$$S = \{(p, x), (q, x), (q, y), (s, z), (t, z)\}.$$

Then $S \circ R = \{(1, x), (1, y), (2, x), (2, y), (4, z)\}$.

Example

Let $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x + 1\}$ and $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}$. Then

$$R \circ S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2 + 1\},$$
$$S \circ R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = (x + 1)^2\}.$$

Therefore, $S \circ R \neq R \circ S$.

§3.1 Relations

Theorem

Suppose that A, B, C, D are sets, R be a relation from A to B, S be a relation from B to C, and T be a relation from C to D.

(a) $(R^{-1})^{-1} = R$.

(b) $T \circ (S \circ R) = (T \circ S) \circ R$ (*so composition is associative*).

(c) $I_B \circ R = R$ *and* $R \circ I_A = R$.

(d) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Proof of (a).

(a) holds since

$$(a, b) \in (R^{-1})^{-1} \Leftrightarrow (b, a) \in R^{-1} \Leftrightarrow (a, b) \in R\,. \qquad \square$$

§3.1 Relations

Proof of (b) $T \circ (S \circ R) = (T \circ S) \circ R$.

Since $S \circ R$ is a relation from A to C, $T \circ (S \circ R)$ is a relation from $A \to D$. Similarly, $(T \circ S) \circ R$ is also a relation from A to D. Let $(a, d) \in A \times D$. Then

$$
\begin{aligned}
&(a, d) \in T \circ (S \circ R) \\
&\qquad \Leftrightarrow (\exists\, c \in C)\big[(a, c) \in S \circ R \wedge (c, d) \in T\big] \\
&\qquad \Leftrightarrow (\exists\, c \in C)(\exists\, b \in B)\big[(a, b) \in R \wedge (b, c) \in S \wedge (c, d) \in T\big] \\
&\qquad \Leftrightarrow (\exists\, (b, c) \in B \times C)\big[(a, b) \in R \wedge (b, c) \in S \wedge (c, d) \in T\big] \\
&\qquad \Leftrightarrow (\exists\, b \in B)(\exists\, c \in C)\big[(a, b) \in R \wedge (b, c) \in S \wedge (c, d) \in T\big] \\
&\qquad \Leftrightarrow (\exists\, b \in B)\big[(a, b) \in R \wedge (b, d) \in T \circ S\big] \\
&\qquad \Leftrightarrow (a, d) \in (T \circ S) \circ R\,.
\end{aligned}
$$

Therefore, $T \circ (S \circ R) = (T \circ S) \circ R$. □

§3.1 Relations

Proof of (c) $I_B \circ R = R = R \circ I_A$.

Let $(a, b) \in A \times B$ be given. Then

$$(a, b) \in I_B \circ R \Leftrightarrow (\exists\, c \in B)\big[(a, c) \in R \wedge (c, b) \in I_B\big]\,.$$

Note that $(c, b) \in I_B$ if and only if $c = b$; thus

$$(\exists\, c \in B)\big[(a, c) \in R \wedge (c, b) \in I_B\big] \Leftrightarrow (a, b) \in R\,.$$

Therefore, $(a, b) \in I_B \circ R \Leftrightarrow (a, b) \in R$. Similarly, $(a, b) \in R \circ I_A \Leftrightarrow (a, b) \in R$. □

Proof of (d) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Let $(a, c) \in A \times C$. Then

$$\begin{aligned}(c, a) \in (S \circ R)^{-1} &\Leftrightarrow (a, c) \in S \circ R \\ &\Leftrightarrow (\exists\, b \in B)\big[(a, b) \in R \wedge (b, c) \in S\big] \\ &\Leftrightarrow (\exists\, b \in B)\big[(c, b) \in S^{-1} \wedge (b, a) \in R^{-1}\big] \\ &\Leftrightarrow (c, a) \in R^{-1} \circ S^{-1}\,.\end{aligned}$$

□

§3.2 Equivalence Relations

Definition

Let A be a set and R be a relation on A.

1. R is ***reflexive*** on A if $(\forall\, x \in A)(xRx)$.
2. R is ***symmetric*** on A if $\big[\forall\,(x,y) \in A \times A\big](xRy \Leftrightarrow yRx)$.
3. R is ***transitive*** on A if

$$\big[\forall\,(x,y,z) \in A \times A \times A\big]\big[(xRy) \wedge (yRz)\big] \Rightarrow (xRz)\big].$$

A relation R on A which is reflexive, symmetric and transitive is called an ***equivalence relation*** on A.

An equivalence relation is often denoted by $\sim$ (the same symbol as negation but $\sim$ as negation is always in front of a proposition while $\sim$ as an equivalence relation is always between two elements in a set).

§3.2 Equivalence Relations

Example

The relation "divides" on $\mathbb{N}$ is reflexive and transitive, but not symmetric. The relation "is greater than" on $\mathbb{N}$ is only transitive（遞移律）but not reflexive and transitive.

Example

Let A be a set. The relation "is a subset of" on the power set $\mathcal{P}(A)$ is reflexive, transitive but not symmetric.

Example

The relation $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 = y^2\}$ is reflexive, symmetric and transitive on $\mathbb{R}$.

Example

The relation R on $\mathbb{Z}$ defined by $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x + y \text{ is even}\}$ is reflexive, symmetric and transitive.

§3.2 Equivalence Relations

Definition

Let A be a set and R be an equivalence relation on A. For $x \in A$, the ***equivalence class of*** x ***modulo*** R (or simply x ***mod*** R) is a subset of A given by

$$\bar{x} = \left\{ y \in A \,\middle|\, xRy \right\}.$$

Each element of $\bar{x}$ is called a ***representative*** of this class. The collection of all equivalence classes modulo R, called A ***modulo*** R, is denoted by A/R $\big($and is the set $A/R = \{\bar{x} \,|\, x \in A\}\big)$.

Example

The relation $H = \big\{(1,1),(2,2),(3,3),(1,2),(2,1)\big\}$ is an equivalence relation on the set $A = \{1,2,3\}$. Then

$$\overline{1} = \overline{2} = \{1,2\} \quad \text{and} \quad \overline{3} = \{3\}.$$

Therefore, $A/H = \big\{\{1,2\},\{3\}\big\}$.

§3.2 Equivalence Relations

Theorem

Let A be a non-empty set and R be an equivalence relation on A. For all $x, y \in A$, we have

(a) $x \in \bar{x}$ *and* $\bar{x} \subseteq A$.

(b) xRy *if and only if* $\bar{x} = \bar{y}$.

(c) $x \not R y$ *if and only if* $\bar{x} \cap \bar{y} = \varnothing$.

Proof.

It is clear that (a) holds. To see (b) and (c), it suffices to show that "$xRy \Rightarrow \bar{x} = \bar{y}$" and "$x \not R y \Rightarrow \bar{x} \cap \bar{y} = \varnothing$".

Assume that xRy. Then if $z \in \bar{x}$, we have xRz. The symmetry and transitivity of R then implies that yRz; thus $z \in \bar{y}$ which implies that $\bar{x} \subseteq \bar{y}$. Similarly, $\bar{y} \subseteq \bar{x}$; hence we conclude that "$xRy \Rightarrow \bar{x} = \bar{y}$".

Now assume that $\bar{x} \cap \bar{y} \neq \varnothing$. Then for for some $z \in A$ we have $z \in \bar{x} \cap \bar{y}$. Therefore, xRz and yRz. Since R is symmetric and transitive, then xRy which implies that "$x \not R y \Rightarrow \bar{x} \cap \bar{y} = \varnothing$". □

§3.2 Equivalence Relations

Definition

Let m be a fixed positive integer. For $x, y \in \mathbb{Z}$, we say x ***is congruent to*** y ***modulo*** m（以 m 為除數時 x 同餘 y）and write $x = y$ (**mod** m) if m divides $(x - y)$. The number m is called the ***modulus*** of the congruence.

Example

Using 4 as the modulus, we have

$$\begin{aligned} 3 &= 3 \pmod 4 \text{ because } 4 \text{ divides } 3-3=0\,, \\ 9 &= 5 \pmod 4 \text{ because } 4 \text{ divides } 9-5=4\,, \\ -27 &= 1 \pmod 4 \text{ because } 4 \text{ divides } -27-1=-28\,, \\ 20 &= 8 \pmod 4 \text{ because } 4 \text{ divides } 20-8=12\,, \\ 100 &= 0 \pmod 4 \text{ because } 4 \text{ divides } 100-0=100\,. \end{aligned}$$

§3.2 Equivalence Relations

Theorem

For every fixed positive integer m, the relation "congruence modulo m" is an equivalence relation on $\mathbb{Z}$.

Proof.

1. **(Reflexivity)** It is easy to see that $x \equiv x \pmod m$ for all $x \in \mathbb{Z}$. Therefore, congruence modulo m is reflexive on $\mathbb{Z}$.
2. **(Symmetry)** Assume that $x \equiv y \pmod m$. Then m divides $x - y$; that is, $x - y = mk$ for some $k \in \mathbb{Z}$. Therefore, $y - x = m(-k)$ which implies that m divides $y - x$; thus $y \equiv x \pmod m$.
3. **(Transitivity)** Assume that $x \equiv y \pmod m$ and $y \equiv z \pmod m$. Then $x - y = mk$ and $y - z = m\ell$ for some $k, \ell \in \mathbb{Z}$. Therefore, $x - z = m(k + \ell)$ which implies that m divides $x - z$; thus $x \equiv z \pmod m$. □

§3.2 Equivalence Relations

Definition

The set of equivalence classes for the relation congruence modulo m is denoted by $\mathbb{Z}_m$.

Remark: The elements of $\mathbb{Z}_m$ are sometimes called the ***residue*** (or ***remainder***) classes modulo m.

Example

For congruence modulo 4, there are four equivalence classes:

$$\overline{0} = \{\cdots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \cdots\} = \{4k \,|\, k \in \mathbb{Z}\},$$
$$\overline{1} = \{\cdots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \cdots\} = \{4k+1 \,|\, k \in \mathbb{Z}\},$$
$$\overline{2} = \{\cdots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \cdots\} = \{4k+2 \,|\, k \in \mathbb{Z}\},$$
$$\overline{3} = \{\cdots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \cdots\} = \{4k+3 \,|\, k \in \mathbb{Z}\}.$$

§3.2 Equivalence Relations

In general, we will prove that the equivalence relation "congruence modulo m" produces m equivalence classes

$$\bar{j} = \{mk + j \mid k \in \mathbb{Z}\}, \qquad j = 0, 1, \cdots, m-1.$$

The collection of these equivalence classes, by definition $\mathbb{Z}/(\text{mod } m)$, is usually denoted by $\mathbb{Z}_m$.

Theorem

Let m be a fixed positive integer. Then

1. *For integers x and y, $x = y \pmod m$ if and only if the remainder when x is divided by m* equals *the remainder when y divided by m.*
2. *$\mathbb{Z}_m$ consists of m distinct equivalence classes:*

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \cdots, \overline{m-1}\}.$$

§3.2 Equivalence Relations

Proof.

1. For a given $x \in \mathbb{Z}$, let $\big(q(x), r(x)\big)$ denote the unique pair in $\mathbb{Z} \times \mathbb{Z}$ obtained by the division algorithm satisfying

$$x = mq(x) + r(x) \quad \text{and} \quad 0 \leqslant r(x) < m\,.$$

Then

$$\begin{aligned} x = y \pmod{m} &\Leftrightarrow m \text{ divides } x - y \\ &\Leftrightarrow m \text{ divides } m\big(q(x) - q(y)\big) + r(x) - r(y) \\ &\Leftrightarrow m \text{ divides } r(x) - r(y) \\ &\Leftrightarrow r(x) - r(y) = 0\,. \end{aligned}$$

where the last equivalence following from the fact that $0 \leqslant r(x), r(y) < m$. □

§3.2 Equivalence Relations

Proof. (Cont'd).

2. Using ①, x and y are in the same equivalence classes (produced by the equivalence relation "congruence modulo m") if and only if x and y has the same remainder when they are divided by m. Therefore, we find that

$$\bar{x} = \left\{ mk + r(x) \,\middle|\, k \in \mathbb{Z} \right\} = \overline{r(x)} \qquad \forall\, x \in \mathbb{Z}\,.$$

Since $r(x)$ has values from $\{0, 1, \cdots, m-1\}$, we find that $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \cdots, \overline{m-1}\}$. The proof is completed if we show that $\overline{k} \cap \overline{j} = \varnothing$ if $k \neq j$ and $k, j \in \{0, 1, \cdots, m-1\}$. However, if $x \in \overline{k} \cap \overline{j}$, then

$$x = mq_1 + k = mq_2 + j$$

which is impossible since $k \neq j$ and $k, j \in \{0, 1, \cdots, m-1\}$. Therefore, there are exactly m equivalence classes. □

§3.3 Partitions

Definition

Let A be a non-empty set. $\mathcal{P}$ is a ***partition*** of A if $\mathcal{P}$ is a collection of subsets of A such that

1. if $X \in \mathcal{P}$, then $X \neq \varnothing$.
2. if $X \in \mathcal{P}$ and $Y \in \mathcal{P}$, then $X = Y$ or $X \cap Y = \varnothing$.
3. $\bigcup\limits_{X \in \mathcal{P}} X = A$.

In other words, a partition of a set A is a pairwise disjoint collection of non-empty subsets of A whose union is A.

§3.3 Partitions

Example

The family $\mathcal{G} = \big\{[n, n+1) \,\big|\, n \in \mathbb{Z}\big\}$ is a partition of $\mathbb{R}$.

Example

Each of the following is a partition of $\mathbb{Z}$:

1. $\mathcal{P} = \{E, D\}$, where E is the collection of even integers and D is the collection of odd integers.
2. $\mathcal{X} = \{\mathbb{N}, \{0\}, \mathbb{Z}^-\}$, where $\mathbb{Z}^-$ is the collection of negative integers.
3. $\mathcal{H} = \{A_k \,|\, k \in \mathbb{Z}\}$, where $A_k = \{3k, 3k+1, 3k+2\}$.

§3.3 Partitions

Theorem

If R is an equivalent relation on a non-empty set A, then A/R is a partition of A.

Proof.

First of all, each equivalence class $\bar{x} \in A/R$ must be non-empty since it contains x. Let $\bar{x}$ and $\bar{y}$ be two equivalence classes in A/R. If $\bar{x} \cap \bar{y} \neq \varnothing$, then there exists $z \in \bar{x} \cap \bar{y}$ which implies that xRz and yRz. By the symmetry and the transitivity of R we have xRy which implies that $\bar{x} = \bar{y}$.

Finally, it is clear that $\bigcup\limits_{\bar{x} \in A/R} \bar{x} \subseteq A$ since each $\bar{x} \subseteq A$. On the other hand, since each $y \in A$ belongs to the equivalence class $\bar{y}$, we must have $A \subseteq \bigcup\limits_{\bar{x} \in A/R} \bar{x}$. Therefore, $A = \bigcup\limits_{\bar{x} \in A/R} \bar{x}$. □

§3.3 Partitions

Theorem

Let $\mathcal{P}$ be a partition of a non-empty set A. For $x, y \in A$, define xQy if and only if there exists $C \in \mathcal{P}$ such that $x, y \in C$. Then

1. *Q is an equivalence relation on A.*
2. *$A/Q = \mathcal{P}$.*

Proof.

It is clear that Q is reflexive and symmetric on A, so it suffices to show the transitivity of Q to complete ①. Suppose that xQy and yQz. By the definition of the relation Q there exists C_1 and C_2 in $\mathcal{P}$ such that $x, y \in C_1$ and $y, z \in C_2$; hence $C_1 \cap C_2 \neq \varnothing$. Then $C_1 = C_2$ by the fact that $\mathcal{P}$ is a partition and $C_1, C_2 \in \mathcal{P}$. Therefore, $x, z \in C_1$ which implies that xQz. □

§3.3 Partitions

Proof. (Cont'd).

Next, we claim that if $C \in \mathcal{P}$, then $x \in C$ if and only if $\bar{x} = C$. It suffices to show the direction "$\Rightarrow$" since $x \in \bar{x}$.

Suppose that $C \in \mathcal{P}$ and $x \in C$.

1. "$C \subseteq \bar{x}$": Let $y \in C$ be given. By the fact that $x \in C$ we must have yQx. Therefore, $y \in \bar{x}$ which shows $C \subseteq \bar{x}$.
2. "$\bar{x} \subseteq C$": Let $y \in \bar{x}$ be given. Then there exists $\widetilde{C} \in \mathcal{P}$ such that $x, y \in \widetilde{C}$. By the fact that $x \in C$, we find that $C \cap \widetilde{C} \neq \varnothing$. Since $\mathcal{P}$ is a partition of A and $C, \widetilde{C} \in \mathcal{P}$, we must have $C = \widetilde{C}$; thus $y \in C$. Therefore, $\bar{x} \subseteq C$. □

§3.3 Partitions

Proof. (Cont'd).

Now we show that $A/Q = \mathcal{P}$. If $C \in \mathcal{P}$, then $C \neq \varnothing$; thus there exists $x \in C$ for some $x \in A$. Then the claim above shows that $C = \overline{x} \in A/Q$. Therefore, $\mathcal{P} \subseteq A/Q$. On the other hand, if $\overline{x} \in A/Q$, by the fact that $\mathcal{P}$ is a partition of A, there exists $C \in \mathcal{P}$ such that $x \in C$. Then the claim above shows that $\overline{x} = C$. Therefore, $A/Q \subseteq \mathcal{P}$. □

Remark: The relation Q defined in the theorem proved above is called ***the equivalence relation associated with the partition*** $\mathcal{P}$.

§3.3 Partitions

Example

Let $A = \{1,2,3,4\}$, and let $\mathcal{P} = \{\{1\},\{2,3\},\{4\}\}$ be a partition of A with three sets. The equivalence relation Q associated with $\mathcal{P}$ is $\{(1,1),(2,2),(3,3),(4,4),(2,3),(3,2)\}$. The three equivalence classes for Q are $\overline{1} = \{1\}$, $\overline{2} = \overline{3} = \{2,3\}$ and $\overline{4} = \{4\}$. The collection of all equivalence classes A/Q is precisely $\mathcal{P}$.

Example

The collect $\mathcal{P} = \{A_0, A_1, A_2, A_3\}$, where

$$A_j = \{4k + j \,|\, k \in \mathbb{Z}\} \text{ for } j = \{0,1,2,3\},$$

is a partition of $\mathbb{Z}$ because of the division algorithm. The equivalence relation associated with the partition $\mathcal{P}$ is the relation of congruence modulo 4, and each A_j is the residue class of j modulo 4 for $j = 0,1,2,3$.

§3.4 Modular Arithmetic

Theorem

Let m be a positive integer and a, b, c and d be integers. If $a = c \pmod{m}$ and $b = d \pmod{m}$, then $a + b = c + d \pmod{m}$ and $a \cdot b = c \cdot d \pmod{m}$.

Proof.

Since $a = c \pmod{m}$ and $b = d \pmod{m}$, we have $a - c = mk_1$ and $b - d = mk_2$ for some $k_1, k_2 \in \mathbb{Z}$. Then

$$a + b = c + mk_1 + d + mk_2 = c + d + m(k_1 + k_2)$$

and

$$a \cdot b = (c + mk_1) \cdot (d + mk_2) = c \cdot d + m(c \cdot k_2 + d \cdot k_1 + k_1 \cdot k_2) .$$

Therefore, $a + b = c + d \pmod{m}$ and $a \cdot b = c \cdot d \pmod{m}$. □

§3.4 Modular Arithmetic

Definition

For each natural number m,

1. the ***sum of the classes*** $\overline{x}$ and $\overline{y}$ in $\mathbb{Z}_m$, denoted by $\overline{x}+\overline{y}$, is defined to be the class containing the integer $x+y$;
2. the ***product of the classes*** $\overline{x}$ and $\overline{y}$ in $\mathbb{Z}_m$, denoted by $\overline{x}\cdot\overline{y}$, is defined to be the class containing the integer $x\cdot y$.

In symbols, $\overline{x}+\overline{y}=\overline{x+y}$ and $\overline{x}\cdot\overline{y}=\overline{x\cdot y}$.

Example

In $\mathbb{Z}_6$, $\overline{5}+\overline{3}=\overline{2}$ and $\overline{4}\cdot\overline{5}=\overline{2}$.

Example

In $\mathbb{Z}_8$, $(\overline{5}+\overline{7})\cdot(\overline{6}+\overline{5})=\overline{12}\cdot\overline{11}=\overline{4}\cdot\overline{3}=\overline{12}=\overline{4}$.

§3.4 Modular Arithmetic

Example

Find $\overline{3^{63}}$ in $\mathbb{Z}_7$. Since

$$\overline{3^1} = \overline{3}\,, \quad \overline{3^2} = \overline{2}\,, \quad \overline{3^3} = \overline{6}\,, \quad \overline{3^4} = \overline{4}\,, \quad \overline{3^5} = \overline{5}\,, \quad \overline{3^6} = \overline{1}\,,$$

we have $\overline{3^{63}} = \overline{3^{60} \cdot 3^3} = \overline{6}$.

Example

For every integer k, 6 divides $k^3 + 5k$. In fact, by the division algorithm, for each $k \in \mathbb{Z}$ there exists a unique pair (q, r) such that $k = 6q + r$ for some $0 \leqslant r < 5$. Therefore, in $\mathbb{Z}_6$ we have

$$\begin{aligned} \overline{k^3 + 5k} &= \overline{(6q + r)^3} + \overline{5(6q + r)} = \overline{r^3} + \overline{5 \cdot r} \\ &= \overline{r^3} + \overline{(-1) \cdot r} = \overline{r^3 - r}\,. \end{aligned}$$

It is clear that then $\overline{k^3 + 5k} = \overline{0}$ since

$$\overline{0^3 - 0} = \overline{1^3 - 1} = \overline{2^3 - 2} = \overline{3^3 - 3} = \overline{4^3 - 4} = \overline{5^3 - 5}\,.$$

§3.4 Modular Arithmetic

Theorem

Let m be a positive composite integer. Then there exists non-zero equivalence classes $\bar{x}$ and $\bar{y}$ in $\mathbb{Z}_m$ such that $\bar{x} \cdot \bar{y} = \bar{0}$.

Proof.

Since m is a positive composite integer, $m = x \cdot y$ for some $x, y \in \mathbb{N}$, $1 < x, y < m$. Since $1 < x, y < m$, $\bar{x}, \bar{y} \neq \bar{0}$. Therefore, in $\mathbb{Z}_m$ $\bar{0} = \bar{m} = \bar{x} \cdot \bar{y}$ which concludes the theorem. □

Theorem

Let p be a prime. If $\bar{x} \cdot \bar{y} = \bar{0}$ in $\mathbb{Z}_p$, then either $\bar{x} = \bar{0}$ or $\bar{y} = \bar{0}$.

Proof.

Let $\bar{x}, \bar{y} \in \mathbb{Z}_p$ and $\bar{x} \cdot \bar{y} = \bar{0}$. Then $x \cdot y = 0 \pmod{p}$. Therefore, p divides $x \cdot y$. Since p is prime, $p \mid x$ or $p \mid y$ which implies that $\bar{x} = \bar{0}$ or $\bar{y} = \bar{0}$. □

§3.4 Modular Arithmetic

Theorem

Let p be a prime. If $xy = xz \pmod{p}$ and $x \neq 0 \pmod{p}$, then $y = z \pmod{p}$.

Proof.

If $xy = xz \pmod{p}$, then $x(y-z) = 0 \pmod{p}$. By the previous theorem $\overline{x} = \overline{0}$ or $\overline{y-z} = \overline{0}$. Since $x \neq 0 \pmod{p}$, we must have $\overline{y} = \overline{z}$; thus $y = z \pmod{p}$. □

Corollary (Cancellation Law for $\mathbb{Z}_p$)

Let p be a prime, and $\overline{x}, \overline{y}, \overline{z} \in \mathbb{Z}_p$. If $\overline{x} \cdot \overline{y} = \overline{x} \cdot \overline{z}$, then $\overline{x} \neq \overline{0}$ or $\overline{y} = \overline{z}$.