§3.3 Partitions

Example

Let $A = \{1,2,3,4\}$, and let $\mathcal{P} = \big\{\{1\},\{2,3\},\{4\}\big\}$ be a partition of A with three sets. The equivalence relation Q associated with $\mathcal{P}$ is $\big\{(1,1),(2,2),(3,3),(4,4),(2,3),(3,2)\big\}$. The three equivalence classes for Q are $\bar{1} = \{1\}$, $\bar{2} = \bar{3} = \{2,3\}$ and $\bar{4} = \{4\}$. 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, $p | x$ or $p | y$ 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 $\overline{y} = \overline{z}$.