

## 4.2 Proofs involving Congruence of Integers

*(Def)*  $a, b \in \mathbb{Z}$ ,  $n \geq 2$ , we say that  $a$  is **congruent to  $b$  modulo  $n$** , written  $a \equiv b \pmod{n}$ , if  $n \mid (a - b)$ .

i.e.,  $a$  and  $b$  have the same remainder when divided by  $n$ .

e.g.,

$$\begin{aligned} \cdot \forall x \in \mathbb{Z} \Rightarrow x = 2q \text{ or } x = 2q + 1 \text{ for some } q \in \mathbb{Z} \\ \Rightarrow 2 \mid (x - 0) \text{ or } 2 \mid (x - 1) \\ \Rightarrow x \equiv 0 \pmod{2} \text{ or } x \equiv 1 \pmod{2} \end{aligned}$$

$$\begin{aligned} \cdot \forall x \in \mathbb{Z} \Rightarrow x = 3q \text{ or } x = 3q + 1 \text{ or } x = 3q + 2 \text{ for some } q \in \mathbb{Z} \\ \Rightarrow 3 \mid (x - 0) \text{ or } 3 \mid (x - 1) \text{ or } 3 \mid (x - 2) \\ \Rightarrow x \equiv 0 \pmod{3} \text{ or } x \equiv 1 \pmod{3} \text{ or } x \equiv 2 \pmod{3} \end{aligned}$$

$\vdots$   
 $\vdots$

$$\cdot \forall x \in \mathbb{Z} \Rightarrow x \equiv 0 \pmod{n} \text{ or } x \equiv 1 \pmod{n} \text{ or } x \equiv 2 \pmod{n} \text{ or } \dots, x \equiv n - 1 \pmod{n}.$$

R4.8 Let  $a, b, k, n \in \mathbb{Z}$ , where  $n \geq 2$ .

If  $a \equiv b \pmod{n} \implies ka \equiv kb \pmod{n}$

*(Pf)*:

(4.2 cont.)

R4.9 Let  $a, b, c, d, n \in \mathbb{Z}$ , where  $n \geq 2$ .

If  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n} \implies a + c \equiv b + d \pmod{n}$

$\langle Pf \rangle$ :

R4.10 Let  $a, b, c, d, n \in \mathbb{Z}$ , where  $n \geq 2$ .

If  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n} \implies ac \equiv bd \pmod{n}$

$\langle Pf \rangle$ :

(4.2 cont.)

R4.11  $\Rightarrow$  Ex4.10 Let  $a, b \in \mathbb{Z}$ , prove that if  $a^2 + 2b^2 \equiv 0 \pmod{3}$   
 $\Rightarrow$  either  $a \equiv 0 \pmod{3}$  and  $b \equiv 0 \pmod{3}$   
or  $a \not\equiv 0 \pmod{3}$  and  $b \not\equiv 0 \pmod{3}$   
(Pf):