

## Congruence

Let  $n \in \mathbb{N} \setminus \{1\}$  and  $a \in \mathbb{Z}$ . Then  $a$  modulo  $n$ , denoted by  $a \bmod n$ , is  $r$  such that

$$n = aq + r$$

where  $0 \leq r < n$  and  $q \in \mathbb{Z}$ .

**Example 4.26.**  $49 \bmod 7 = 0$  since  $49 = 7(7) + 0$ .

**Problem 4.27.** Determine  $63 \bmod 6$ .

The integers  $a$  and  $b$  are congruent modulo  $n$ , denoted by  $a \equiv b \bmod n$ , if and only if  $ak_1 + r = bk_2 + r = n$  where  $r, k_1, k_2 \in \mathbb{Z}$  and  $r < n$ . In other words,  $a \equiv b \bmod n$  if and only if  $n \mid a - b$ .

**Example 4.28.** Determine if 6 is congruent to 2 modulo 4. First note that  $6 = 1(4) + 2$  and  $4 = 1(2) + 2$ . Hence  $6 \equiv 2 \bmod 4$ .

**Theorem 4.29.** If  $a \equiv b \bmod n$  and  $c \equiv d \bmod n$  then  $a + c \equiv b + d \bmod n$ .

*Proof.* Suppose  $a \equiv b \bmod n$  and  $c \equiv d \bmod n$ . Then  $n \mid a - b$  and  $n \mid c - d$ . Hence there exists  $k$  and  $\ell$  such that  $a - b = nk$  and  $c - d = n\ell$ . Thus  $(a + c) - (b + d) = n(k + \ell)$  which implies  $a + c \equiv b + d \bmod n$ .  $\square$