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 mod 7 = 0 since 49 = 7(7) + 0.

Problem 4.27. *Determine* 63 mod 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 $n \mid a - b$. To see that the definitions are equivalent let us the Division Algorithm to write $a = nq_a + r_a$ and $b = nq_b + r_b$ where $0 \leq r_a, r_b < n$. Since $n \mid (a - b)$ implies there exists $q \in \mathbb{Z}$ such that $a - b = nq$ we have

$$\begin{aligned} n|(a-b) &\iff a - b = nq \\ &\iff a = nq + b \\ &\iff a = nq + nq_b + r_b \quad \text{where} \quad 0 \leq r_b < n \\ &\iff a = n(q + q_b) + r_b \quad \text{where} \quad 0 \leq r_b < n. \end{aligned}$$

Therefore $r_b = r_a$ as desired.

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* $a \equiv b \mod n$ *and* $c \equiv d \bmod n$ *then* $a + c \equiv b + d \mod n$*.*

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 ℓ such that $a - b = nk$ and $c - d = n\ell$. Thus $(a + c) - (b + d) = n(k + \ell)$ which implies $a + c \equiv b + d \bmod n$. $\square$