0: Congruence and Mod Equivalence

Let a and b be integers, and let m be a positive integer. Then, $a \equiv_m b$ iff $a \mod m = b \mod m$.

To prove the iff statement, we will prove the implication in both directions.

Suppose that $a \equiv_m b$. Thus, by definition of mod congruence

$$m|(a-b)$$

By definition of $|$, there exists a $k \in \mathbb{Z}$ such that,

$$a - b = mk$$

$$a = mk + b$$

$$a \mod m = (mk + b) \mod m$$

The intuition for the next statement is as follows: the $k + l \mod m$ operation can be thought of travelling around one modular circle with m notches $k + l$ number of times and returning the final position on the circle. Since we make a complete loop every m steps, they don't contribute to the final position of the on the circle. As such, we can ignore the complete loops around the circle by taking the mod of each number and returning the sum of that.

$$a \mod m = mk \mod m + b \mod m$$

$$a \mod m = b \mod m \text{ [it is obvious that } \frac{m * k}{m} \text{ will have a remainder of 0]}$$

Thus, we have shown that $a \equiv_m b \Rightarrow a \mod m = b \mod m$.

Now we will prove the implication in the other direction. Suppose that $a \mod m = b \mod m$. Using this and the definition of $\mod m$, we can say that there exists a $k_0, k_1 \in \mathbb{Z}$ such that $a = mk_0 + a \mod m$ (1) and $b = mk_1 + b \mod m$ (2).

$a - b = (mk_0 + a \mod m) - (mk_1 + b \mod m)$	[(1) − (2)]
$a - b = m(k_0 - k_1) + (a \mod m - b \mod m)$	
$a - b = m(k_0 - k_1)$	$(a \mod m = b \mod m)$
$m\|(a - b)$	[definition of $\|$ since $k_0 - k_1 \in \mathbb{Z}$]
$a \equiv_m b$	[definition of mod congruence]

As such, we have shown that $a \mod m = b \mod m \Rightarrow a \equiv_m b$.

Since we have proved the implication in both directions, we have proved the iff statement that $a \equiv_m b$ iff $a \mod m = b \mod m$. □

1: Adding Congruences

Let $a, b, c, d \in \mathbb{Z}$, and let m be a positive integer. Then, if $a \equiv_m b$ and $c \equiv_m d$, then $a + c \equiv_m b + d$.

We start by unrolling the definition of $\equiv_m$ and writing that

$$m|(a - b)$$

$$m|(c - d)$$

By the definition of $|$, there exists a $k_0, k_1 \in \mathbb{Z}$ such that

$$a = mk_0 + b \ (1)$$

$$c = mk_1 + d \ (2)$$

We can now perform the follow calculations:

$$\begin{aligned}
a + c &= (mk_0 + b) + (mk_1 + d) && [(1) + (2)] \\
a + c - b - d &= mk_0 + mk_1 \\
(a + c) - (b + d) &= m(k_0 - k_1) && [\text{associativity of arithmetic expressions}] \\
m|[(a + c) - (b + d)] &&& [\text{definition of } | \text{ since } k_0 - k_1 \in \mathbb{Z}] \\
a + c &\equiv_m (b + d) && [\text{definition of mod congruence}]
\end{aligned}$$

Thus, we have shown that if $a \equiv_m b$, then $a + c \equiv_m b + d$. □