Modular Arithmetic

September 2017

Unless specified, assume all variables are natural (positive integers).

Definition $a \equiv b \pmod{n}$ means there exists an integer k such that $a = kn + b$.
(This says that a and b both have the same remainder when divided by n.)
You say "a and b are congruent modulo n".

1. Find $57 \pmod{11}$.

2. Prove that $a \equiv b \pmod{n} \Leftrightarrow (a - b) \equiv 0 \pmod{n}$.

3. Prove that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.

4. Prove that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

5. Prove that $a \equiv b \pmod{n} \Leftrightarrow ac \equiv bc \pmod{nc}$ for any c.

6. Solve the following linear congruences (find all solutions):

(a) $3x \equiv 5 \pmod{7}$

(b) $6x \equiv 1 \pmod{3}$

(c) $4x \equiv 0 \pmod{6}$

7. Solve the following simultaneous congruences:

$$\begin{cases} 2x \equiv 5 \pmod{7} \\ 5x \equiv 7 \pmod{9} \end{cases}$$