The Calculus of Remainders

Notation: 1) If $a, m \in \mathbb{Z}$ are integers and $m > 0$, then $\mathrm{rem}(a, m)$ denotes the remainder obtained when a is divided by m; i.e. $r = \mathrm{rem}(a, m)$ satisfies

$$0 \leq r < m \quad \text{and} \quad r = a - qm,$$

for some integer q.

2) For integers $a, b, m \in \mathbb{Z}$ write

$$a \equiv b \pmod{m} \quad \text{or} \quad a \equiv b\,(m)$$

if a and b have the same remainders when divided by m:

$$\mathrm{rem}(a, m) = \mathrm{rem}(b, m).$$

Theorem 1: $a \equiv b \pmod{m} \;\Leftrightarrow\; m|(a-b)$.

Theorem 2: (Computational Rules)
Let $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$ and $n \in \mathbb{N}$. Then:

a) $a \pm c \equiv b \pm d \pmod{m}$;

b) $ac \equiv bd \pmod{m}$;

c) $a^n \equiv b^n \pmod{m}$.