Modular Arithmetic

Let \( \mathbb{Z} \) denote the set of all integers. \( \mathbb{Z} = \{0, \pm 1, \pm 2, \ldots \} \).

For \( a, b \in \mathbb{Z} \),

\[ a \mid b \iff \text{there is } q \in \mathbb{Z} \text{ such that } aq = b. \]

\textbf{a divides } b
The Division Theorem

For every $a, b \in \mathbb{Z}, b \neq 0$, there are unique $q, r \in \mathbb{Z}$

$$a = qb + r, \quad 0 \leq r < |b| .$$

Write: $r = a \% b \quad q = a \text{ div } b$

Note that $b \mid a \iff r = 0$ in the above.
An integer \( p > 1 \) is called **prime** if its only divisors are \( \pm 1 \) and \( \pm p \). I.e.

\[
x \mid p \implies x \in \{1, -1, p, -p\}
\]

**Theorem:** If \( p \) is prime and \( p \mid ab \) then \( p \mid a \) or \( p \mid b \).
Let $n$ be a positive integer. For any two integers $a$ and $b$, define

$$a \equiv b \pmod{n} \iff n \mid (a - b)$$

$a$ is congruent to $b$ modulo $n$.

Sometimes write $a \equiv b \pmod{n}$ or $a \equiv_n b$

**Fact:** $a \equiv b \pmod{n}$ if and only if $a \% n = b \% n$. 
The set of possible remainders: \( \mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\} \) yields a complete set of residue class representatives modulo \( n \).

Warning: in some programming languages, \( a \% b \) is negative when \( a \) is negative.
We can do arithmetic on the set $\mathbb{Z}_n$ by adding, subtracting or multiplying as integers, and then dividing by $n$ and keeping the remainder.

Example: with $n = 12$:

$8 + 6 = 2 \quad 4 - 11 = -7 = 5$

$5 \times 6 = 6 \quad 8 \times 6 = 0$. 