CSE 311: Foundations of Computing I

Modular Arithmetic: Definitions and Properties

Definition: "a divides b"

For $a \in \mathbb{Z}, b \in \mathbb{Z}$ with $a \neq 0$:

$\boxed{a \mid b \leftrightarrow \exists k \in \mathbb{Z}\ (b = ka)}$

Division Theorem

For $a \in \mathbb{Z}, d \in \mathbb{Z}$ with $d > 0$, there exist *unique integers* q, r with $0 \leq r < d$, such that $a = dq + r$.

To put it another way, if we divide d into a, we get a unique quotient ($q = a$ div d) and non-negative remainder smaller than d ($r = a$ mod d).

Definition: "a is congruent to b modulo m"

For $a, b, m \in \mathbb{Z}$ with $m > 0$:

$\boxed{a \equiv_m b \leftrightarrow m \mid (a - b)}$

Properties of mod

Let a, b, c, d, m be integers with $m > 0$.

- If $a \equiv_m b$, then $b \equiv_m a$.
- If $a \equiv_m b$ and $c \equiv_m d$, then $a + c \equiv_m b + d$.
- If $a \equiv_m b$ and $c \equiv_m d$, then $ac \equiv_m bd$.
- If $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$.
- $a \equiv_m b$ if and only if $a \ \% \ m = b \ \% \ m$.

Definition: Prime

- An integer p greater than 1 is called **prime** if the only positive factors of p are 1 and p.
- A positive integer that is greater than 1 and is not prime is called **composite**.

GCD and Euclid's algorithm

- $\gcd(a, b)$ is the largest integer d such that $d \mid a$ and $d \mid b$.
- **Euclid's algorithm:** To efficiently compute $\gcd(a, b)$, you can repeatedly apply these facts:
  - $\gcd(a, b) = \gcd(b, a \bmod b)$
  - $\gcd(a, 0) = a$