# CSE 311: Foundations of Computing I

## Modular Arithmetic: Definitions and Properties

### Definition: "a divides b"

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

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

### 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 $a, b, m$ be integers with $m > 0$. Then, $a \equiv_m b$ if and only if $a$ mod $m = b$ mod $m$.
- Let $m$ be a positive integer. If $a \equiv_m b$ and $c \equiv_m d$, then $a + c \equiv_m b + d$.
- Let $m$ be a positive integer. If $a \equiv_m b$ and $c \equiv_m d$, then $ac \equiv_m bd$.
- Let $a, b, m$ be integers with $m > 0$. Then, $(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$.
  - You can derive this using the Multiplication Property of Congruences; note that $a \equiv_m (a \bmod m)$ and $b \equiv_m (b \bmod m)$.

### 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:
  - $\gcd(a, b) = \gcd(b, a \bmod b)$
  - $\gcd(a, 0) = a$

### Bézout's Theorem and Multiplicative Inverses

- **Bézout's Theorem:** If $a$ and $b$ are positive integers, then there exist integers $s$ and $t$ such that $\gcd(a, b) = sa + tb$.
  - To find $s$ and $t$, you can use the Extended Euclidean Algorithm. See slides for a full walkthrough.
- The **multiplicative inverse mod** $m$ of $a \bmod m$ is $b \bmod m$ iff $ab \equiv_m 1$.
- Suppose $\gcd(a, m) = 1$. By Bézout's Theorem, there exist integers $s$ and $t$ such that $sa + tm = 1$. Taking the mod of both sides, we get $(sa + tm) \bmod m = 1 \bmod m = 1$, so $sa \equiv_m 1$. Thus, $s \bmod m$ is the multiplicative inverse of $a$.