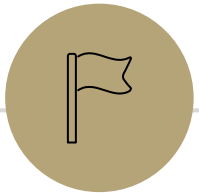
Number Theory Cont.

CSE 311: Foundations of Computing I
Lecture 10

Announcements

- HW2 solutions and Number Theory Reference Sheets are at the front
- HW3 is due tonight at 11:59 pm



Review

Modular Arithmetic

Divides

For integers a, b, we say $a \mid b$ ("a divides b") iff there exists some integer k such that $b = ka$.

Division Theorem

For any integer a and positive integer d, there exist unique integers q, r with $0 \leq r < d$ such that $a = qd + r$.

Congruence

For integers a, b and positive integer m, we say $a \equiv_m b$ iff $m \mid (a - b)$.

Notation

We will work with the notation $a \equiv_m b$.

$$(19 + 33) \cdot 5 \equiv_{10} 52 \cdot 5 \equiv_{10} 260 \equiv_{10} 0$$

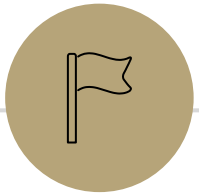
In practice, you'll often see the notation $a \equiv b \pmod{m}$.

$$(19 + 33) \cdot 5 \equiv 52 \cdot 5 \equiv 260 \equiv 0 \pmod{10}$$

Properties of Mod

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

- 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 $a \equiv_m c$.



Modular Arithmetic Proofs

Prove or Disprove

Definition
$a \mid b \coloneqq \exists k \in \mathbb{Z}\,(b = ka)$

Claim 1: For integers a, b, c if $b \mid a$ and $c \mid a$ then $bc \mid a$.

Claim 2: For integers a, b, c if $a \mid b$ and $a \mid c$ then $a \mid bc$.

Poll Everywhere
pollev.com/anjalia

Prove or Disprove

Definition
$a \mid b \coloneqq \exists k \in \mathbb{Z}\,(b = ka)$

Claim 1: For integers a, b, c if $b \mid a$ and $c \mid a$ then $bc \mid a$.

Prove or Disprove

Definition
$a \mid b \coloneqq \exists k \in \mathbb{Z}\,(b = ka)$

Claim 2: For integers a, b, c if $a \mid b$ and $a \mid c$ then $a \mid bc$.

For integers a, b and $m > 0$, $a \equiv_m b$ if and only if $a \,\%\, m = b \,\%\, m$.

$\Rightarrow$

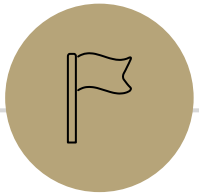
For integers a, b and $m > 0$, $a \equiv_m b$ if and only if $a \,\%\, m = b \,\%\, m$.

$\Leftarrow$

Summary: Properties of Mod

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

- 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 $a \,\%\, m = b \,\%\, m$.



Primes & GCD

Prime and Composite

Definition:

An integer $p > 1$ is prime iff _____

_____.

An integer $p > 1$ is composite iff _____

_____.

Greatest Common Divisor

Definition:

The Greatest Common Divisor of integers a and b (denoted $\gcd(a, b)$) is

_____

_____.

For Example:

$\gcd(99,18) =$

$\gcd(100, 125) =$

$\gcd(7,11) =$

$\gcd(13,0) =$

Calculating the GCD: Approach 1

Fundamental Theorem of Arithmetic: _____

_____.

Approach 1 to finding $\mathbf{gcd}(a, b)$:

- Find the prime factorization of a
- Find the prime factorization of b
- Identify all common prime factors.
- Multiply the common prime factors together. This is the GCD.

Calculating the GCD: Approach 2

Claim: _____.

For example:

We'll prove this in a minute. But first: how can we use this fact to devise an algorithm for computing $\mathbf{gcd}(a, b)$?

Calculating the GCD: Approach 2

Euclid's Algorithm. To find $\mathbf{gcd}(a, b)$:

- Repeatedly use $\mathbf{gcd}(a, b) = \mathbf{gcd}(b, a \,\%\, b)$ to reduce numbers
- Stop once you reach $\mathbf{gcd}(g, 0)$. Return g.

For Example:

$\mathbf{gcd}(660,126) =$

Euclid’s Algorithm in Java

Proof of Claim

Claim: For positive integers a, b, $\gcd(a, b) = \gcd(b, a \,\%\, b)$.

How do you show that two GCDs are equal?

Claim: For positive integers a, b, $\gcd(a, b) = \gcd(b, a \,\%\, b)$.