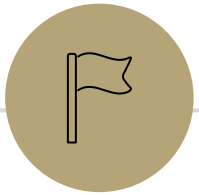
Number Theory Cont.

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 $a \equiv_m b$.

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

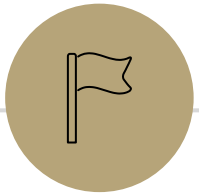
In practice, you'll often see the notation $a \equiv b \pmod{m}$.

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

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 $bc \mid a$.

This claim is false. Consider $a = 10, b = 5, c = 5$. Then $b \mid a$ and $c \mid a$ but $bc \nmid a$. Thus this is a counterexample to the claim.

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 $a \mid bc$.

This claim is true. Let a, b, c be arbitrary integers. Suppose $a \mid b$ and $a \mid c$. Then there exists some integers k, j such that $b = ak$ and $c = aj$. Then $bc = ak \cdot aj = a(akj)$. Since a, k, j are integers akj is an integer. So by definition of divides, $a \mid bc$. Since a, b, c were arbitrary, the claim holds.

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

$\Rightarrow$ Let $a, b, m > 0$ be arbitrary integers, and suppose $a \equiv_m b$. Then $m \mid (a - b)$. So there exists some integer k such that $a - b = km$. So $a = km + b$.

By the Division Theorem, $a = qm + (a \,\%\, m)$ for some integer q, where $0 \leq a \,\%\, m < m$. Thus:

$$km + b = qm + (a \,\%\, m)$$

$$b = qm - km + (a \,\%\, m)$$

$$b = (q - k)m + (a \,\%\, m)$$

By the Division Theorem again, we have that $b \,\%\, m = a \,\%\, m$. Since a, b, m were arbitrary, the claim holds.

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

$\Leftarrow$ Let $a, b, m > 0$ be arbitrary integers, and suppose $a \,\%\, m = b \,\%\, m$. By the Division Theorem, $a = mq + (a \,\%\, m)$ for some integer q, and $b = ms + (b \,\%\, m)$ for some integer s. Thus:

$$a - b = \big(mq + (a \,\%\, m)\big) - \big(ms + (b \,\%\, m)\big)$$

$$a - b = mq - ms + (a \,\%\, m) - (b \,\%\, m)$$

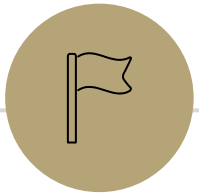
$$a - b = m(q - s)$$

Since q, s are integers, $q - s$ is an integer. So $m \mid (a - b)$. So $a \equiv_m b$. Since a, b, m were arbitrary, the claim holds.

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 its only positive divisors are 1 and p.

An integer $p > 1$ is composite iff it is not prime.

Greatest Common Divisor

Definition:

The Greatest Common Divisor of integers a and b (denoted $\gcd(a, b)$) is the largest integer c such that $c \mid a$ and $c \mid b$.

For Example:

$\gcd(99,18) = 9$

$\gcd(100, 125) = 25$

$\gcd(7,11) = 1$

$\gcd(13,0) = 13$

Calculating the GCD: Approach 1

Fundamental Theorem of Arithmetic: Every positive integer greater than 1 has a unique prime factorization.

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

For example:

$$\gcd(10, 6) = \gcd(6,4)$$

$$\gcd(110,30) = \gcd(30,20)$$

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

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:

$$\begin{aligned}\mathbf{gcd}(660,126) &= \mathbf{gcd}(126,30)\\ &= \mathbf{gcd}(30,6)\\ &= \mathbf{gcd}(6,0)\\ &= 6\end{aligned}$$

Euclid's Algorithm in Java

```
// assumes a >= 0 and b >= 0
public int gcd(int a, int b) {
     if (b == 0) {
          return a;
     } else {
          return gcd(b, a % b);
     }
}
```

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?

- First consider some arbitrary common divisor of a and b, call it d. Prove that d is a divisor of $a \,\%\, b$.
- Then consider some arbitrary common divisor of b and $a \,\%\, b$, call it d. Prove that d is a divisor of a.
- Thus a and b have the same common divisors as b and $a \,\%\, b$. So their GCDs are equal.

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

Let a, b be arbitrary positive integers. By the Division Theorem, $a = qb + (a \,\%\, b)$ for some int q.

Let d be arbitrary. Suppose $d \mid b$ and $d \mid a \,\%\, b$. We aim to show that $d \mid a$. By definition of divides, $b = kd$ and $a \,\%\, b = jd$ for some integers k, j. Then it follows that:

$$a = qb + (a \,\%\, b) = q \cdot kd + jd = d(qk + j)$$

Since q, k, j are integers, $qk + j$ is an integer. So $d \mid a$.

Now suppose $d \mid a$ and $d \mid b$. We aim to show that $d \mid a \,\%\, b$. By definition of divides, $a = md$ and $b = nd$ for some integers m, n. Then it follows that:

$$a \,\%\, b = a - qb = md - qnd = d(m - qn)$$

Since q, m, n are integers, $m - qn$ is an integer. So $d \mid a \,\%\, b$.

Thus a and b have the same common divisors as b and $a \,\%\, b$. So $\gcd(a, b) = \gcd(b, a \,\%\, b)$.

Since a, b were arbitrary, the claim holds.