Lecture 2C: Modular Arithmetic I

UC Berkeley EECS 70
Summer 2022
Tarang Srivastava

Announcements!

- Read the Weekly Post
- We have caught people for Academic Misconduct on HW1
- **HW 2** and **Vitamin 2** have been released, due **Thu** (grace period Fri)
- No lecture, OH, or Discussions on July 4th

Hopefully Review (Divides)

Def: We say $b|a$ if there exists some integer k such that $a = bk$

Hopefully Review (GCD)

Def: The greatest common divisor (GCD) of integers a and b is the greatest integer d such that $d|a$ and $d|b$

Examples:

gcd(4, 2) =

gcd(12, 16) =

gcd(51, 17) =

gcd(15, 16) =

gcd(7, 96) =

Hopefully Review (Division Algorithm)

Thm: For any two integers a, b. There are unique integers q, r with $0 \leq r \leq b$ such that $a = qb + r$

Hopefully Review (Fundamental Theorem of Arithmetic)

Thm: Every integer ≥ 2 can be **uniquely** expressed as a product of primes.

Mod as an *Operation*

You can think of mod as just an operation (i.e. what you're used to in 61A)

$x \pmod{y}$

Example:

Euclid's (GCD) Algorithm

Thm: Let $x \geq y \geq 0$. Then, $\gcd(x, y) = \gcd(y, x \pmod{y})$

Consider example $x = 10$, $y = 32$

Mod as an *Operation* (cont.)

You can think of mod as just an operation (i.e. what you're used to in 61A)

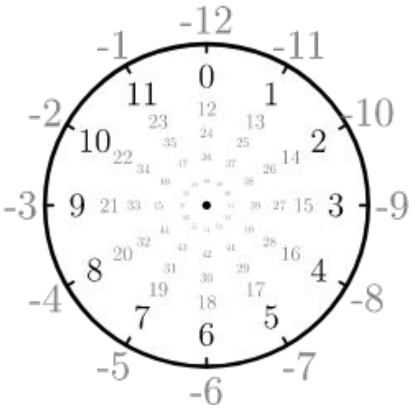
$x \pmod{y}$

Example:

Mod as a *Clock*

You can think of adding in mod as just going around a clock.

We will say all the numbers at the same step of the clock are part of the same **equivalence class**. (ex: ..., -11, 1, 13, 25, 37, ...)



Mod as *Space*

You can consider doing ALL your arithmetic in a given mod *space*.

Let's come up with some rules:

Inverses (Modular Division)

We can redefine division in regular math, to just being multiplying by inverse.
The inverse of a is such a number a^{-1} such that $aa^{-1} = 1$
In (mod m) the inverse of a only exists if a and m are **coprime** (i.e. $\gcd(a, m) = 1$).

Sometimes we say **relatively prime** same thing as coprime.

Let's Bridge Algebraic Form with Modular Form

$a \equiv b \pmod{m}$ iff there exists some integer q such that $a = mq + b$

(GCD Algorithm): Let $x \geq y \geq 0$. Then, $\gcd(x, y) = \gcd(y, x \pmod{y})$

Extended Euclid's Algorithm: How to find inverses

Find the **inverse of x in (mod y)** by finding a, b such that $1 = ax + by$
Example 2: $x = 7$, $y = 32$

Repeated Squaring

How to find $x^y \pmod{m}$ for large exponents.
Example: $4^{42} \pmod{7}$