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 $a = bk$

$b, a \in \mathbb{Z}$

$\frac{a}{b} = k \in \mathbb{Z}$

$b | 0$

$0 = b \cdot 0$

<u>Example</u>: 17, 51

$17 | 51$?

$k = 3$

$\underset{a}{51} = \underset{b}{17} \cdot \underset{k}{3}$

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:

$n = \max(a,b)$

$O(n)$

for i in range(n):

$i \mid a$?

$i \mid b$?

gcd(4, 2) = 2 $\quad 2|2$ ✓ $\quad 2|4$

gcd(12, 16) = 4 $\quad 4|12 \quad 4|16$

gcd(51, 17) = 17 $\mapsto$ since 17 is prime, gcd will be 17 or 1

gcd(15, 16) = 1 $\mapsto$ share no divisors, 15 and 16 are coprime

gcd(7, 96) = 1 $\mapsto$ since 7 is prime, gcd will be 7 or 1

Hopefully Review (Division Algorithm)

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

4th Grade stuff

$a \div b = q + r$

quotient

remainder

$17 \div 5 = 3$ remainder 2

a b q r

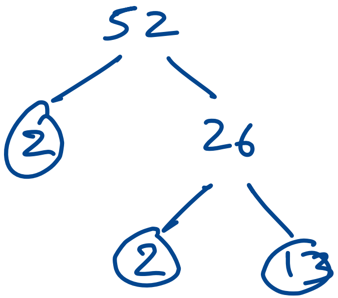
$a \mid b$ iff $r = 0$ in the division algorithm

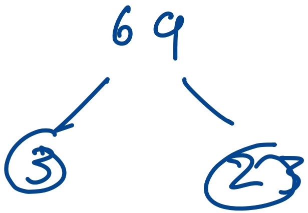
Hopefully Review (Fundamental Theorem of Arithmetic)

(prime factorization)

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

We proved this using induction and well ordering principle Lecture 1C





$52 = 2 \cdot 2 \cdot 13$

this set of primes is unique

$69 = 3 \cdot 23$

Mod as an *Operation*

Python

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

"%"

$x \pmod{y}$

Example:

13 mod 5 = 3

17 mod 2 = 1

17 mod 10 = 7

Euclid's (GCD) Algorithm

Fact:

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

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

$$\gcd(10, 32) = \gcd(32, 10 \pmod{32})$$
$$= \gcd(32, 10)$$
$$= \gcd(10, 32 \bmod 10) = \gcd(10, 2)$$
$$= \gcd(2, 10 \bmod 2) = \gcd(2, 0) = 2 = d$$

$$\gcd(d, 0)$$

$O(\log n)$ $\approx$

Mod as an *Operation* (cont.)

Math 113
114

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

$x \pmod{y}$

Example:

mod m

$m > 0$

$13 \bmod 5 = 3$

$17 \bmod 2 = 1$

$17 \bmod 10 = 7$

equivalence

$\{0, 1, \ldots, m-1\}$

$-17 \bmod \underline{10} \equiv -7 \equiv \boxed{3} \equiv 13$

both | 0

$0, \ldots, 9$

$-17 \xrightarrow{+10} -7 \xrightarrow{+10} 3 \xrightarrow{+10} 13$

$42 \div 5$

$(\bmod 10)\quad -17 = \cancel{10 \cdot (-2)}^{\,0} + 3$

$3 = 3$

Mod as a Clock

(mod 12)

(residue) equivalence class

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, ...)

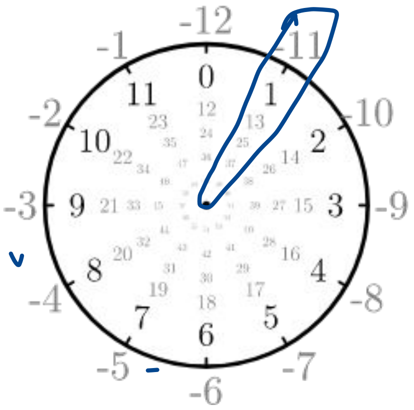
$1 + 0 = 1$

$1 + 12 = 13$

$1 + 12 + 12 = 25$

$1 \equiv 13 \equiv 25 \equiv \dots \pmod{12}$

$1 \equiv -11 \equiv -23 \equiv -35 \pmod{12}$



How many equivalence class?

12

Mod as *Space*

Math 110

Math 113

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

addition ✓

Subtraction ✓

multiplication ✓

division ✓ next slide

Let's come up with some rules:

Addition

$3 + 8 \equiv 11 \equiv 1 \pmod 5$

$3 + 3 \equiv 6 \equiv 1$

$3 + (-2) \equiv 1$

Sub:

$3 - 2 \equiv$

$3 + (-2) \equiv$

$3 + 3 \equiv 1 \pmod 5$

Mul:

$2 \cdot 7 \equiv 14 \equiv 4 \pmod 5$

$2 \cdot 2 \equiv 4 \pmod 5$

Thm: if $a \equiv c \pmod m$, $b \equiv d \pmod m$

$a + b \equiv c + d \pmod m$

$a \cdot b \equiv c \cdot d \pmod m$

CRT

just a symbol

Inverses (Modular Division)

$5 \div 2 = 5 \cdot \frac{1}{2}$

2's inverse is $\frac{1}{2}$

$2 \cdot \frac{1}{2} = 1$

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. $\gcd(a, m) = 1$).

5th Grade

$5 \div \frac{2}{3}$

$5 \cdot \frac{3}{2}$

$\frac{2}{3} \cdot \frac{3}{2} = 1$

$5^{-1} \equiv ? \pmod{17}$

$35 = 17 \cdot 2 + 1$

$5 \cdot 5^{-1} \equiv 1 \pmod{17}$

$5 \cdot 7 \equiv 35 \equiv 1 \pmod{17}$

Example Solving an Equation

Algebra!

$5x + 3 \equiv 7 \pmod{17}$

$5x \cancel{+3} \cancel{-3} \equiv 7 - 3$

$\cancel{5^{-1}} \cancel{5} x \equiv 4 \cdot 5^{-1} \pmod{17}$

$x \equiv 4 \cdot 7 \equiv 28 \equiv 11 \pmod{17}$

$5(11) + 3 = 58 \equiv 7 \pmod{17}$ ✓

prove that the inverse is unique

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 $a = mq + b$ remainder

$a = mq + b \pmod{m}$

$a \equiv 0 \cdot q + b$

$a \equiv b \pmod{m}$

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

Proof. Suppose d is an arbitrary divisor of both x and y ($d \mid x$ and $d \mid y$).

By the division algorithm, we can write $x = qy + r$.

Notice, $x \equiv r \pmod{y}$. Since, $d \mid y$ we know $d \mid qy$.

Then from lecture 1B, we know $d \mid x - qy$. $x - qy = r$

So, $d \mid r$. Thus, x, y and $x \pmod{y}$ share the same divisors since d was arbitrary. Namely they have the same GCD.

Also show that divisors of y and r are divisors of x and y. $\square$

Extended Euclid's Algorithm: How to find inverses

$\gcd(x,y) = 1$

$\gcd(x,y) = ax + by$

$1 = ax + by$

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

Example 2: $x = 7$, $y = 32$

$7^{-1} \pmod{32}$

Solving for a, b gives you the inverses?

Alt. method from in the notes: Goal find a, b

1. $7(1) + 32(0) = 7$
2. $7(0) + 32(1) = 32$
3. $7(5) + 32(0) = 35$
4. $7(5) + 32(-1) = 3$
5. $7(55) + 32(-11) = 33$

$\times 5$, $\times 11$, $-$, $-$

$\underset{x\ \ a}{7(55)} + \underset{y\ \ b}{32(-12)} = \underset{\gcd(x,y)}{1}$

$7^{-1} \pmod{32}$

$55 \equiv 23 \pmod{32}$

$7^{-1} \equiv 23$

$7 \cdot 23 \equiv 161 \equiv 1 \pmod{32}$

$1 = ax + by \pmod{y}$

$1 \equiv ax + \cancel{b}(0)$

inverse of x

$1 = ax + by \pmod{x}$

$1 \equiv by$

$y^{-1} \equiv b \pmod{x}$

$32^{-1} \pmod{7}$

$4^{-1} \pmod{7}$

$-12 \pmod{7}$

$4 \cdot 2 \equiv 8 \equiv 1 \pmod{7}$

Repeated Squaring

$xa \equiv x'a \pmod{n}$

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

$\pmod{7}$

$4^0 = 1$

$4^1 = 4$

$4^2 = (4^1)^2 = 4^2 = 16 = 2$

$(4^2)^2 = 4^4 = 2^2 = 4$

$(4)^8 = 16 = 2$

$(4)^{16} = 4$

$(4)^{32} = 2$

$4^{42} \equiv 4^{32} \cdot 4^8 \cdot 4^2$

$\equiv 2 \cdot 2 \cdot 2$

$\equiv 8 \pmod{7}$

$\equiv 1$