Lecture 19: Divisibility and Modular Arithmetic

Jingjin Yu |Computer Science @ Rutgers

RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

November 17, 2020

Algorithmic Robotics & Control Lab

Outline

- Lecture 18 review
- Divisibility
  - Definition
  - Basic properties
  - Division algorithm
- Modular arithmetic
  - Useful properties
- Arithmetic modulo

- A repeating note: **make sure you read the textbook**

L18: Relation: Operations & Representations

- Relations are sets – so we can do **union**, **intersection**, **difference**, and so on, over them.
- Given sets A, B, C and relations $R \subset A \times B$ and $S \subset B \times C$, the **composition** $S \circ R$ is

$$S \circ R = \{(a, c) \mid (a, b) \in R \; and \; (b, c) \in S\}$$

- Relations can be represented using matrices and directed graphs (digraphs)

Number Theory

- **Def^n**: **Number theory** is the part of mathematics devoted to the study of integers.

$4 = 2+2$ $\quad 5+7=12$

$6 = 3+3$ $\quad$ "$1+1=2$"

$8 = 3+5$

- **Ex**: Goldbach conjecture
- **Ex**: Twin-prime conjecture
- **Ex**: There is an infinite number of prime numbers $p, p+2$

Proof via contradiction suppose there are n $p, p+2$ prime # $p_1, \dots, p_n$

let $p = p_1 \cdot p_2 \cdots p_n + 1$, p is a prime #, $p \neq p_i$ $1 \leq i \leq n$

Divisibility

- **Def^n: Divisibility**. Let a and b be integers. Then, a **divides** b if $b = ac$ for some integer c. Otherwise, a does not divide b.
  - Notation
    - a divides b: $a \mid b$
    - a does not divide b: $a \nmid b$
      - In this case, $b = aq + r$ for some integers q (**quotient**) and $0 < r < b$ (**remainder**)

- **Ex**: $a = 4, b = 12$. $a \mid b$? ✓ $12 = 4 \cdot 3$
- **Ex**: $a = 3, b = 10$. $a \mid b$? ✗ $10 = 3 \cdot 3 + 1$

Divisibility: More Examples

- **Ex:** $a = 3, b = 111111.$ $a \mid b$?

$1+1+1+1+1+1=6$

$3 \mid 6 \Rightarrow a \mid b$

- **Ex:** n and d are positive integers. How many positive integers not exceeding n are divisible by d ?

$n=7,\ d=3$, $1\ 2\ 3\ 4\ 5\ 6\ 7$ 2

$n=14,\ d=3$ $3, 6, 9, 12$ 4 $\left\lfloor \frac{n}{d} \right\rfloor$

Divisibility: Basic Properties

- **Theorem 1.** a, b, and c are integers and $a \neq 0$. Then:
  - (i) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
  - (ii) If $a \mid b$, then $a \mid bc$ for all integers c.
  - (iii) If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: (i) $b = a \cdot p$, $c = a \cdot q \Rightarrow b + c = a(p+q)$

$a \mid b+c$

(ii) $b = a \cdot p \Rightarrow bc = a \cdot p \cdot c \Rightarrow a \mid (bc)$

(iii) $b = a \cdot p$, $c = b \cdot r \Rightarrow c = a \cdot p \cdot r \Rightarrow a \mid c$

Divisibility: "Division Algorithm"

- **Theorem 2.** a and $d > 0$ are integers. Then there are **unique** integers q and r with $0 \leq r < d$ s.t. $a = dq + r$.

Proof. ① uniqueness of q via contradiction.

suppose q is not unique, $a = dq_1 + r_1 = dq_2 + r_2$, s.t. $q_1 \neq q_2$

$d(q_1 - q_2) = r_2 - r_1 \Rightarrow |d(q_1 - q_2)| = |r_1 - r_2| \Rightarrow$ contradiction

$\geq d$ $\quad$ $< d$

② $a = dq_1 + r_1 = dq_2 + r_2 \Rightarrow r_1 = r_2$

"Division Algorithm" Examples

- **Ex:** $a = 47, d = 8.$

$47 = 8 \cdot 5 + 7$ $\quad q = 5, r = 7$

- **Ex:** $a = -14, d = 5.$

$-14 = 5 \cdot (-3) + 1$ $\quad q = -3, r = 1$

Modular Arithmetic

- Notation: $a \bmod m$ is the remainder of a divided by m.
- **Def^n**: Let a and b be integers and m a positive integer. We say a is **congruent** to b modulo m if $m \mid (a - b)$.
  - Notations:
    - $a \equiv b \pmod{m}$ if and only if $m \mid (a - b)$
    - $a \not\equiv b \pmod{m}$ if and only if $m \nmid (a - b)$
- **Theorem 3.** a, b, and $m > 0$ are integers. Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$
- **Ex**: $a = 17, b = 5, m = 6$. $a \equiv b \pmod{m}$?

  $a \bmod m = 17 \bmod 6 = 5$, $b \bmod m = 5$
- **Ex**: $a = 24, b = 516, m = 6$. $a \equiv b \pmod{m}$?

  $24 \bmod 6 = 0$, $516 \bmod 6 = 0$

Proof of Theorem 3

- **Theorem 3.** a, b, and $m > 0$ are integers. Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$

Proof. "only if": $a \equiv b \pmod m \rightarrow a \bmod m \equiv b \bmod m$

$a = m \cdot q_1 + r_1 \cdot b = m \cdot q_2 + r_2$, WLOG assume $r_1 \geq r_2$

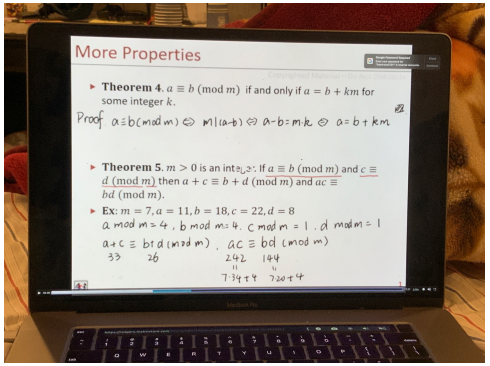
$a - b = m(q_1 - q_2) + (r_1 - r_2) \Leftrightarrow r_1 - r_2 = 0$

"if", $a \bmod m = b \bmod m \rightarrow a \equiv b \pmod m$

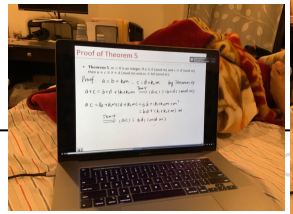
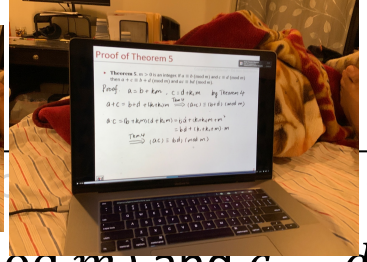
More Properties

- **Theorem 4.** $a \equiv b \pmod{m}$ if and only if $a = b + km$ for some integer k.

- **Theorem 5.** $m > 0$ is an integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.
- **Ex:** $m = 7, a = 11, b = 18, c = 22, d = 8$



Proof of Theorem 5

- **Theorem 5.** $m > 0$ is an integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$.

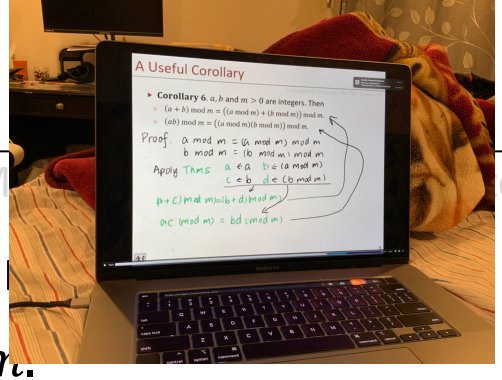
Proof. $a = b + k_1 m$, $c = d + k_2 m$ by Theorem

$a + c = b + d + (k_1 + k_2)m \overset{\text{Thm}}{\Rightarrow} (a+c) \equiv (b+d) \pmod{m}$

$a \cdot c = (b + k_1 m)(d + k_2 m) = bd + (k_1 + k_2)m + m^2$

Thm $\Rightarrow (ac) = (bd) \pmod{m}$

A Useful Corollary



- **Corollary 6.** a, b and $m > 0$ are integers. Then
  - $(a + b) \bmod m = \big((a \bmod m) + (b \bmod m)\big) \bmod m.$
  - $(ab) \bmod m = \big((a \bmod m)(b \bmod m)\big) \bmod m.$

Proof. $a \bmod m = (a \bmod m) \bmod m$

$b \bmod m = (b \bmod m) \bmod m$

Apply Thms $a \leftarrow a$ $b \leftarrow (a \bmod m)$

$c \leftarrow b$ $d \leftarrow (b \bmod m)$

A Useful Corollary: Application

- **Ex:** $a = 13241, b = 479, m = 3.$
  - $(a + b) \bmod m = ?$
  - $(ab) \bmod m = ?$

$a = 13241 = 13200 + 41$ $a \bmod 3 = 41 \bmod 32$

$b \bmod 3 = 2$

$(a+b) \bmod m = (2+2) \bmod m = 1$

$(ab) \bmod 3 = (2 \cdot 2) \bmod 3 = 1$

$a \bmod m$

$b \bmod m$

$a^2 + ba^2 + b^3$

Arithmetic Modulo

- **Def^n**: $\mathbb{Z}_m = \{0, \ldots, m-1\}$.
- **Def^n**: For $a, b \in \mathbb{Z}_m$, $a +_m b = (a + b) \bmod m$.
- **Def^n**: For $a, b \in \mathbb{Z}_m$, $a \cdot_m b = (ab) \bmod m$.

- **Ex**: $7 +_{11} 9$ $= (7+9) \bmod 11 = 5$

- **Ex**: $7 \cdot_{11} 9$ $= (7 \cdot 9) \bmod 11 = 8$