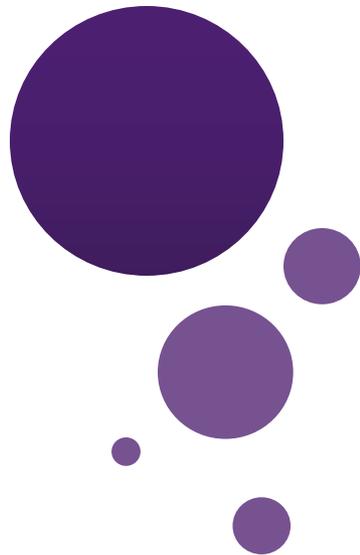




UNIVERSITY
AT ALBANY

State University of New York



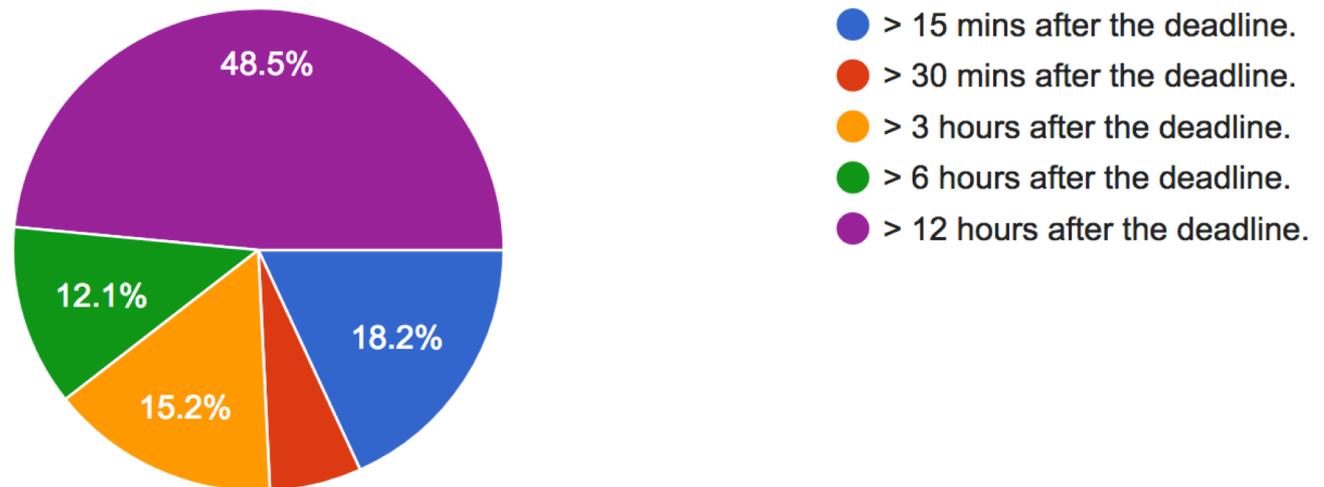
Lecture 16: Modular Arithmetic

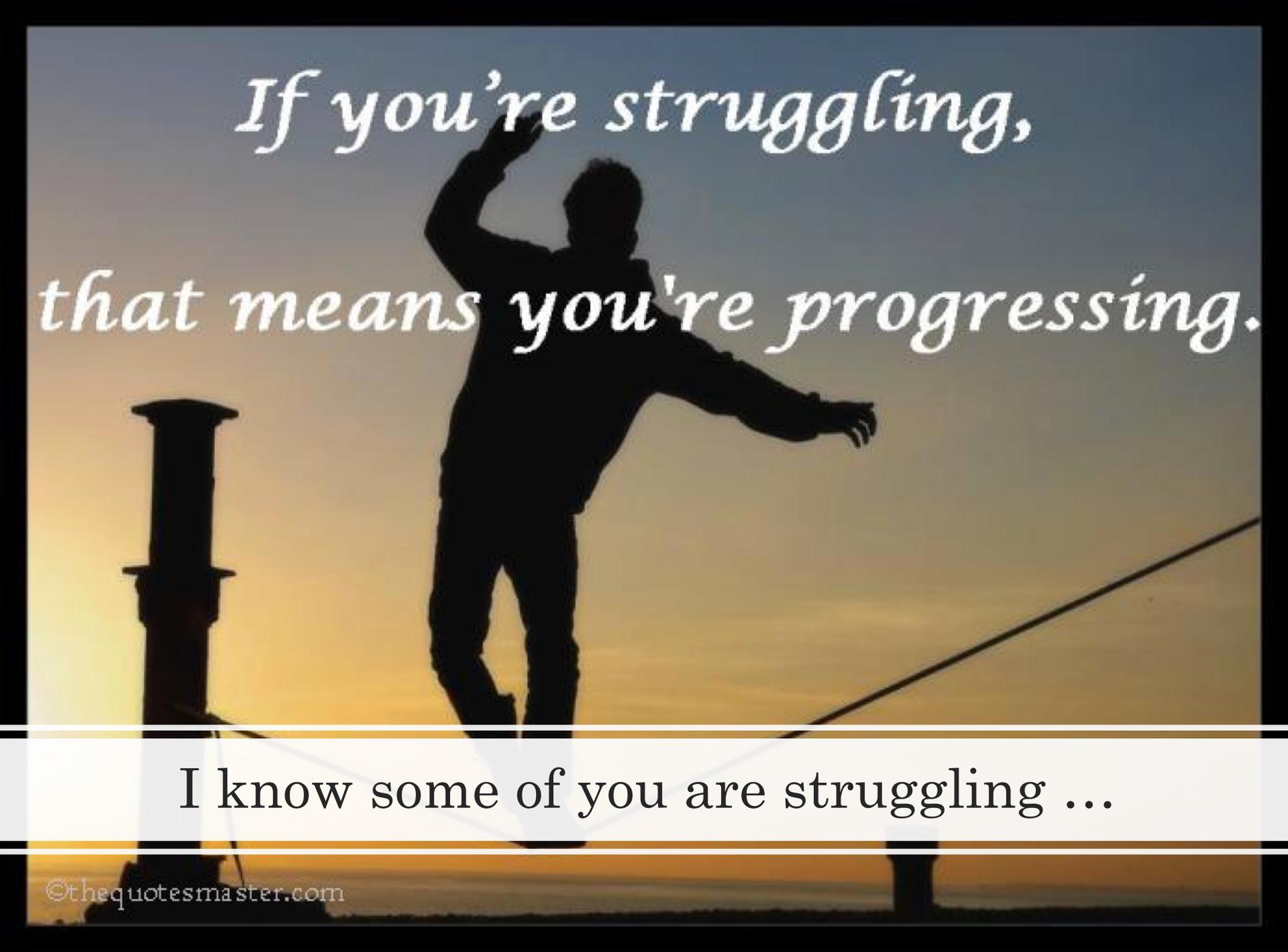
Dr. Chengjiang Long
Computer Vision Researcher at Kitware Inc.
Adjunct Professor at SUNY at Albany.
Email: clong2@albany.edu

About the late submission

2. [Late submission policy] What is the best criteria you would like to rate as "late submission"?

33 responses



A silhouette of a person walking a tightrope against a sunset background. The person is in the center, balancing on a thin wire that stretches from the bottom left towards the right. To the left of the person is a tall, dark, cylindrical structure, possibly a support for the tightrope. The background is a gradient of colors from dark blue at the top to bright yellow and orange at the bottom, representing a sunset or sunrise. The overall mood is one of challenge and perseverance.

If you're struggling,

that means you're progressing.

I know some of you are struggling ...

I am here to **help** you,



Outline

- Introduction to Modular Arithmetic
- Properties of Mod Function
- Arithmetic Modulo m
- Applications

Outline

- **Introduction to Modular Arithmetic**
- Properties of Mod Function
- Arithmetic Modulo m
- Applications

Division Algorithm – Theorem of Existence

- *Recall:*
- According to the Division Algorithm
 - $32 \bmod 7 = 4$ because $32 = 7 \cdot 4 + 4$.
 - $-10 \bmod 7 = 4$ because $-10 = 7 \cdot (-2) + 4$.
- What is common between 32 and -10?

The remainder.

Modulus

- The concept of positive remainder allows mapping of any set of integers to its subset defined by any positive integer m (modulus)
 - $f: S \subseteq \mathbf{Z} \rightarrow \mathbf{Z}_m = \{0, \dots, m-1\} \subseteq S$.

Modular Arithmetic

- Let $(a, b) \in \mathbb{Z}^2$, $m \in \mathbb{Z}^+$ then a is **a congruent to b modulo m** if m divides $a - b$.
Notation: $a \equiv b \pmod{m}$.
- Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.
- The equivalent definitions of congruency:

Let m be a positive integer. The integers a and b are congruent modulo m if and only if

$$\exists k \in \mathbb{Z}; a = b + km$$

$(\text{mod } m)$ and $\text{mod } m$

- $a \text{ mod } m = b$ denotes function that results in b .
- $a \equiv b \pmod{m}$ denotes statement (“equation”) that could be true or false.

Example

- $17 \equiv 5 \pmod{6}$?

$$6 \mid (17 - 5) = 12 \Rightarrow 17 \equiv 5 \pmod{6}$$

- $24 \equiv 14 \pmod{6}$?

6 does not divide 10

$\Rightarrow 24$ is not congruent to $14 \pmod{6}$

Algebraic Operations and Congruencies

- If $a \equiv b \pmod{m}$ holds then $c \cdot a \equiv c \cdot b \pmod{m}$, where c is any integer, holds.
- If $a \equiv b \pmod{m}$ holds then $c + a \equiv c + b \pmod{m}$, where c is any integer, holds.
- Dividing a congruence by an integer does not always produce a valid congruence.
- **Example:**
- The congruence $14 \equiv 8 \pmod{6}$ holds.
- But dividing both sides by 2 does not produce a valid congruence since $14/2 = 7$ and $8/2 = 4$, but $7 \not\equiv 4 \pmod{6}$.

Example

- $17 \equiv 5 \pmod{6}$
 $6 \mid (17 - 5) = 12 \Rightarrow 17 \equiv 5 \pmod{6}$
- $8 \equiv 14 \pmod{6}$
 $6 \mid (8 - 14) = -6 \Rightarrow 8 \equiv 14 \pmod{6}$

$$17 + 8 \equiv 5 + 14 \pmod{6} ? \Rightarrow 25 \equiv 19 \pmod{6} ?$$

$$17 \times 8 \equiv 5 \times 14 \pmod{6} ? \Rightarrow 136 \equiv 70 \pmod{6} ?$$

Congruencies of Sums and Products

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
 $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$

Example:

- Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$,
 $18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$
- $77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}$

Outline

- Introduction to Modular Arithmetic
- **Properties of Mod Function**
- Arithmetic Modulo m
- Applications

Properties of **mod** Function

- Let m be a positive integer and let a and b be integers.
 - Then
 - $(a + b) \text{ (mod } m) = ((a \text{ mod } m) + (b \text{ mod } m)) \text{ mod } m$
- and
- $ab \text{ mod } m = ((a \text{ mod } m) (b \text{ mod } m)) \text{ mod } m.$

Practice

- It is often asked to find remainder of the positive powers of 10 over an integer number:

$10 \bmod 3$, $10^2 \bmod 3$, $10^3 \bmod 3$, etc.

- or

$10 \bmod 7$, $10^2 \bmod 7$, $10^3 \bmod 7$, etc.

Practice

- Use of the properties of the mod function reduce computing:
 - $10^n \bmod m = (10 \bmod m)^n \bmod m$, where $n \in \mathbf{Z}^+$.
- $10 \bmod 3 = 1 \rightarrow 10^n \bmod 3 = (10 \bmod 3)^n \bmod 3 = 1$
(Division Algorithm: $1 = 0 \times 3 + 1$)
- $10 \bmod 7 = 3 \rightarrow 10^n \bmod 7 = (10 \bmod 7)^n \bmod 7 = 3^n \bmod 7$

Computations

- Suppose we need to compute $a^n \bmod m$. It could be solved by sequences of multiplications and divisions. There is the faster approach.
- For example, we need to compute $a^8 \bmod n$. Instead of 7 multiplications and one reduction mod of a big number perform 3 multiplications and 3 mod operations of a smaller numbers:
 - $a^8 \bmod m = ((a^2 \bmod m)^2 \bmod m)^2 \bmod m$.
- The same,
 - $a^{16} \bmod m = (((a^2 \bmod m)^2 \bmod m)^2 \bmod m)^2 \bmod m$.

Outline

- Introduction to Modular Arithmetic
- Properties of Mod Function
- **Arithmetic Modulo m**
- Applications

Arithmetic Modulo m

Definitions: Let \mathbf{Z}_m be the set of nonnegative integers less than m : $\{0, 1, \dots, m-1\}$

- The operation $+_m$ is defined as $a +_m b = (a + b) \mathbf{mod} m$. This is *addition modulo m* .
- The operation \cdot_m is defined as $a \cdot_m b = (a \cdot b) \mathbf{mod} m$. This is *multiplication modulo m* .
- Using these operations is said to be doing *arithmetic modulo m* .

Example

- **Example:** Find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Solution: Using the definitions above:

- $7 +_{11} 9 = (7 + 9) \bmod 11 = 16 \bmod 11 = 5$
- $7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8$

Properties of Arithmetic Modulo m

- The operations $+_m$ and \cdot_m satisfy many of the same properties as ordinary addition and multiplication if operands belong to \mathbf{Z}_m .
 - *Closure*: If a and b belong to \mathbf{Z}_m , then $a +_m b$ and $a \cdot_m b$ belong to \mathbf{Z}_m .
 - *Associativity*: If a , b , and c belong to \mathbf{Z}_m , then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
 - *Commutativity*: If a and b belong to \mathbf{Z}_m , then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.
 - *Identity elements*: The elements 0 and 1 are identity elements for addition and multiplication modulo m , respectively.
 - If a belongs to \mathbf{Z}_m , then $a +_m 0 = a$ and $a \cdot_m 1 = a$.

Properties of Arithmetic Modulo m , cont'd

- *Additive inverses*: If $a \neq 0$ belongs to \mathbf{Z}_m , then $m - a$ is the additive inverse of a modulo m and 0 is its own additive inverse.
 - $a +_m (m - a) = 0$ and $0 +_m 0 = 0$
- *Distributivity*: If a , b , and c belong to \mathbf{Z}_m , then
 - $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and
 $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.
- Multiplicative inverses have not been included since they do not always exist. For example, there is no multiplicative inverse of 2 modulo 6

Practice

- **Problem:** Prove that $A \bmod 3 = D \bmod 3$, where A is a positive integer number, D is a sum of decimal digits of A .
- For example, $6371 \bmod 3 = 17 \bmod 3$.
- **Solution:** Weighted Positional Notation $A = a_n 10^n + \dots + a_1 10^1 + a_0 10^0$ (e.g. $6371 = 6 \times 10^3 + 3 \times 10^2 + 7 \times 10^1 + 1 \times 10^0$).
- $A \bmod 3 = (a_n \times 10^n + \dots + a_1 \times 10^1 + a_0 \times 10^0) \bmod 3$
 $= ((a_n \times 10^n) \bmod 3 + \dots + (a_1 \times 10^1) \bmod 3 + (a_0 \times 10^0) \bmod 3) \bmod 3$

Each term $(a_i \times 10^i) \bmod 3 = ((a_i \bmod 3) \times (10^i \bmod 3)) \bmod 3 = ((a_i \bmod 3) \times 1) \bmod 3$ (see Practice example above), i.e.

- $A \bmod 3 = ((a_n \bmod 3) \bmod 3 + \dots + (a_1 \bmod 3) \bmod 3 + (a_0 \bmod 3) \bmod 3) \bmod 3 =$
 $= (a_n \bmod 3 + \dots + a_1 \bmod 3 + a_0 \bmod 3) \bmod 3$
 $= (a_n + \dots + a_1 + a_0) \bmod 3$

Results of Modular Arithmetic

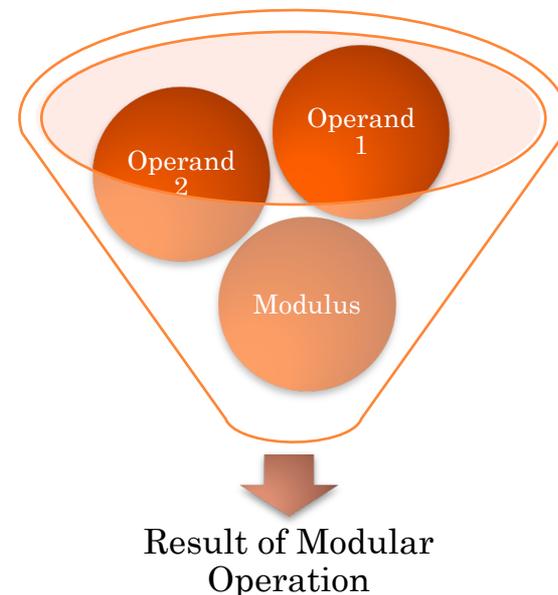
Module arithmetic replaces operations on integer numbers with operations on remainders of the division of the numbers by specified positive integer m .

It is obvious that different integers may result in the same numbers:

$$(16 \times 2) \bmod 7 = 4$$

$$(20 - 30) \bmod 7 = 4$$

How to evaluate such results?



Outline

- Introduction to Modular Arithmetic
- Properties of Mod Function
- Arithmetic Modulo m
- **Applications**

Applications of Congruences: Hash Functions

Assignment of memory location to a student record

$$h(k) = k \bmod m$$

Key: social security #

of available
memory location

Example: $h(064212848) = 064212848 \bmod 111 = 14$
when $m = 111$

Applications of Congruences: Cryptology

a) Encryption:

- Making messages secrets by shifting each letter three letters forward in the alphabet

$$B \rightarrow E \qquad X \rightarrow A$$

- Mathematical expression:

$$f(p) = (p + 3) \bmod 26 \quad 0 \leq p \leq 25$$

Applications of Congruences: Cryptology

- **Example:** What is the secret message produced from the message “Meet you in the park”

Solution:

1. Replace letters with numbers:

meet = 12 4 4 19

you = 24 14 20

in = 8 1 3

the = 19 7 4

park = 15 0 17 10

2. Replace each of these numbers p by $f(p) = (p + 3) \bmod 26$

meet = 15 7 7 22

you = 1 17 23

in = 11 16

the = 22 10 7

park = 18 3 20 13

3. Translate back into letters: “PHHW BRX LQ WKH SDUN”

Applications of Congruences: Cryptology

b) Decryption (Deciphering)

$$f(p) = (p + k) \bmod 26 \text{ (shift cipher)}$$

$$\Rightarrow f^{-1}(p) = (p - k) \bmod 26$$

Caesar's method and shift cipher are very vulnerable and thus have low level of security (reason frequency of occurrence of letters in the message)

\Rightarrow Replace letters with blocks of letters.

Next class

- Topic: Integer Representations
- Pre-class reading: Chap 4.2

