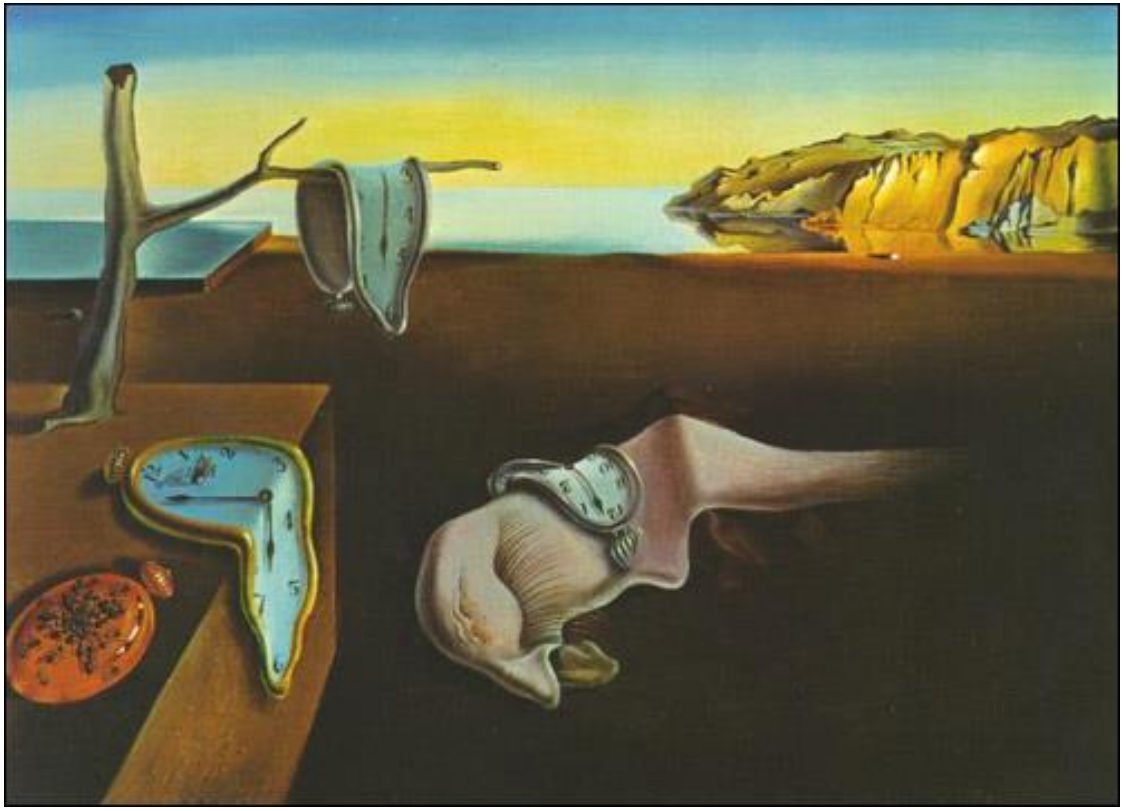
Congruence and Sets



Dali - “The Persistence of Memory”

Discrete Structures (CS 173) Lecture 5

Gul Agha

University of Illinois at Urbana-Champaign

Based on lecture notes by Derek Hoiem

Review of Last Class

- A composite integer k can be **factored** into smaller integers whose product is equal to k
- a **divides** b means that b$= ka$ for some integer k
- Two numbers are **relatively prime** if they have no common prime factors
- $\mathbf{gcd}(a, b)$ is the largest integer that divides both a and b
- $\mathbf{lcm}(a, b)$ is the smallest integer that both a and b divide

Goals of this lecture

- Introduce the concept of *congruence mod k*

$$3 \equiv 15 \pmod{12}$$

- Be able to perform *modulus arithmetic*

- Brief introduction to *sets*

Applications of congruence

- bitwise operations
- error checking
- computing 2D coordinates in images
- encryption
- telling time
- etc.

Congruence mod k

- Two integers are *congruent mod k* if they differ by an integer multiple of k
- Definition: If k is any positive integer, two integers a and b are congruent mod k iff k divides $(a - b)$

$$a \equiv b \bmod k \leftrightarrow \quad k \mid (a - b)$$

Examples of congruent mod k

overhead

Modulus addition proof

Claim: For any integers a, b, c, d, k with $k > 0$, if $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$ then $(a + c) \equiv (b + d) \pmod{k}$

Definition: $a \equiv b \pmod{k} \quad \leftrightarrow \quad k \mid (a - b)$

overhead

Modulus multiplication proof

Claim: For any integers a, b, c, d, k with $k > 0$, if $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$ then $ac \equiv bd \pmod{k}$

Definition: $a \equiv b \pmod{k} \iff k \mid (a - b)$

overhead

Equivalence classes with modulus

The equivalence class of integer x (written $[x]$) is the set of all integers congruent to $x \pmod{k}$

In (mod 7), $[3] = \{\dots, -11, -4, 3, 10, 17, \dots\}$

In (mod 5), $[3] = \{\dots, -7, -2, 3, 8, 13, \dots\}$

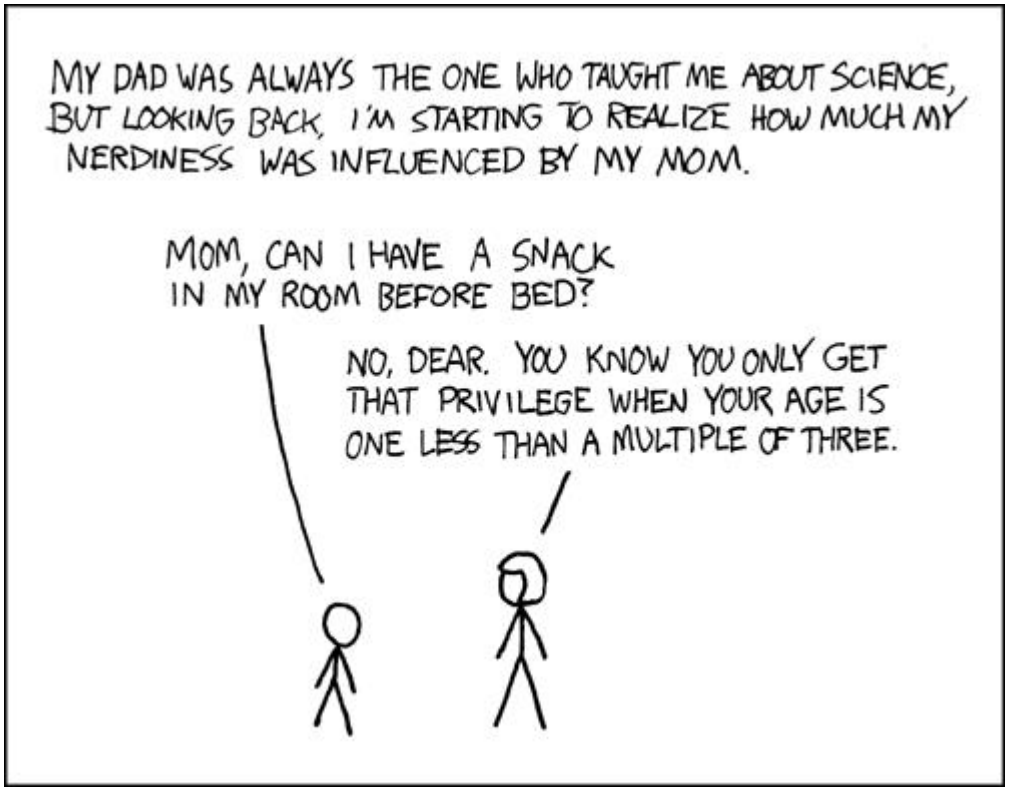
In Z_5, $[3] = [8] = [-2]$

Modulus arithmetic

$[x] + [y] = [x + y]$
$[x] * [y] = [x * y]$

overhead

Short Break



xkcd #183

$$(25^{17}+26)^2 \equiv \_\_\_\_\_ \ (mod\ 3)$$

RSA Key Generation

- Creating the public and private keys for encryption/decryption
  - Choose two prime numbers p and q
  - $n = pq$
  - $k = (p-1)(q-1)$
  - Choose an integer e such that $e \leq k$ and e is relatively prime with k
  - Solve for $de \equiv 1 (\mathrm{mod}\ k)$ (e.g., with extended Euclidean algorithm)

- Using the keys
  - Public key: n, e
  - Private key: d
  - Encryption
    - Turn message into an integer m
    - Coded message $c \equiv m^e (\mathrm{mod}\ n)$
  - Decryption
    - Original message $m \equiv c^d (\mathrm{mod}\ n)$

Another congruence proof

Claim: If n is odd, then $n^2 \equiv 1 \pmod 8$

Definition: $a \equiv b \pmod k \quad \leftrightarrow \quad k \mid (a - b)$

overhead

Sets

Topics: lists, set builders, tuples vs. sets, equivalence, cardinality, subsets and supersets

overhead

Things to remember

- Concept of congruence mod k, it's definition in terms of divide, and equivalence classes
  - Many applications in CS
- The key to modular arithmetic is keeping numbers small
- Concept of sets and set equivalence

Set Application: analysis of purchasing patterns

- How similar are two shopper's purchases? (e.g., intersection / union of purchased items)
- If someone buys *x* and *y*, what might she buy next?

Application: counting

- 1000 people are asked whether they like tea and/or coffee
  - 600 like tea
  - 500 like coffee
  - 200 like neither
  - How many like both?

Thinking about sets

overhead

Constructing sets

- Miscellaneous elements: *extensional definition*
- Constructors: multiples of 3, squared numbers, quadrant, line segment (*intentional definition)*

overhead

The empty set

- ∅ (in latex: \emptyset)
- All sets are supersets of the empty set
- The empty set contains no elements

Subset transitivity proof

Claim: For any sets A, B, C, if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$

Definition: A is a subset of B if every element of A is also an element of B

Set operations

- Intersection, union, difference
- De Morgan's Laws

overhead

Sizes of sets

- For discrete sets: the number of unique elements in the set
- For continuous sets: measures of *cardinality.*

- $|A \cup B| = |A| + |B| - |A \cap B|$

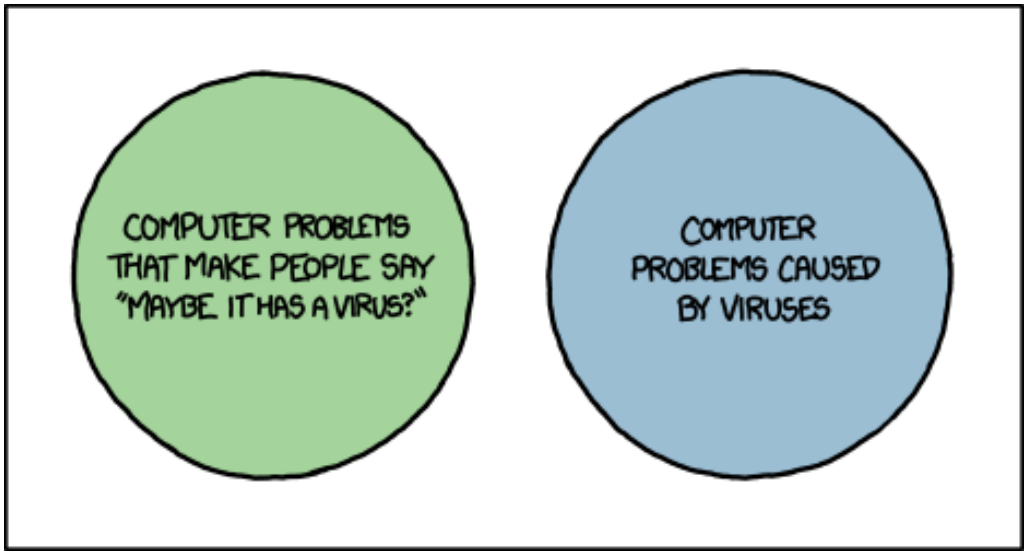
Set size problems

- 1000 people are asked whether they like mint and/or chamomile:
  - 600 like mint
  - 500 like chamomile
  - 200 like neither
  - How many like both?

- How many numbers from 0 to 99 have a “7” in them?

overhead

Short break



xkcd 1180

1. All humanoids eat bananas, except humanoids with unpainted yellow noses (to avoid confusion).
2. There are 1,000 humanoids on Krog, of which 200 naturally have yellow noses.
3. There have been two recent sprees of nose-paintings. 50 originally yellow-nosed humanoids were painted in each spree, and 10 unlucky ones were painted twice.
4. How many banana-eating humanoids are left?

Cartesian products (cross-products)

- Cartesian product $A \times B$ consists of pairs (x, y) for each $x \in A$ and $y \in B$
- Creates tuples that provide all ordered combinations of sets

overhead

Inclusion proof

Claim: Let $A = \{(x, 5 - (x-3)^2) : x \in [1,5]\}$,

$$B = \{(x,y) \in R, x \geq 0, y \geq 0\}.$$

Show $A \subseteq B$.

Definition: A is a subset of B if every element of A is also an element of B

overhead

Contrapositive proof

Claim: For any sets A and B, if $(A - B) \cup (B - A) = A \cup B$, then $A \cap B = \emptyset$.

overhead

Things to remember

- Sets and set constructors
- How to operate on sets: intersection, union, difference, not, Cartesian product
- How to count elements of a set or combination of sets
- Proof strategies for sets

Administrative

- First Examlet on Thursday!
- DRES and auditors: let me know who you are
- There will be a new moodle activity due Friday