CSE 20
DISCRETE MATH

Fall 2017

http://cseweb.ucsd.edu/classes/fa17/cse20-ab/
Today's learning goals

• Define and use the congruence modulo \( m \) equivalence relation
• Apply modular arithmetic to solve problems
  • new proof strategies
  • simplify computations
  • memory indexing (hash functions)
  • cryptography (Diffie-Hellman key exchange)
  • pseudo-random number generation
Equivalence relations

Two formulations

A relation $R$ on set $A$ is an equivalence relation if it is reflexive, symmetric, and transitive.

$$x \; R \; y \; \text{iff } x \text{ and } y \text{ are "similar"}$$

Partition $A$ into equivalence classes, each of which consists of "similar" elements: collection of disjoint, nonempty subsets that have $A$ as their union

$$x, y \text{ both in } A_i \text{ iff } x \text{ and } y \text{ are "similar"}$$
Relation on a set A

A relation $R$ is called **reflexive** iff
\[ \forall a \ ( (a,a) \in R ) \]

**symmetric** iff
\[ \forall a \forall b \ ( (a,b) \in R \rightarrow (b,a) \in R ) \]

**transitive** iff
\[ \forall a \forall b \forall c \ ( [(a,b) \in R \land (b,c) \in R] \rightarrow (a,c) \in R ) \]

Given an equivalence relation $R$ on set $A$, for $a$ in $A$, the **equivalence of class** of $a$ is
\[ [a]_R = \{ s \mid (a,s) \text{ is in } R \} \]
For $a, b$ in $\mathbb{Z}$ and $m$ in $\mathbb{Z}^+$ we say $a$ is congruent to $b$ mod $m$ iff 

$$a \equiv b \pmod{m} \iff a \mod m = b \mod m \iff m \mid (a-b) \iff \exists q (a-b = qm)$$

and in this case, we write

Which of the following is true?

A. $5 \equiv 10 \pmod{3}$
B. $5 \equiv 1 \pmod{3}$
C. $5 \equiv 3 \pmod{3}$
D. $5 \equiv -1 \pmod{3}$
E. None of the above.
Claim: Congruence mod $m$ is an equivalence relation

Proof:

Reflexive?
Symmetric?
Transitive?
*The* example

**Claim:** Congruence mod m is an equivalence relation

**Congruence classes:** \([a]_m = \{s \mid (a,s) \text{ is in } R\} = \{s \mid a \mod m = s \mod m\}

*What partition of the integers is associated with this equivalence relation?*

E.g. \(m=6\)

\([0]_6 = \{ s \mid 0 \equiv s \pmod{6}\}\)

\[\begin{align*}
\{0, 6, 12, 18, 24, \ldots\} & \quad \{3, 9, 15, 21, 27, \ldots\} \\
\{1, 7, 13, 19, 25, \ldots\} & \quad \{4, 10, 16, 22, 28, \ldots\} \\
\{2, 8, 14, 20, 26, \ldots\} & \quad \{5, 11, 17, 23, 29, \ldots\}
\end{align*}\]
Application 1: Proof by cases

Claim: The square of each integer is either divisible by 4 or has remainder 1 upon division by 4.

\[ \forall n \left( n^2 \mod 4 = 1 \lor n^2 \mod 4 = 0 \right) \]

Proof:

Induction? Structural \( \mathbb{Z} \)
Contradiction? 
Exhaustive? infinitely many in \( \mathbb{Z} \)
Application 1: Proof by cases

**Claim:** The square of each integer is either divisible by 4 or has remainder 1 upon division by 4.

**Proof:** Let $n$ be an integer and consider its remainder upon division by 4.

Alternate strategy: Two cases $\begin{cases} n \text{ even} & \vdots \ n^2 \ ? \\ n \text{ odd} & \vdots \ n^2 \ ? \end{cases}$

**Four cases:** remainder is 0, 1, 2, or 3.

- **Case 0** $n \mod 4 = 0$
  - By def, there's $n = 4q + 0 = 4q$
  - Squaring: $n^2 = (4q)^2 = 4(4q^2)$ so $n^2 \mod 4 = 0$
Arithmetic modulo $m$

\[ (a+b) \mod m = ( (a \mod m) + (b \mod m) ) \mod m \]

\[ ab \mod m = ((a \mod m) (b \mod m)) \mod m \]

\[ n^2 \mod m = ((n \mod m)(n \mod m)) \mod m \]

prev ex: if \( n \mod m = 0 \)
Arithmetic modulo $m$

Rosen p. 242-243

$$(a+b) \mod m = ((a \mod m) + (b \mod m)) \mod m$$

$$ab \mod m = ((a \mod m)(b \mod m)) \mod m$$

**Modular addition and multiplication are well-defined on equivalence classes!**

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Application 2: Last digit

What's the last digit of $2017^{2017}$?
A. 1
B. 3
C. 9
D. 7
E. Can't tell without a calculator.

Last digit of decimal representation of $n$ is $n \mod 10$
We saw that, for all integers $a,b$ and all positive integers $m$,

$$(a+b) \mod m = ( (a \mod m) + (b \mod m) ) \mod m$$

$$ab \mod m = ((a \mod m) (b \mod m)) \mod m$$

Which of the following is also true?

A. $(a-b) \mod m = ( (a \mod m) - (b \mod m) ) \mod m$

B. $(a/b) \mod m = ( (a \mod m) / (b \mod m) ) \mod m$

C. $a^b \mod m = ( (a \mod m) (b \mod m) ) \mod m$

D. More than one of the above.

E. None of the above.
Modular operations

\[(a-b) \mod m = ( (a \mod m) - (b \mod m) ) \mod m\]

\[(-b) \mod m = (m-b) \mod m\]

\[(a/b) \mod m = ( (a \mod m) / (b \mod m) ) \mod m\]

Counterexample: \( a = 16, b = 8, m = 10\)

\[a^b \mod m = ( (a \mod m)^{(b \mod m)} ) \mod m\]

Counterexample: \( a = 2, b = 10, m = 10\)
Application 3: hashing

Rosen Sec 4.5 p. 287

Data records

Memory
Application 3: hashing

Data records
Encoded by ints, may not be consecutive

Well-defined? Onto? One-to-one?

Rosen Sec 4.5 p. 287

Memory

h(k) = k mod m

0
1
2
...

m-1

m slots
Application 3: hashing

Data records
Encoded by ints, may not be consecutive

$h(k) = k \mod m$

A collision occurs when more than one record is assigned to the same memory location

Rosen Sec 4.5 p. 287
Application 4: key exchange

Rosen Sec 4.6, p. 302
Application 4: key exchange

Sender starts with
- Public key, public prime: $a, p$
- Private key: $k_1$

Receiver starts with
- Public key, public prime: $a, p$
- Own private key: $k_2$

Idea: exchange information so that sender and receiver will have shared **key** (number) but no-one looking at messages will be able to decode them without knowing either or both of $k_1, k_2$
Basic assumptions in cryptography

1. **Factoring is hard**: given a 400 digit number that is a product of two 200 digit primes, can't efficiently find these primes.

2. **Discrete logarithm is hard**: given a 300 digit prime and the result of exponentiation mod this prime, find the logarithm, i.e. find $k$ when given $a^k \mod p$. 
Application 4: key exchange

Fix \( a, p \), sender's private key \( k_1 \), receiver's private key \( k_2 \)

**Idea:** exchange information so that sender and receiver will have **shared key (number)** but no-one looking at messages will be able to decode them without knowing either or both of \( k_1, k_2 \)

1. Sender sends \( a^{k_1} \mod p \) to receiver.
2. Receiver sends \( a^{k_2} \mod p \) to sender.

Shared key is \( a^{(k_1)(k_2)} \mod p \).
Diffie & Hellman
Application 5: Pseudorandom generators

\[ x_{n+1} = (ax_n + c) \mod m \]

Parameters:
- modulus \( m \)
- multiplier \( a \) \((2 \leq a < m)\)
- increment \( c \) \((0 \leq c < m)\)
- seed \( x_0 \) \((0 \leq x_0 < m)\)

What's the maximum number of terms before the sequence starts to repeat?

A. \( m \)
B. \( a \)
C. \( c \)
D. \( x_0 \)
E. Depends on the parameters; maybe never!
Application 5: Pseudorandom generators

\[ x_{n+1} = (ax_n + c) \mod m \]

Parameters:
- modulus \( m \)
- multiplier \( a \) \((2 \leq a < m)\)
- increment \( c \) \((0 \leq c < m)\)
- seed \( x_0 \) \((0 \leq x_0 < m)\)

\( m = 8, a = 5, c = 1, x_0 = 1 \)
1, 6, 7, 4, 5, 2, 3, 0, 1, 6, 7, 4, 5, 2, 3, …

\( m = 8, a = 5, c = 4, x_0 = 1 \)
1, 1, 1, 1, 1, …
Next up: review for final exam

Final exam is Saturday December 16
11:30am-2:30pm