CSE 20
DISCRETE MATH

Winter 2017

http://cseweb.ucsd.edu/classes/wi17/cse20-ab/

Today's learning goals

- Define and use the congruence modulo m equivalence relation
- Perform computations using modular arithmetic
- Explain how primality and modular arithmetic are related

The final exam is **Saturday March 18 8am-11am**.

Lecture A will take the exam in GH 242

Lecture B will take the exam in SOLIS 107

Practice questions for the final exam are now available on Piazza.

Solutions will not be posted for these questions. However, the TAs will discuss them in the review session **Thursday 03/16/2017 8:00p-10:50p PETER 108.**

Equivalence relations

Rosen p. 608

Two formulations

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

x R y iff x and y are "similar"

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

x,y both in A_i iff x and y are "similar"

The example

Rosen p. 240

For a,b in **Z** and m in $\mathbf{Z}^+$ we say **a is congruent to b mod m**
iff

$$m \mid (a-b)$$

i.e.

$$\exists q(a - b = qm)$$

and in this case, we write

$$a \equiv b \pmod{m}$$

Claim: Congruence mod m is an equivalence relation

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

mod is mod?

Theorem 3 p. 241

Let a and b be integers and m be a positive integer.

Then $a \equiv b \pmod{m}$ iff a mod m = b mod m

Proof:

Arithmetic modulo *m*

Rosen p. 242-243

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

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

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Arithmetic modulo *m*

Rosen p. 242-243

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

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

What is (1068+785) mod 3?

A. 0
B. 1
C. 2
D. I need a calculator
E. I don't have enough time!

Division?

Find an example of two integers a,b that are **not** multiples of 6 but where

$$ab \textbf{ mod } 6 = 0$$

Zero divisors

Primes

Rosen p. 257

An integer p greater than 1 is **prime** if its only positive factors are 1 and p.

Primes

Rosen p. 257

An integer p greater than 1 is **prime** if its only positive factors are 1 and p.

Fact: There are no zero divisors mod p.

Why? Suppose ab mod p = 0. Then ab = kp so p | (ab).

Is it possible to have (ab) be a multiple of p at the same time as a and b both **not** multiples of p…

Excursion: gcd

Rosen p. 265

For two integers a,b (not both 0), the largest integer d such that d | a and d | b is called the **greatest common divisor** of a and b, **gcd(a,b)**.

A. gcd(a,b) < a
B. gcd(a,b) could be negative.
C. gcd (a,b) can never equal b.
D. gcd (a,b) can equal 1.
E. None of the above.

Excursion: gcd

Rosen p. 265

For two integers a,b (not both 0), the largest integer d such that d | a and d | b is called the **greatest common divisor** of a and b, **gcd(a,b)**.

If p is prime and a is an integer, then

A. gcd(a,p) depends on a
B. gcd(a,p) equals 1
C. gcd (a,p) equals p
D. gcd (a,p) equals ap
E. None of the above.

Calculating gcd(a,b)

Rosen p. 267

Euclidean Algorithm

Remember HW 1?

procedure $gcd(a, b :$ pos ints$)$

$x := a$

$y := b$

while $y \neq 0$

$r := x$ **mod** y

$x := y$

$y := r$

return x

Euclidean algorithm

Rosen p. 267

1. Algorithm for calculating GCD
2. Theoretical consequence: Bézout's Theorem

If a,b are positive ints then there are ints s,t such that

$$\gcd(a,b) = sa + tb$$

Back to primes

Is it possible to have (ab) be a multiple of p at the same time as a and b both **not** multiples of p?

For simplicity, assume $0 \leq a,b \leq p$

Back to primes

Is it possible to have (ab) be a multiple of p at the same time as a and b both **not** multiples of p?

For simplicity, assume $0 \leq a,b \leq p$

Know $ab = kp$ and $\gcd(a,p) = 1$

By Bézout's Theorem, there are ints s,t with

$$1 = \gcd(a,p) = sa + tp$$

Back to primes

Is it possible to have (ab) be a multiple of p at the same time as a and b both **not** multiples of p?

For simplicity, assume $0 \le a,b \le p$

Know $ab = kp$ and $\gcd(a,p) = 1$

By Bézout's Theorem, there are ints s,t with

$$1 = \gcd(a,p) = sa + tp$$

$$b = b\,(sa + tp) = s(ab)+(bt)p = s(kp) + (bt)p = (sk+bt)p$$

Primes

Rosen p. 257

An integer p greater than 1 is **prime** if its only positive factors are 1 and p.

Fact: There are no zero divisors mod p.

Why? Suppose ab mod p = 0. Then ab = kp so p | (ab).

So p|a and p|b. That is, a mod p = 0 and b mod p=0.

mod b there are no zero divisors

Arithmetic

- modulo p, arithmetic looks very familiar

Fundamental Theorem of Arithmetic

Rosen p 336

- Strong induction!

- P(n) "n can be written as the product of primes"

Infinitely many primes

Rosen p. 260

- Proof by contradiction!

Open questions

- Can we efficiently factor a large number into primes?
- Is every even number the sum of two primes
  - Goldbach's conjecture
- Are there infinitely many "twin primes"?