

CSE 20—Discrete Math

Spring, 2006

October 13 (Day 7)
Number Theory

Instructor: Neil Rhodes

Modulo

Remainder when dividing two positive integers (mod as an operator):

- $n = m \lfloor n/m \rfloor + (n \bmod m)$

Extended to negative numbers ($y \neq 0$)

- $x \bmod y = x - y \lfloor x/y \rfloor$

Equivalence classes (mod as an equivalence relation)

- $a \equiv b \bmod m$ iff $a-b$ is a multiple of m

Residue classes mod m

- m of them
 - All a such that $a \equiv 0 \bmod m$
 - All a such that $a \equiv 1 \bmod m$
 - ...
 - All a such that $a \equiv m-1 \bmod m$

2

Modulo Arithmetic

If:

- $x = x' \bmod m$
- $y = y' \bmod m$
- $z = z' \bmod m$

Then

- $x + y \equiv x' + y' \bmod m$
- $x - y \equiv x' - y' \bmod m$
- $xy \equiv x'y' \bmod m$
- $xy+z \equiv x'y' + z' \bmod m$

3

Casting out 9's

Given x , how to calculate $x \bmod 9$

- Take all the digits of x
- Add them together. If the result is bigger than 9, use this formula recursively

Shortcut:

- As you are adding the digits of x , if you ever have an intermediate value ≥ 9 , add its two digits together
- If you ever find a 9, throw it away (*cast it out*)
- Casting out 9's

$$\begin{array}{r} 532 \\ + 656 \\ 95 \\ \hline 1273 \end{array}$$

$$\begin{array}{r} 5723386 \\ \times 51553 \\ \hline 295057718458 \end{array}$$

Why it works:

- $10 \equiv 1 \bmod 9$
- $10^n \equiv 1 \bmod 9$
- $10^na \equiv a \bmod 9$
- $10^na + 10^{n-1}b + 10^{n-2}c + \dots + 10y + z = (a + b + c + \dots + y + z) \bmod 9$

Limitations:

4

Casting out 11's

Given x , how to calculate $x \bmod 11$

- Starting from the right, alternately add and subtract each digit

$$\begin{array}{r} 532 \\ + 656 \\ \hline 1823 \end{array} \qquad \begin{array}{r} 5723386 \\ \times 51553 \\ \hline 259057718458 \end{array}$$

Why it works

- $10 \equiv -1 \pmod{11}$
- $100 \equiv (10 \cdot 10) \pmod{11} \equiv (-1 \cdot -1) \pmod{11} = 1 \pmod{11}$
- if n is
 - even: $10^n \equiv 1 \pmod{11}$
 - odd: $10^n \equiv -1 \pmod{11}$
- $10^n a \equiv a \pmod{11}$ (or $10^n a \equiv -a \pmod{11}$)
- $10^n a + 10^{n-1} b + 10^{n-2} c + \dots + 10y + z \equiv (z + (-1)^n y + \dots + (-1)^n c + (-1)^{n-1} b + (-1)^{n-2} a) \pmod{11}$

5

Application: ISBN Check digit

Check digit for ISBN:

- 1•first digit
- + 2•second digit
- + 3•third digit
- ...
- + 9•9th' digit
- total mod 11 = check digit

Alternatively:

- 10•first-digit
- +9•second digit
- +8•third-digit
- +2•ninth digit
- +1•check digit

$$\text{total} = 0 \pmod{11}$$

6

Rationals and Irrationals

Rationals are closed under addition, subtraction, multiplication, and division

- except division by zero

Irrationals are *not* closed under multiplication

- Irrational * irrational may equal rational
- What about irrational * (non-zero) rational?

7

Mersenne Primes

Primes of the form $2^n - 1$

- For example, 3, 7, 31, 63
- Any such prime must actually be of the form $2^p - 1$
 - Because $2^{km} - 1 = 2^m - 1(2^{m(k-1)} + 2^{m(k-2)} + \dots + 1)$
- 43rd known Mersenne prime: $2^{30,402,457} - 1$
 - Contains >9,000,000 digits

8

Sieve of Erataosthenes

Make a list of natural numbers

Circle the first number, 2, and mark all its multiples

Repeat

- Circle the first uncircled unmarked number
- Mark all its multiples

Circled numbers are prime

9

Distribution of Prime Numbers

There are approximately $x/\ln x$ primes $\leq x$

- (The size of the n th prime is approximately $n/\ln n$)

10

gcd, lcm, Φ

Greatest Common Divisor (gcd)

- $\gcd(m, n)$ is the largest integer k that divides integers m and n
 - $k \mid m$ and $k \mid n$
- $\gcd(m, n)$ is a *linear combination* (with integer coefficients) of m and n
 - $\exists i, j \in \mathbb{Z}: \gcd(m, n) = im + jn$
- To calculate $\gcd(m, n)$
 - Compute prime factorization of m and n
 - $\gcd(m, n)$ = common prime factors (and powers) of m and n
- Euclid's algorithm
 - int $\gcd(m, n)$
 - if $(n == 0)$ return m
 - else return $\gcd(n, n \% m)$

Least Common Multiple (lcm)

- $\text{lcm}(m, n)$ is the smallest integer k such that integers m and n divide k
 - $m \mid k$ and $n \mid k$
- To calculate $\text{lcm}(m, n)$
 - Compute prime factorizations of m and n
 - $\text{lcm}(m, n)$ = union of prime factors (and powers) of m and n

Φ (Euler function, or totient function)

- $\Phi(n)$ = the number of positive integers $k \leq n$ such that $k \perp n$ ($\gcd(k, n) = 1$)

11

Properties of the totient function

Given p prime:

- $\Phi(p) = p - 1$

Given p prime:

$$\Phi(p^k) = (p - 1)p^{k-1}$$

Given p and q relatively prime

- $\Phi(pq) = \Phi(p) \Phi(q)$

Given $p_1, \dots, p_i$ are all primes:

$$\Phi(p_1^{k_1} p_2^{k_2} \dots p_i^{k_i}) = (p_1 - 1)p_1^{k_1-1} (p_2 - 1)p_2^{k_2-1} \dots (p_i - 1)p_i^{k_i-1}$$

Call the $\Phi(n)$ numbers relatively prime to n *units*

- Given a unit of n , $a: a^{\Phi(n)} \equiv 1 \pmod{n}$

Thus, given two distinct primes, p and q

- $m \perp pq \rightarrow m^{(p-1)(q-1)} \equiv 1 \pmod{pq}$

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\Phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8

12

Cryptography

Definitions:

- Plaintext: message being encoded
- Ciphertext: encoded plaintext
- Key: parameter to crypto algorithms
 - $C = E(P, K_E)$
 - $P = D(C, K_D)$

Simple cipher (Caesar cipher):

- $K_E = K_D$ = permutation from letters to letters
 - $A \rightarrow X$
 - $B \rightarrow L$
 - ...
 - $Z \rightarrow R$
- E = apply K_E to each character in plaintext
- D = apply K_E^{-1} to each character in ciphertext
- Weakness: letter frequencies

13

Unbreakable Code

One-time pad

- $K_E = K_D$ = long stream of random bytes
 - Really random, not pseudo-random
- $E(P, K_E)$
 - for $i = 1$ to $\text{length}(P)$
 $C[i] = P[i] \text{ XOR } K_E[i]$
- $D = E$
- Alice sends message to Bob
 - Uses secret one-time pad
 - Encrypts P
 - Destroys P and one-time pad
- Bob decrypts
 - Using one-time pad
- Alternative encryption (by-hand)
 - Modular arithmetic
- Weakness
 - Key must be as long as plaintext
 - Key must be used only once
 - Key must be truly random

14

Reusing Key

Problem

- If plaintext and ciphertext are both known, key can be reverse-engineered
 - $K_E[i] = P[i] \text{ XOR } C[i]$
- How to know plaintext if it is encrypted?
 - Cause specific plaintext to be sent
 - British would mine specific areas in WWII so that the Germans would send message including "minen" and location.

15