**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):

- \( n = m \cdot \lfloor \frac{n}{m} \rfloor + (n \mod m) \)

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

- \( x \mod y = x - y \cdot \lfloor \frac{x}{y} \rfloor \)

**Equivalence classes (mod as an equivalence relation)**

- \( a \equiv b \mod m \) iff \( a - b \) is a multiple of \( m \)

**Residue classes mod \( m \)**

- \( m \) of them
  - All \( a \) such that \( a \equiv 0 \mod m \)
  - All \( a \) such that \( a \equiv 1 \mod m \)
  - \( \ldots \)
  - All \( a \) such that \( a \equiv m-1 \mod m \)

---

**Modulo Arithmetic**

If:

- \( x = x' \mod m \)
- \( y = y' \mod m \)
- \( z = z' \mod m \)

Then

- \( x + y \equiv x' + y' \mod m \)
- \( x - y \equiv x' - y' \mod m \)
- \( xy \equiv x'y' \mod m \)
- \( xy+z \equiv x'y' +z' \mod m \)

---

**Casting out 9’s**

**Given \( x \), how to calculate \( x \mod 9 \)**

- 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 \( \geq 9 \), add its two digits together
- If you ever find a 9, throw it away *(cast it out)*

**Example:**

- 532 + 656
- 1273

**Why it works:**

- \( 10 \equiv 1 \mod 9 \)
- \( 10^n \equiv 1 \mod 9 \)
- \( 10^a \equiv a \mod 9 \)
- \( 10^a+10^{a+1}b+10^{a+2}c+\ldots+10y+z \equiv (a + b + c + \ldots + y + z) \mod 9 \)

**Limitations:**
Casting out 11’s

Given $x$, how to calculate $x \mod 11$
- Starting from the right, alternately add and subtract each digit

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>532</td>
<td>+</td>
<td>656</td>
</tr>
<tr>
<td>95</td>
<td>x</td>
<td>5723386</td>
</tr>
<tr>
<td></td>
<td></td>
<td>51553</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1823</td>
</tr>
<tr>
<td></td>
<td></td>
<td>259057718458</td>
</tr>
</tbody>
</table>

Why it works
- $10 \equiv -1 \mod 11$
- $100 \equiv (10\times10) \mod 11 \equiv (-1\times-1) \mod 11 = 1 \mod 11$
- if $n$ is
  - even: $10^n \equiv 1 \mod 1$
  - odd: $10^n \equiv -1 \mod 1$
- $10^a \equiv a \mod 11$ (or $10^a \equiv -a \mod 11$)
- $10^a + 10^{a-1}b + 10^{a-2}c + \ldots + 10y + z \equiv (z - y + \ldots - c + b - a) \mod 11$

Application: ISBN Check digit

Check digit for ISBN:
- 1•first digit
- + 2•second digit
- + 3•third digit
- + 9•9th’ digit
- + total $\mod 11 = \text{check digit}$

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

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?

Mersenne Primes

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

Distribution of Prime Numbers
There are approximately $x/\ln x$ primes ≤ $x$
• (The size of the $n$th prime is approximately $n/\ln n$)

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

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 $n$
  - $\text{lcm}(m, n) = \text{union of prime factors (and powers) of } m \text{ and } n$

$\Phi$ (Euler function, or totient function)
• $\Phi(n) = $ the number of positive integers $k \leq n$ such that $k \perp n \Leftrightarrow (\text{gcd}(k, n) = 1)$
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
  - $A \rightarrow X$
  - $B \rightarrow L$
  - $\ldots$
  - $Z \rightarrow R$
- $E = $ apply $K_E$ to each character in plaintext
- $D = $ apply $K_E^{-1}$ to each character in ciphertext
- Weakness: letter frequencies

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 length($P$)
    - $C[i] = P[i] XOR K_E[i]$
- $D = E$
- 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

Reusing Key

Problem
- If plaintext and ciphertext are both known, key can be reverse-engineered
  - $K_E[i] = P[i] XOR C[i]$
- 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.