CSE 321 Discrete Structures

Winter 2008
Lecture 8
Number Theory: Modular Arithmetic

Announcements

- Readings
  - Today:
    - 3.4 (5th Edition: 2.4)
  - Monday and Wednesday:
    - 3.5, 3.6, 3.7 (5th Edition: 2.5, 2.6)

Highlights from Lecture 7

- Set Theory and ties to Logic
- Review of terminology:
  - Complement, Universe of Discourse, Cartesian Product, Cardinality, Power Set, Empty Set, N, Z, Z^+, Q, R, Subset, Proper Subset, Venn Diagram, Set Difference, Symmetric Difference, De Morgan's Laws, Distributive Laws

Number Theory (and applications to computing)

- Branch of Mathematics with direct relevance to computing
- Many significant applications
  - Cryptography
  - Hashing
  - Security
- Important tool set

Modular Arithmetic

- Arithmetic over a finite domain
- In computing, almost all computations are over a finite domain

What are the values computed?

```
public void Test1() {
        byte x = 250;
        byte y = 20;
        byte z = (byte) (x + y);
        Console.WriteLine(z);
}
```

```
public void Test2() {
        sbyte x = 120;
        sbyte y = 20;
        sbyte z = (sbyte) (x + y);
        Console.WriteLine(z);
}
```

Arithmetic mod 7

- a $+_7$ b = (a + b) mod 7
- a $\times_7$ b = (a $\times$ b) mod 7

+	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

x	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

Group Theory

- A group G=(S, •) is a set S with a binary operator • that is "well behaved":
  - Closed under •
  - Associative: a • (b • c) = (a • b) • c
  - Has an identity
  - Each element has an inverse
- A group is commutative if the • operator also satisfies a• b = b • a

Groups, mod 7

- {0,1,2,3,4,5,6} is a group under $+_7$
- {1,2,3,4,5,6} is a group under $\times_7$

Multiplicative Inverses

- Euclid's theorem: if *x* and *y* are relatively prime, then there exists integers *s*, *t*, such that:

$$sx + ty = 1$$

- Prove $a \in \{1, 2, 3, 4, 5, 6\}$ has a multiplicative inverse under $\times_7$

Generalizations

- ({0,…, *n*-1}, $+_n$) forms a group for all positive integers *n*
- ({1,…, *n*-1}, $\times_n$) is a group if and only if *n* is prime

Basic applications

- Hashing: store keys in a large domain 0…M-1 in a much smaller domain 0…n-1

Pseudo Random number generation

- Linear Congruential method

$$x_{n+1} = (a\, x_n + c) \bmod m$$

Simple cipher

- Caesar cipher, a = 1, b = 2, . . .
  - HELLO WORLD
- Shift cipher
  - f(p) = (p + k) mod 26
  - f^{-1}(p) = (p – k) mod 26
- f(p) = (ap + b) mod 26

Modular Exponentiation

x	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

a	a^1	a^2	a^3	a^4	a^5	a^6
1						
2						
3						
4						
5						
6						