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

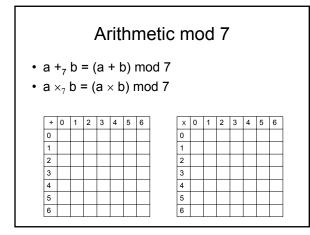
Modular Arithmetic

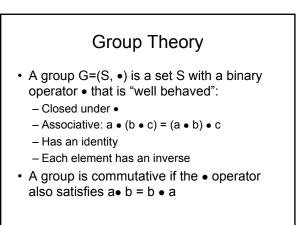
- · Arithmetic over a finite domain
- In computing, almost all computations are over a finite domain

What are the values computed?

}

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





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 ∈ {1, 2, 3, 4, 5, 6} has a multiplicative inverse under ×₇

Generalizations

- ({0,..., n-1}, +_n) forms a group for all positive integers n
- ({1,..., n-1}, ×_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

