CSE 321 Discrete Structures
Winter 2008
Lecture 9
Number Theory: Modular Arithmetic

Announcements

• Readings
  – Today:
    • Modular Exponentiation
      – 3.5, 3.6 (5th Edition: 2.5)
  – Wednesday:
    • Primality
      – 3.6 (5th Edition: 2.5)
  – Friday:
    • Applications of Number Theory
      – 3.7 (5th Edition: 2.6)

Highlights from Lecture 8

• Modular Arithmetic
  – a mod n: remainder when divided by n
    • 0 \leq a \mod n \leq n-1
  – a \equiv b \pmod{n} means a \mod n = b \mod n
  – a + nb = (a + b) \mod n
  – a \times b = (a \times b) \mod n
• Finite domain arithmetic
  – Well behaved, especially if n is prime
  – Applications to computing

Hashing

• Map values from a large domain, 0…M-1
  in a much smaller domain, 0…n-1
• Index lookup
• Test for equality
• Hash(x) = x \mod p
• Often want the hash function to depend on all of the bits of the data
  – Collision management

Pseudo Random number generation

• Linear Congruential method
  \[ x_{n+1} = (a \times x_n + c) \mod m \]

Data Permutations

• Caesar cipher, a = 1, b = 2, …
  – HELLO WORLD
• Shift cipher
  – f(x) = (x + k) \mod n
  – f^{-1}(x) = (x - k) \mod n
• Affine cipher
  – f(x) = (ax + b) \mod n
  – f^{-1}(x) = (a^{-1}(x-b)) \mod n
Modular Exponentiation

Fermat’s Little Theorem
- If p is prime, \(0 < a \leq p-1\), \(a^{p-1} \equiv 1 \pmod{p}\)
- Group theory
  - Index of \(x\), smallest \(i > 0\) such that \(x^i = 1\)
  - The index of \(x\) divides the order of the group

Exponentiation
- Compute \(78365^{81453}\)
- Compute \(78365^{81453} \mod 104729\)

Fast exponentiation
- What if the exponent is not a power of two?
  \(81453 = 2^{16} + 2^{13} + 2^{12} + 2^{11} + 2^{10} + 2^9 + 2^8 + 2^7 + 2^5 + 2^0\)
- The fast multiplication algorithm computes \(a^n \mod p\) in time \(O(\log n)\)
Discrete Log Problem

• Given integers \( a, b \) in \([1, \ldots, p-1]\), find \( k \) such that \( a^k \mod p = b \)

Primality

• An integer \( p \) is prime if its only divisors are 1 and \( p \)
• An integer that is greater than 1, and not prime is called composite
• Fundamental theorem of arithmetic:
  – Every positive integer greater than one has a unique prime factorization

Factorization

• If \( n \) is composite, it has a factor of size at most \( \sqrt{n} \)

Euclid’s theorem

• There are an infinite number of primes.
• Proof by contradiction:
  • Suppose there are a finite number of primes: \( p_1, p_2, \ldots, p_n \)