CSE 321 Discrete Structures

Winter 2008
Lecture 10
Number Theory: Primality

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 9

- Modular Exponentiation
  - $a^{p-1} \equiv 1 \pmod p$ for p prime
  - $a^k \bmod n$ can be computed in O(log k) time

Big number arithmetic

- Computer Arithmetic 32 bit (or 64 bit, or 128 bit)
- Arbitrary precision arithmetic
  - Store number in arrays or linked lists
- Runtimes for standard algorithms for n digit numbers
  - Addition:
  - Multiplication:

Discrete Log Problem

- Given integers a, b in [1,…, p-1], find k such that $a^k \bmod p = b$

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, . . . p_n

Distribution of Primes

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89
97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173
179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263
269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359

- If you pick a random number n in the range [x, 2x], what is the chance that n is prime?

Famous Algorithmic Problems

- Primality Testing:
  – Given an integer n, determine if n is prime
- Factoring
  – Given an integer n, determine the prime factorization of n

Primality Testing

- Is the following 200 digit number prime:

40992408416096028179761232532587525402909285099086220133403920525409552083528606215439915948260875718893797824735118621138192569490840098061133066650255608065609253901288801302035441884878187944219033

Showing a number is NOT prime

- Trial division by small primes
- Fermat's little theorem
  – a^{p-1} mod p = 1 if p is prime
- Miller's Test
  – if p is prime, the only square roots of one are 1 and -1
  – if p is composite other numbers can be the square root of one
  – repeated squaring used to find a non-trivial square root of one from a starting value b

Probabilistic Primality Testing

- Conduct Miller's test for a random b
  - If p is prime, it always passes the test
  - If p is not prime, it fails with probability ¾
- Primality testing
  - Choose 100 random b's and perform Miller's test on each
  - If any say false, answer "Composite"
  - If all say true, answer "Prime"