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
  – \(a^k \pmod{n}\) 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 \(a^k \pmod{p} = b\)

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: \( p_1, p_2, \ldots, p_n \)

Distribution of Primes
- 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:
  40962408416066282179761232532587525402993285090822201334
  03502525409520855266254398159442526875718937978247351
  186211381295694684009606113306665025560806656092539012888
  013003544184878187944219033

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 $\frac{3}{4}$
- 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”