CSE 15
Discrete Mathematics

Lecture 16 – Number Theory & Cryptography (2)

Announcement

- HW #8
  - To be assigned after the MT #2.
- Midterm #2 on Tuesday (11/13)
  - In the class, starting at 9AM.
  - Covers
    - sections 2.1 – 3.3
    - HWs 4-7
    - CLOSED BOOK AND NOTES
- Reading assignment
  - Ch. 5.1 – 5.4 of textbook

Binary Modular Exponentiation

- In cryptography, it is important to compute b^n **mod** m efficiently, where b, n, and m are large integers.
- Use the binary expansion of n, $n = (a_{k-1},\ldots,a_1,a_0)_2$, to compute b^n .

 Note that:

$$b^n = b^{a_{k-1}\cdot 2^{k-1}+\cdots+a_1\cdot 2+a_0} = b^{a_{k-1}\cdot 2^{k-1}} \cdots b^{a_1\cdot 2} \cdot b^{a_0}.$$

Example: Compute 3^{11} using this method.

Solution: Note that $11 = (1011)_2$ so that $3^{11} = 3^8\, 3^2\, 3^1 = ((3^2)^2)^2\, 3^2\, 3^1 = (9^2)^2 \cdot 9 \cdot 3 = (81)^2 \cdot 9 \cdot 3 = 6561 \cdot 9 \cdot 3 = 117{,}147$.

continued →

Primes, Greatest Common Divisors, LCMs (Ch. 4.3)

- Prime Numbers and their Properties
- Conjectures and Open Problems About Primes
- Greatest Common Divisors and Least Common Multiples
- The Euclidian Algorithm

Primes

Definition: A positive integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p.

A positive integer that is greater than 1 and is not prime is called *composite*.

Example: The integer 7 is prime because its only positive factors are 1 and 7, but 9 is composite because it is divisible by 3.

The Fundamental Theorem of Arithmetic

Theorem: Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes.

Examples:

- $100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$
- $641 = 641$ (a prime number)
- $999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$
- $1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

Theorem

- Theorem: If *n* is a composite integer, then *n* has a prime divisor less than or equal to $\sqrt{n}$.
- As *n* is composite, *n* has factors 1<*a*,*b* such that *n*=*ab*.
- Then a≤$\sqrt{n}$ or b ≤$\sqrt{n}$.
- Thus *n* has a divisor not exceeding $\sqrt{n}$.

Determining Primality by Trial Division

- A very inefficient method of determining if a number n is prime, is to try every prime integer $i \leq \sqrt{n}$ and see if n is divisible by i.
- Example:
  - Show that 101 is prime.
  - The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, 7.
  - As 101 is not divisible by 2, 3, 5, 7, it follows that 101 is prime .

Procedure for Prime Factorization

- Begin by diving *n* by successive primes, starting with 2.
- If *n* has a prime factor, we would find a prime factor not exceeding $\sqrt{n}$.
- If no prime factor is found, then *n* is prime.
- Otherwise, if a prime factor *p* is found, continue by factoring *n*/*p.*
- If *n*/*p* has no prime factor greater than or equal to *p* and not exceeding its square root, then it is prime.
- Otherwise, if it has a prime factor *q*, continue by factoring *n*/(*pq*).
- Continue until factorization has been reduced to a prime

Example

- Find the prime factorization of 7007.
- Start with 2, 3, 5, and then 7, 7007/7=1001.
- Then, divide 1001 by successive primes, beginning with 7, and find 1001/7=143.
- Continue by dividing 143 by successive primes, starting with 7, and find 143/11=13.
- As 13 is prime, the procedure stops.
- $7007=7\cdot 7\cdot 11\cdot 13=7^2\cdot 11\cdot 13$

The Sieve of Erastosthenes

- The *Sieve of Erastosthenes* can be used to find all primes not exceeding a specified positive integer. For example, begin with the list of integers between 1 and 100.

a. Delete all the integers, other than 2, divisible by 2.
b. Delete all the integers, other than 3, divisible by 3.
c. Next, delete all the integers, other than 5, divisible by 5.
d. Next, delete all the integers, other than 7, divisible by 7.
e. Since all the remaining integers are not divisible by any of the previous integers, other than 1, the primes are:

{2,3,7,11,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89, 97}

continued →

Mersenne Primes

Definition: Prime numbers of the form $2^p - 1$, where *p* is prime, are called *Mersenne primes*.

- $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, and $2^7 - 1 = 127$ are Mersenne primes.
- $2^{11} - 1 = 2047$ is not a Mersenne prime since $2047 = 23 \cdot 89$.
- There is an efficient test for determining if $2^p - 1$ is prime.
- The largest known prime numbers are Mersenne primes.
- As of mid 2011, 47 Mersenne primes were known, the largest is $2^{43,112,609} - 1$, which has nearly 13 million decimal digits.

Distribution of Primes

- What is the distribution of prime numbers among the positive integers.
- In the nineteenth century, the *prime number theorem* was proved which gives an asymptotic estimate for the number of primes not exceeding x.

The **Prime Number Theorem**: The ratio of the number of primes not exceeding x and $x/\ln x$ approaches 1 as x grows without bound. ("ln x" is the natural logarithm of x)

  - The theorem tells us that the number of primes not exceeding x, can be approximated by $x/\ln x$.
  - The odds that a randomly selected positive integer less than n is prime are approximately $(n/\ln n)/n = 1/\ln n$.

Generating Primes

- So far, no useful closed formula that always produces primes has been found.
- That is, there is no simple function $f(n)$ such that $f(n)$ is prime for all positive integers n.
- But $f(n) = n^2 - n + 41$ is prime for all integers 1,2,..., 40. Because of this, we might conjecture that $f(n)$ is prime for all positive integers n. But $f(41) = 41^2$ is not prime.
- There is no polynomial such that $f(n)$ is prime for all positive integers n.
- *My Method: 3*n+1 and/or 3*n-1 are primes when n is even.*

n=2: 5/7; n=4: 11/13; n=6: 17 /19; n=8: 23/25 (failed); n=10: 29/31; n=12: 35/37; n=14: 41/43; n=16: 47/49, n=18: 53/55; n=20: 59/61; n=22: 65/67; n=24: 71/73; n=26: 77/79; n=28: 83/85; n=30: 89/91.

n=1000000: 3000001/2999999

Conjectures about Primes

- *Goldbach's Conjecture*: Every even integer n, $n > 2$, is the sum of two primes. It has been verified by computer for all positive even integers up to $1.6 \cdot 10^{18}$.
- There are infinitely many primes of the form $n^2 + 1$, where n is a positive integer. (does not work for n=3,5,7, 8, 9, 11, 12, 13, 15, …)

  (definitely not a prime when n is an odd number.)
- There are infinitely many positive integers n such that $n^2 + 1$ is prime or the product of at most two primes.
- *The Twin Prime Conjecture*: There are infinitely many pairs of twin primes. <u>Twin primes are pairs of primes that differ by 2</u>. Examples are 3 and 5, 5 and 7, 11 and 13, etc.
- The current world's record for twin primes (as of mid 2011) consists of numbers $65{,}516{,}468{,}355 \cdot 23^{333{,}333} \pm 1$, which have 100,355 decimal digits.

Greatest Common Divisor (GCD)

Definition: Let *a* and *b* be integers, not both zero. The largest integer *d* such that *d* | *a* and also *d* | *b* is called ***the greatest common divisor*** of *a* and *b*. The greatest common divisor of *a* and *b* is denoted by ***gcd(a,b)***.

One can find greatest common divisors of small numbers by inspection.

Example: What is the greatest common divisor of 24 and 36?

Solution: gcd$(24,36)$ = 12

Example: What is the greatest common divisor of 17 and 22?

Solution: gcd$(17,22)$ = 1

Greatest Common Divisor (GCD)

Definition: The integers a and b are *relatively prime* if their greatest common divisor is 1.

Example: 17 and 22

Definition: The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j)=1$ whenever $1 \leq i<j \leq n$.

Example: Determine whether the integers 10, 17 and 21 are pairwise relatively prime.

Solution: $\gcd(10,17)=1$, $\gcd(10,21)=1$, and $\gcd(17,21)=1$, thus, 10, 17, and 21 are pairwise relatively prime.

Example: Determine whether the integers 10, 19, and 24 are pairwise relatively prime.

Solution: Because $\gcd(10,24)=2$, 10, 19, and 24 are not pairwise relatively prime.

Finding the Greatest Common Divisor Using Prime Factorizations

- Suppose the prime factorizations of *a* and *b* are:

  $$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}\ , \qquad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}\ ,$$

  where each exponent is a nonnegative integer, and where all primes occurring in either prime factorization are included in both. Then:

  $$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \dots p_n^{\min(a_n,b_n)}\ .$$

- This formula is valid since the integer on the right (of the equals sign) divides both *a* and *b*. No larger integer divides both *a* and *b*.

Example: $120 = 2^3 \cdot 3 \cdot 5 \qquad 500 = 2^2 \cdot 5^3$

$\gcd(120,500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 3^0 \cdot 5^1 = 20$

Least Common Multiple (LCM)

Definition: The ***least common multiple*** of the positive integers *a* and *b* is the smallest positive integer that is divisible by both *a* and *b*. It is denoted by ***lcm(a,b)***.

- The least common multiple can also be computed from the prime factorizations.

$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

This number is divisible by both *a* and *b* and no smaller number is divisible by *a* and *b*.

Example: $\text{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)}\, 3^{\max(5,3)}\, 7^{\max(2,0)} = 2^4\, 3^5\, 7^2$

- The greatest common divisor and the least common multiple of two integers are related by:

Theorem 5: Let a and b be positive integers. Then

$$ab = \gcd(a,b) \cdot \text{lcm}(a,b)$$

Euclidean Algorithm for GCD

- The Euclidian algorithm is an efficient method for computing the GCD of two integers. It is based on the idea that gcd(a,b) is equal to gcd(b,c) when $a > b$ and c is the remainder when a is divided by b.

Example: Find $\gcd(287, 91)$:

- $287 = 91 \cdot 3 + 14$
- $91 = 14 \cdot 6 + 7$
- $14 = 7 \cdot 2 + 0$

Divide 287 by 91

Divide 91 by 14

Divide 14 by 7

Stopping condition

gcd(287, 91) = gcd(91, 14) = gcd(14, 7) = 7

continued →

Euclidean Algorithm

- The Euclidean algorithm expressed in pseudocode is:

procedure *gcd*(*a, b*: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return x {gcd(a,b) is x}

- The time complexity of the algorithm is $O(\log b)$, where a > b.