CSL202: Discrete Mathematical Structures

Ragesh Jaiswal, CSE, IIT Delhi

Number Theory and Cryptography

Theorem

Let b be an integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0,$$

where k is a nonnegative integer, $a_0, a_1, ..., a_k$ are nonnegative integers less than b, and $a_k \neq 0$.

- What is the running time of each of the following operations:
  - Adding an m bit number with an n bit number.
  - Multiplying an m bit number with an n bit number.
  - Dividing an m bit number by an n bit number.
  - Computing an m bit number modulo an n bit number.

Definition

An 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*.

Theorem (Fundamental theorem of arithmetic)

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Theorem

If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

- How can we find all prime numbers ≤ 100?
  - Show that any composite number ≤ 100 are divisible by $2, 3, 5, 7$.
  - Sieve of Eratosthenes uses this idea to eliminate all composites and list all primes.

Theorem

There are infinitely many primes.

Definition

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

Definition

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

Definition

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

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. The least common multiple of a and b is denoted by $lcm(a, b)$.

Theorem

Let a and b be positive integers. Then $ab = gcd(a, b) \cdot lcm(a, b)$.

Theorem

Let $a = bq + r$, where $a, b, q,$ and r are integers. Then $gcd(a, b) = gcd(b, r)$.

- Using the above theorem, design an algorithm to compute gcd of two n bit numbers. What is the worst-case running time of your algorithm?

Theorem

Let $a = bq + r$, where a, b, q, and r are integers. Then $gcd(a, b) = gcd(b, r)$.

- Using the above theorem, design an algorithm to compute gcd of two n bit numbers. What is the worst-case running time of your algorithm?

Euclid-GCD(a, b)
  If ($b = 0$) then return(a)
  else return(Euclid-GCD($b, a \ (mod \ b)$))

Euclid-GCD(a, b)
  If ($b = 0$) then return(a)
  else return(Euclid-GCD($b, a \ (mod \ b)$))

- How many recursive calls are made by the algorithm?
- What is the worst-case time complexity of the algorithm?

End