

ACOL1002: Discrete Mathematical Structures

Ragesh Jaiswal, CSE, IIT Delhi

Number Theory and Cryptography

Number Theory and Cryptography

Divisibility and Modular Arithmetic

Theorem

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \quad \text{and} \quad ac \equiv bd \pmod{m}.$$

Theorem

Let m be a positive integer and let a and b be integers. Then

$$(a + b) \pmod{m} = ((a \pmod{m}) + (b \pmod{m})) \pmod{m}$$

and

$$ab \pmod{m} = ((a \pmod{m})(b \pmod{m})) \pmod{m}.$$

Number Theory and Cryptography

Divisibility and Modular Arithmetic

- Let $Z_m = \{0, 1, 2, \dots, m - 1\}$.
- We can define the following arithmetic operations on Z_m :
 - $+_m$: This is defined as $a +_m b = (a + b) \pmod{m}$.
 - $\cdot_m$: This is defined as $a \cdot_m b = (a \cdot b) \pmod{m}$.
- Show that $+_m$ and $\cdot_m$ satisfies the following properties:
 - Closure
 - Associativity
 - Commutativity
 - Identity
 - Additive inverse
 - Distributivity

Number Theory and Cryptography

Divisibility and Modular Arithmetic

Theorem

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

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

where k is a nonnegative integer, $a_0, a_1, \dots, a_k$ 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.

Number Theory and Cryptography

Binary Multiplication

Problem

Multiplying two n -bit numbers: Given two n -bit numbers, A and B , Design an algorithm to output $A \cdot B$.

Number Theory and Cryptography

Binary Multiplication

Problem

Multiplying two n -bit numbers: Given two n -bit numbers, A and B , Design an algorithm to output $A \cdot B$.

- Solution 1: Use long multiplication.
- What is the running time of the algorithm that uses long multiplication?

Number Theory and Cryptography

Binary Multiplication

Problem

Multiplying two n -bit numbers: Given two n -bit numbers, A and B , Design an algorithm to output $A \cdot B$.

- Solution 1: Use long multiplication.
- What is the running time of the algorithm that uses long multiplication? $O(n^2)$
- Is there a faster algorithm?

Number Theory and Cryptography

Divisibility and Modular Arithmetic

Theorem

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

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

where k is a nonnegative integer, $a_0, a_1, \dots, a_k$ 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.

End