COL202: Discrete Mathematical Structures

Ragesh Jaiswal, CSE, IIT Delhi

Number Theory and Cryptography

Definition

If a and b are integers with $a \neq 0$, we say that a *divides* b if there is an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer. When a divides b we say that a is a *factor* or *divisor* of b and that b is a *multiple* of a. The notation $a|b$ denotes that a divides b. We write $a \not| b$ when a does not divide b.

Theorem

Let a, b, and c be integers, where $a \neq 0$. Then

1. *If $a|b$ and $a|c$, then $a|(b+c)$.*
2. *If $a|b$, then $a|bc$ for all integers c.*
3. *If $a|b$ and $b|c$, then $a|c$.*

Definition

If a and b are integers with $a \neq 0$, we say that a *divides* b if there is an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer. When a divides b we say that a is a *factor* or *divisor* of b and that b is a *multiple* of a. The notation $a|b$ denotes that a divides b. We write $a \not| b$ when a does not divide b.

Theorem

Let a, b, and c be integers, where $a \neq 0$. Then

1. *If $a|b$ and $a|c$, then $a|(b + c)$.*
2. *If $a|b$, then $a|bc$ for all integers c.*
3. *If $a|b$ and $b|c$, then $a|c$.*

Corollary

If a, b, and c are integers, where $a \neq 0$, such that $a|b$ and $a|c$, then $a|(mb + nc)$ whenever m and n are integers.

Theorem (Division Theorem)

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

Definition

In the equality given in the division theorem, d is called the divisor, a is called the dividend, q is called the quotient, and r is called the remainder. This notation is used to express the quotient and remainder:

$$q = a \ (div \ \ d), \quad r = a \ (mod \ \ d)$$

Definition

If a and b are integers and m is a positive integer, then a is *congruent* to b *modulo* m if m divides $a - b$. We use the notation $a \equiv b \pmod{m}$ to indicate that a is congruent to b modulo m. We say that $a \equiv b \pmod{m}$ is a *congruence* and that m is its *modulus*. If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$.

Theorem

Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \pmod{m} = b \pmod{m}$.

Theorem

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Theorem

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

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

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

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

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

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.

End