

ACOL1002: Discrete Mathematical Structures

Ragesh Jaiswal, CSE, IIT Delhi

Number Theory and Cryptography

Number Theory and Cryptography

Primes and GCD

Theorem

Let a, b be positive integers. Then there exist integers x, y such that $xa + yb = \gcd(a, b)$. Furthermore, $\gcd(a, b)$ is the smallest positive integer that can be expressed in this way.

Number Theory and Cryptography

Primes and GCD

- For any positive integer m , let Z_m denote the set $\{0, 1, \dots, m-1\}$.
- Consider the set $Z_m^* = \{x \in Z_m \mid \gcd(x, m) = 1\}$ and the operator $\cdot_m$ which is basically the operation multiplication modulo m .
- Show that $\cdot_m$ satisfies the following properties:
 - Closure
 - Associativity
 - Commutativity
 - Identity
 - **Inverse**
- How do you compute the inverse of $x \in Z_m^*$ modulo m ?

Number Theory and Cryptography

Primes and GCD

- Problem: Given integers $a \geq b > 0$, design an algorithm for computing integers x, y such that $xa + yb = \gcd(a, b)$.

Extended-Euclid-GCD(a, b)

 If($b = 0$), then return($a, 1, 0$)

 else

 Compute integers q, r such that $a = qb + r$ and $0 \leq r < b$.

 Let $(d, x, y) = \text{Extended-Euclid-GCD}(b, r)$

 return($d, y, x - yq$)

Number Theory and Cryptography

Primes and GCD

- Problem: Given integers $a \geq b > 0$, design an algorithm for computing integers x, y such that $xa + yb = \gcd(a, b)$.

Extended-Euclid-GCD(a, b)

 If($b = 0$), then return($a, 1, 0$)

 else

 Compute integers q, r such that $a = qb + r$ and $0 \leq r < b$.

 Let $(d, x, y) = \text{Extended-Euclid-GCD}(b, r)$

 return($d, y, x - yq$)

- How do you compute the inverse of $x \in Z_m^*$ modulo m ?

Number Theory and Cryptography

Primes and GCD

- Problem: Given integers $a \geq b > 0$, design an algorithm for computing integers x, y such that $xa + yb = \gcd(a, b)$.

Extended-Euclid-GCD(a, b)

If ($b = 0$), then return($a, 1, 0$)

else

 Compute integers q, r such that $a = qb + r$ and $0 \leq r < b$.

 Let $(d, x, y) = \text{Extended-Euclid-GCD}(b, r)$

 return($d, y, x - yq$)

- How do you compute the inverse of $x \in \mathbb{Z}_m^*$ modulo m ?
 - Find the inverse of 25 modulo 53.
 - What are the solutions of linear congruence $3x \equiv 4 \pmod{7}$?

Number Theory and Cryptography

Primes and GCD

- Worst-case time complexity of simple operations. In each of the cases the input size is denoted by $n = |a| + |b|$.

Operation	Time complexity
$a \pm b$	?
$a \cdot b$	?
$a \text{ (div } b)$	?
$a \text{ (mod } b)$	?
$a^{-1} \text{ (mod } b)$ for relatively prime a, b	?

Number Theory and Cryptography

Primes and GCD

- Worst-case time complexity of simple operations. In each of the cases the input size is denoted by $n = |a| + |b|$.

Operation	Time complexity
$a \pm b$	$O(n)$
$a \cdot b$	$O(n^2)$
$a \text{ (div } b)$	$O(n^2)$
$a \text{ (mod } b)$	$O(n^2)$
$a^{-1} \text{ (mod } b)$ for relatively prime a, b	$O(n^3)$

End