COL202: Discrete Mathematical Structures

Ragesh Jaiswal, CSE, IIT Delhi

Number Theory and Cryptography

Problem

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

Algorithm

`Karatsuba`(A, B)

- If $(|A| = |B| = 1)$ return$(A \cdot B)$
- Split A into A_L and A_R
- Split B into B_L and B_R
- $P \leftarrow$ `Karatsuba`(A_L, B_L)
- $Q \leftarrow$ `Karatsuba`(A_R, B_R)
- $R \leftarrow$ `Karatsuba`$(A_L + A_R, B_L + B_R)$
- return(`Combine`(P, Q, R))

- Recurrence relation: $T(n) \leq 3 \cdot T(n/2) + cn$; $T(1) \leq c$.
- What is the solution of this recurrence relation?
  $T(n) \leq O(n^{\log_2 3})$

Theorem

Let a, b be positive integers. Then there exists 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.

Theorem

Let a, b be positive integers. Then there exists 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.

Theorem

If a, b, and c are positive integers such that $gcd(a, b) = 1$ and $a|bc$, then $a|c$.

Theorem

If p is a prime and $p|a_1 a_2 ... a_n$, where each a_i is an integer, then $p|a_i$ for some i.

- For any positive integer m, let Z_m denote the set $\{0, 1, ..., m-1\}$.
- Consider the set $Z_m^* = \{x \in Z_m | gcd(x, m) = 1\}$ 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?

- 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 ≤ r < b.
       Let (d, x, y) = Extended-Euclid-GCD(b, r)
       return(d, y, x − yq)
```

- 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) = Extended-Euclid-GCD(b, r)
    return($d, y, x - yq$)

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

- 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) = Extended-Euclid-GCD(b, r)
    return($d, y, x - yq$)

- How do you compute the inverse of $x \in Z_m^*$ modulo m?
  - Find the inverse of 25 modulo 53.
  - What are the solutions of linear congruence $3x \equiv 4 \ (mod\ 7)$?

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

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

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

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

Theorem (Chinese Remaindering Theorem)

Let $m_1, m_2, ..., m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, ..., a_n$ arbitrary integers. Then the system

$$x \equiv a_1 \ (mod \ m_1),$$
$$x \equiv a_2 \ (mod \ m_2),$$
$$\vdots$$
$$x \equiv a_n \ (mod \ m_n)$$

has a unique solution modulo $m = m_1 m_2 ... m_n$. (That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

End