

ACOL1002: Discrete Mathematical Structures

Ragesh Jaiswal, CSE, IIT Delhi

Number Theory and Cryptography

Number Theory and Cryptography

Primes and GCD

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($b, a \bmod b$)))

Number Theory and Cryptography

Primes and GCD

Euclid-GCD(a, b)

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

 else return(Euclid-GCD($b, a \pmod{b}$)))

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

Number Theory and Cryptography

Primes and GCD

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.

Number Theory and Cryptography

Primes and GCD

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 $p|a_1a_2\dots a_n$, where each a_i is an integer, then $p|a_i$ for some i .

End