

Cryptography CS 555

Lecture 10



Department of Computer Sciences
Purdue University

Important Topics We have Covered

- Classical ciphers & their cryptanalysis
 - Shift, substitution, Vigenere
- Perfect secrecy
 - definition, proofs, limitation
- One-time pad
- Semantic security
- Adversary modes
 - ciphertext only, random plaintext, (adaptive) chosen plaintext, (adaptive) chosen ciphertext

Important Topics We have Covered

- Stream ciphers & PRNG
 - Security properties of PRNG
 - Security properties of stream ciphers
 - LFSR's & their cryptanalysis
 - the limitations of RC4

Important Topics We have Covered

- Block ciphers
 - Feistel network
 - Attacks on DES: brute force (exhaustive key search, dictionary attack), the effectiveness of Linear & Differential analysis
 - 2DES, 3DES
 - encryption modes and their properties: ECB, CBC, CFB, OFB, CTB
 - parameters of AES, IDEA

Important topics for Hash Functions and MAC

- Different security properties of cryptographic hash functions and their relationship
- Merkle-Damgard construction, and its security proof
- Parameters and basic structures of MD5 and SHA-1
- Birthday attacks & choosing length of hash functions
- Concept and security definitions of MAC
- Weakness of certain MAC constructions from collision-resistant Hash functions
- HMAC structure and security properties (no proof required)

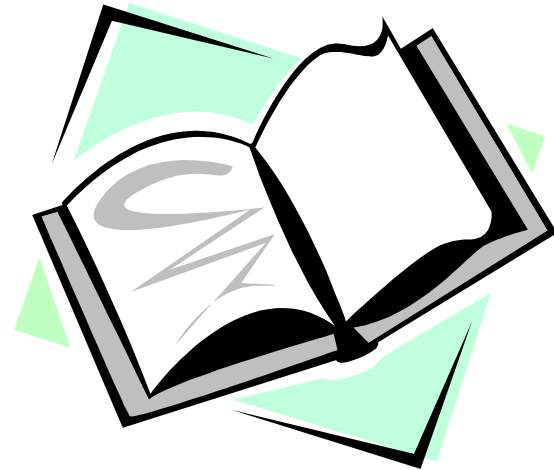
Lecture Outline

- Prime and composite number
- GCD and LCM
- Euclid's algorithm
- Distribution of prime numbers
- Fermat's theorem



Recommended Reading

- Stallings, the number theory chapter
- Wagstaff, Chapters 4 and 5



Divisibility

Definition

Given integers a and b , $b \neq 0$, b divides a (denoted $b|a$) if \exists integer c , s.t. $a = cb$.
 b is called a **divisor** of a .

Theorem (Transitivity)

Given integers a , b , c , all > 1 , with $a|b$ and $b|c$, then $a|c$.

Proof:

$$a | b \Rightarrow \exists m \text{ s.t. } ma = b$$

$$b | c \Rightarrow \exists n \text{ s.t. } nb = c, nma = c,$$

We obtain that $\exists q = mn$, s.t. $c = aq$, so $a | c$

Divisibility (cont.)

Theorem

Given integers a, b, c, x, y all > 1 , with $a|b$ and $a|c$, then $a|bx + cy$.

Proof:

$$a | b \Rightarrow \exists m \text{ s.t. } ma = b$$

$$a | c \Rightarrow \exists n \text{ s.t. } na = c$$

$$bx + cy = a(mx + ny), \text{ therefore } a | bx + cy$$

Divisibility (cont.)

Theorem (Division algorithm)

Given integers $a > 0$, b , $a < b$ then there exists two unique integers q and r , $0 \leq r < a$ s.t. $b = aq + r$.

Proof:

$a < b \Rightarrow b/a = q + n$, such that $0 \leq n < 1$ and q integer
 $b = aq + an = aq + r$, with r integer and $0 \leq r < a$

Uniqueness of q and r :

assume $\exists q'$ and r' s.t $b = aq' + r'$, $0 \leq r' < a$, q' integer

$q - q' = (r' - r)/a$ and $-1 < (r' - r)/a < 1$

So $-1 < q - q' < 1$, but $q - q'$ is integer, therefore

$q = q'$ and $r = r'$

Prime and Composite Numbers

Definition

An integer $n > 1$ is called a **prime number** if its positive divisors are 1 and n .

Definition

Any integer number $n > 1$ that is not prime, is called a **composite number**.

Example

Prime numbers: 2, 3, 5, 7, 11, 13, 17 ...

Composite numbers: 4, 25, 17778, 900, ...

Decomposition in Product of Primes

Theorem (Fundamental Theorem of Arithmetic)

Any integer number $n > 1$ can be written as a product of prime numbers (>1), and the product is unique if the numbers are written in increasing order.

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

Example: $84 = 2^2 \cdot 3 \cdot 7$

Greatest Common Divisor (GCD)

Definition

Given integers $a > 0$ and $b > 0$, we define $\text{gcd}(a, b) = c$, **the greatest common divisor (GCD)**, as the greatest number that divides both a and b .

Example

$$\text{gcd}(256, 100) = 4$$

Definition

Two integers $a > 0$ and $b > 0$ are relatively prime if $\text{gcd}(a, b) = 1$.

Example

25 and 128 are relatively prime.

GCD Theorem

Theorem

$$\begin{array}{l} \text{Given } n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \quad \text{and} \\ m = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k} \quad \text{then} \end{array}$$

where p_i are prime numbers, $0 < i < (k+1)$
then

$$\gcd(n, m) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_k^{\min(e_k, f_k)}$$

GCD as a Linear Combination

Theorem

Given integers $a, b > 0$ and $a > b$, then $d = \gcd(a,b)$ is the least positive integer that can be represented as $ax + by$, x, y integer numbers.

Proof:

Assume t is the smallest integer, $t = ax + by$
 $d \mid a$ and $d \mid b \Rightarrow d \mid ax + by$, so $d \leq t$

$t \mid a$; otherwise, $a = tu + r$, $0 \leq r < t$;
 $r = a - ut = a - u(ax+by) = a(1-ux) + b(-uy)$, so we found another linear combination and $r < t$. Contradiction
Similarly $t \mid b$, so we obtain $t \leq \gcd(a, b) = d$
So $t = d$

Example

$$\gcd(100, 36) = 4 = 4 \times 100 - 11 \times 36 = 400 - 396$$

GCD and Multiplication

Theorem

Given integers $a, b, m > 1$. If
 $\gcd(a, m) = \gcd(b, m) = 1$, then $\gcd(ab, m) = 1$

Proof idea:

$$ax + ym = 1 = bz + tm$$

Find u and v such that $(ab)u + mv = 1$

Example

$$a = 25, b = 8, m = 3$$

$$\gcd(25, 3) = 1$$

$$\gcd(8, 3) = 1$$

$$\gcd(200, 3) = 1$$

GCD and Division

Theorem

If $g = \gcd(a, b)$, where $a > b$, then $\gcd(a/g, b/g) = 1$ (a/g and b/g are relatively prime).

Proof:

Assume $\gcd(a/g, b/g) = d$, then $a/g = md$ and $b/g = nd$.

$a = gmd$ and $b = gnd$, therefore $gd \mid a$ and $gd \mid b$

Therefore $gd \leq g$, $d \leq 1$, so $d = 1$.

Example

$$\gcd(100, 36) = 4$$

$$\gcd(100/4, 36/4) = \gcd(25, 9) = 1$$

GCD and Division

Theorem

Given integers $a > 0$, b , q , r , such that $b = aq + r$, then $\gcd(b, a) = \gcd(a, r)$.

Proof:

$\gcd(b, a) = d$ and $\gcd(a, r) = e$, this means

$d \mid b$ and $d \mid a$, so $d \mid b - aq$, so $d \mid r$
Since $\gcd(a, r) = e$, we obtain $d \leq e$.

$e \mid a$ and $e \mid r$, so $e \mid aq + r$, so $e \mid b$,
Since $\gcd(b, a) = d$, we obtain $e \leq d$.

Therefore $d = e$

Finding GCD

Theorem

Given integers $a > 0$, b , q , r , such that $b = aq + r$, then $\gcd(b, a) = \gcd(a, r)$.

Euclidian Algorithm

Find $\gcd(b, a)$

```
while  $a \neq 0$  do  
     $r \leftarrow b \bmod a$   
     $b \leftarrow a$   
     $a \leftarrow r$   
return  $a$ 
```

QuickTime™ and a TIFF (Uncompressed) decompressor are needed to see this picture.

Euclidian Algorithm Example

Find $\text{gcd}(143, 110)$

$$143 = 1 \times 110 + 33$$

$$110 = 3 \times 33 + 11$$

$$33 = 3 \times 11 + 0$$



$$\text{gcd}(143, 110) = 11$$

LCM Theorem

Definition

Given integers a and b , we define $\text{lcm}(a, b) = c$, the least common multiple, as the smallest positive integer divisible by both a and b .

Theorem

Given $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and
 $m = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$ then

where p_i are prime numbers, $0 < i < (k+1)$
then

$$\text{lcm}(n, m) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \cdots p_k^{\max(e_k, f_k)}$$

GCD and LCM

Theorem

Given integers a , b , then

$$\gcd(a, b) \operatorname{lcm}(a, b) = ab$$

Proof idea:

Use GCD and LCM theorems and
 $\min(x, y) + \max(x, y) = x + y$

Example

$$\gcd(10, 6) = 2$$

$$\operatorname{lcm}(10, 6) = 30$$

Number of Prime Numbers

Theorem

The number of prime numbers is infinite.

Proof:

consider p_1, p_2, \dots, p_k all primes and $n = p_1 p_2 \dots p_k + 1$.

Then exists p prime s.t. $p \mid n$ (fundamental theorem of arithmetic), and p is not one of the p_1, \dots, p_k (otherwise this will mean that $p \mid 1$).

Therefore, p_1, \dots, p_k were not all the prime numbers.

Distribution of Prime Numbers

Theorem (Gaps between primes)

For every positive integer n , there are n or more consecutive composite numbers.

Proof Idea:

Numbers $(n+1)! + 2, (n+1)! + 3, \dots, (n+1)! + n + 1$ are composite

Distribution of Prime Numbers

Definition

Given real number x , then $\pi(x)$ is the number of prime numbers $\leq x$.

Theorem (prime numbers theorem)

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \ln x} = 1$$

For a very large number x , the number of prime numbers smaller than x is $x / \ln x$.

Equivalence Relation

Definition

A relation is defined as any subset of a cartesian product. We denote a relation $(a,b) \in R$ as aRb , $a \in A$ and $b \in B$.

Definition

A relation is an equivalence relation on a set S , if R is

Reflexive: aRa for all $a \in R$

Symmetric: for all $a, b \in R$, $aRb \Rightarrow bRa$.

Transitive: for all $a,b,c \in R$, aRb and $bRc \Rightarrow aRc$

Example

“=” is an equivalence relation on N

Modulo Operation

Definition:

$$a \bmod n = r \Leftrightarrow \exists q, \text{ s.t. } a = q \times n + r$$

where $0 \leq r \leq n - 1$

Example:

$$7 \bmod 3 = 1$$

$$-7 \bmod 3 = 2$$

Definition (Congruence):

$$a \equiv b \pmod{n} \Leftrightarrow a \bmod n = b \bmod n$$

Congruence Relation

Theorem

Congruence mod n is an equivalence relation:

Reflexive: $a \equiv a \pmod{n}$

Symmetric: $a \equiv b \pmod{n}$ iff $b \equiv a \pmod{n}$.

Transitive: $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \Rightarrow$
 $a \equiv c \pmod{n}$

Congruence Relation Properties

Theorem

- 1) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then:
 $a \pm c \equiv b \pm d \pmod{n}$ and
 $ac \equiv bd \pmod{n}$
- 2) If $a \equiv b \pmod{n}$ and $d \mid n$ then:
 $a \equiv b \pmod{d}$
- 3) $a \equiv b \pmod{n}$, $a \equiv b \pmod{m}$ and $\gcd(m, n)=1$, then
 $a \equiv b \pmod{mn}$

Fermat's Theorem

Fermat's Theorem

If p is a prime number and a is a natural number that is not a multiple of p , then

$$a^{p-1} \equiv 1 \pmod{p}$$

Proof idea:

$\gcd(a, p) = 1$, then the set $\{i \cdot a \pmod{p} \mid 0 < i < p\}$ is a permutation of the set $\{1, \dots, p-1\}$. (otherwise we obtain that $p \mid (ma - na)$, $p \mid (m-n)$, where $m-n < p$)

$$a \cdot 2a \cdot \dots \cdot (p-1)a = (p-1)! a^{p-1} \equiv (p-1)! \pmod{p}$$

Since $\gcd((p-1)!, p) = 1$, we obtain $a^{p-1} \equiv 1 \pmod{p}$

Consequence of Fermat's Theorem

Theorem

- p is a prime number and
- a , e and f are positive numbers
- $e \equiv f \pmod{p-1}$ and
- p does not divide a , then

$$a^e \equiv a^f \pmod{p}$$

Proof idea:

$$a^e = a^{q(p-1) + f} = a^f (a^{(p-1)})^q$$

by applying Fermat's theorem we obtain

$$a^e \equiv a^f \pmod{p}$$

Next ...

- Testing for primality
- Euclid's theorem
- Chinese Remainder Theorem
- Discrete logarithm

