

Cryptography CS 555

Lecture 12



Number Theory Basics

Lecture Outline

- Divisibility
- Prime and composite number
- GCD and Euclid's algorithm
- Chinese Remainder Theorem
- Euler Phi function
- Fermat's theorem



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

Proof:

Uniqueness of q and r :

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

then $aq + r = aq' + r' \Rightarrow a(q - q') = r' - r \Rightarrow q - q' = (r' - r)/a$

as $0 \leq r, r' < a \Rightarrow -a < (r' - r) < a \Rightarrow -1 < (r' - r)/a < 1$

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, 6, 25, 900, 17778, ...

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 $\gcd(a, b) = c$, the greatest common divisor (GCD), as the greatest number that divides both a and b .

Example

$$\gcd(256, 100) = 4$$

Definition

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

Example

25 and 128 are relatively prime.

GCD using Prime Decomposition

Theorem

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

where p_i are prime numbers
then

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

Example: $84 = 2^2 \cdot 3 \cdot 7$ $90 = 2 \cdot 3^2 \cdot 5$

$$\gcd(84, 90) = 2^1 \cdot 3^1 \cdot 5^0 \cdot 7^0$$

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: Let t be the smallest integer, $t = ax + by$
 $d \mid a$ and $d \mid b \Rightarrow d \mid ax + by$, so $d \leq t$.

We now show $t \leq d$.

First $t \mid a$; otherwise, $a = tu + r$, $0 < r < t$;

$r = a - ut = a - u(ax+by) = a(1-ux) + b(-uy)$, so we found another linear combination and $r < t$. Contradiction.

Similarly $t \mid b$, so t is a common divisor of a and b , thus

$$t \leq \gcd(a, b) = d. \quad \text{So } t = d.$$

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 $(ab)u + mv = 1$

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:

Let $\gcd(b, a) = d$ 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

Using the 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 $\text{gcd}(143, 110)$

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

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

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

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

Towards Extended Euclidian Algorithm

- **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.
- How to find such x and y ?
- If a and b are relative prime, then there exist x and y such that $ax + by = 1$.
 - In other words, $ax \bmod b = 1$.

Euclidian Algorithm Example

Find $\gcd(143, 111)$

$$143 = 1 \times 111 + 32$$

$$111 = 3 \times 32 + 15$$

$$32 = 2 \times 15 + 2$$

$$15 = 7 \times 2 + 1$$

$$\gcd(143, 111) = 1$$

$$32 = 143 - 1 \times 111$$

$$\begin{aligned} 15 &= 111 - 3 \times 32 \\ &= 4 \times 111 - 3 \times 143 \end{aligned}$$

$$\begin{aligned} 2 &= 32 - 2 \times 15 \\ &= 7 \times 143 - 9 \times 111 \end{aligned}$$

$$\begin{aligned} 1 &= 15 - 7 \times 2 \\ &= 67 \times 111 - 52 \times 143 \end{aligned}$$

Extended Euclidian Algorithm

```
x=1; y=0; d=a; r=0; s=1; t=b;
while (t>0) {
    q = ⌊d/t⌋
    u=x-qr; v=y-qs; w=d-qt
    x=r;    y=s;    d=t
    r=u;    s=v;    t=w
}
return (d, x, y)
```

Invariants:

$$ax + by = d$$

$$ar + bs = t$$

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:

$$a \pm c \equiv b \pm d \pmod{n} \text{ and}$$

$$ac \equiv bd \pmod{n}$$

2) If $a \equiv b \pmod{n}$ and $d \mid n$ then:

$$a \equiv b \pmod{d}$$

Reduced Set of Residues

Definition: A reduced set of residues (RSR) modulo m is a set of integers R each relatively prime to m , so that every integer relatively prime to m is congruent to exactly one integer in R .

The group (\mathbb{Z}_n^*, \times)

- \mathbb{Z}_n^* consists of all integers in $[1..n-1]$ that are relative prime to n
 - $\mathbb{Z}_n^* = \{ a \mid 1 \leq a \leq n \text{ and } \gcd(a, n) = 1 \}$
 - is a reduced set of residues modulo n
 - (\mathbb{Z}_n^*, \times) is a group
 - $\gcd(a, n) = 1$ and $\gcd(b, n) = 1 \Rightarrow \gcd(ab, n) = 1$
 - given $a \in \mathbb{Z}_n^*$, how to compute a^{-1} ?

Linear Equation Modulo

Theorem

If $\gcd(a, n) = 1$, the equation

$$ax \equiv 1 \pmod{n}$$

has a unique solution, $0 < x < n$

Proof Idea:

if $ax_1 \equiv 1 \pmod{n}$ and $ax_2 \equiv 1 \pmod{n}$, then
 $a(x_1 - x_2) \equiv 0 \pmod{n}$, then $n \mid a(x_1 - x_2)$, then
 $n \mid (x_1 - x_2)$, then $x_1 - x_2 = 0$

Linear Equation Modulo (cont.)

Theorem

If $\gcd(a, n) = 1$, the equation

$$ax \equiv b \pmod{n}$$

has a solution.

Proof Idea:

$$x = a^{-1} b \pmod{n}$$

Chinese Remainder Theorem (CRT)

Theorem

Let n_1, n_2, \dots, n_k be integers s.t. $\gcd(n_i, n_j) = 1$,
 $i \neq j$.

$$x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

...

$$x \equiv a_k \pmod{n_k}$$

There exists a unique solution modulo

$$n = n_1 n_2 \dots n_k$$

Proof of CMT

- Consider the function $\chi: \mathbb{Z}_n \rightarrow \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}$
 $\chi(x) = (x \bmod n_1, \dots, x \bmod n_k)$
- We need to prove that χ is a bijection.
- For $1 \leq i \leq k$, define $m_i = n / n_i$, then $\gcd(m_i, n_i) = 1$
- For $1 \leq i \leq k$, define $y_i = m_i^{-1} \bmod n_i$
- Define function $\rho(a_1, a_2, \dots, a_k) = \sum a_i m_i y_i \bmod n$
 - $a_i m_i y_i \equiv a_i \pmod{n_i}$
 - $a_i m_i y_i \equiv 0 \pmod{n_j}$ where $i \neq j$

Proof of CMT

- Example of the mappings: $n_1=3, n_2=5, n=15$

χ :		ρ :	$m_1=5, y_1=2, m_1y_1=10, m_2y_2=6,$	
1	(1,1)	(1,1)	10+6	1
2	(2,2)	(1,2)	10+12	7
4	(1,4)	(1,3)	10+18	13
7	(1,2)	(1,4)	10+24	4
8	(2,3)	(2,1)	20+6	11
11	(2,1)	(2,2)	20+12	2
13	(1,3)	(2,3)	20+18	8
14	(2,4)	(2,4)	20+24	14

Example of CMT:

$$\begin{aligned}x &\equiv 5 \pmod{7} \\x &\equiv 3 \pmod{11} \\x &\equiv 10 \pmod{13}\end{aligned}$$

- $n_1=7, n_2=11, n_3=13, n=1001$
- $m_1=143, m_2=91, m_3=77$
- $y_1=143^{-1} \pmod{7} = 3^{-1} \pmod{7} = 5$
- $y_2=91^{-1} \pmod{11} = 3^{-1} \pmod{11} = 4$
- $y_3=77^{-1} \pmod{13} = 12^{-1} \pmod{13} = 12$

- $x = (5 \times 143 \times 5 + 3 \times 91 \times 4 + 10 \times 77 \times 12) \pmod{1001}$
 $= 13907 \pmod{1001} = 894$

The Euler Phi Function

Definition

Given an integer n , $\Phi(n) = |Z_n^*|$ is the number of all numbers a such that $0 < a < n$ and a is relatively prime to n (i.e., $\gcd(a, n) = 1$).

Theorem:

If $\gcd(m, n) = 1$, $\Phi(mn) = \Phi(m) \Phi(n)$

The Euler Phi Function

Theorem: Formula for $\Phi(n)$

Let p be prime, e, m, n be positive integers

1) $\Phi(p) = p-1$

2) $\Phi(p^e) = p^e - p^{e-1}$

3) If $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ then

$$\Phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

Fermat's Little Theorem

Fermat's Little 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 have $0 < n < m < p$ s.t. $ma \pmod{p} = na \pmod{p}$)

$$p \mid (ma - na) \Rightarrow p \mid (m-n), \text{ where } 0 < m-n < p$$

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

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

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

Euler's Theorem

Euler's Theorem

Given integer $n > 1$, such that $\gcd(a, n) = 1$ then
$$a^{\Phi(n)} \equiv 1 \pmod{n}$$

Corollary

Given integer $n > 1$, such that $\gcd(a, n) = 1$ then
 $a^{\Phi(n)-1} \pmod{n}$ is a multiplicative inverse of $a \pmod{n}$.

Corollary

Given integer $n > 1$, x , y , and a positive integers with
 $\gcd(a, n) = 1$. If $x \equiv y \pmod{\Phi(n)}$, then
$$a^x \equiv a^y \pmod{n}.$$

Next ...

- RSA
- Prime number distribution and testing
- Efficiency of modular arithmetic

