Cristina Nita-Rotaru

CS355: Cryptography

Lecture 11, 12, 13: Number theory.

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.

$$n = p_1^{e_1} p_2^{e2} \ldots p_k^{ek}$$

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

Number of Prime Numbers

Theorem

The number of prime numbers is infinite.

Proof:

consider $p_1, p_2, \ldots p_k$ all existing primes and $n = p_1 p_2 \ldots p_k+1$

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

Therefore, $p_1, \ldots p_k$ 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, …. (n+1)! + n +1 are composite

Distribution of Prime Numbers

Definition

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

Theorem (prime numbers theorem)

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

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

Greatest Common Divisor (GCD)

Definition - GCD

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- Relatively prime

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

Example

25 and 128 are relatively prime.

OBS: $gcd(a, b) \leq a$ and $gcd(a, b) \leq b$

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: We show $d \le t$

Let t be the smallest positive integer s.t. $t = ax + by$.

We have $d \mid a$ and $d \mid b \Rightarrow d \mid ax + by$, so $d \mid t$, so $d \le t$.

We now show $t \le d$.

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 $t \le \gcd(a, b) = d$. 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 $(ab)u + mv = 1$

GCD and Multiplication

Theorem

Given integers a, b, and prime number p. If p | ab then p|a or p|b.

Proof:

Case 1: If p | a then exists k such that a = pk, *then* ab = pkb so p | ab

Case 2: If p not | a. Then gcd(a,p) = 1, so exists x and y such that ax + py = 1, so abx + bpy = b, since p | abx and p | pby, p | (abx + bpy) so p| b.

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 | b and d | a, so d | b - aq , so d | r
Since gcd(a, r) = e, we obtain d ≤ e.

e | a and e | r, so e | aq + r , so e | b,
Since gcd(b, a) = d, we obtain e ≤ d.

Therefore d = e

Cristina Nita-Rotaru

Finding GCD

Using the Theorem: Given integers a>0, b, q, r, such that b = aq + r, then gcd(b, a) = gcd(a, r).

gcd is the last nonzero remainder

Euclidian Algorithm

Find gcd (b, a)

while a $\neq$0 *do*

r $\leftarrow$ b mod a

b $\leftarrow$ a

a $\leftarrow$ r

return b

Euclidian Algorithm Example

Find gcd(143, 110)

$$b = a \times q + r$$

$$143 = 110 \times 1 + 33$$
$$110 = 33 \times 3 + 11$$
$$33 = 11 \times 3 + 0$$

gcd (143, 110) = 11

Example

gcd(482, 1180)

1180 = 482 x 2 + 216

482 = 216 x 2 + 50

216 = 50 x 4 + 16

50 = 16 x 3 + 2

16 = 2 x 8 + 0

gcd (482, 1180) = 2

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?

- Hint: use a modified version of the Euclidian algorithm

Iterative method

$1180 = 2 \times 482 + 216$

$482 = 2 \times 216 + 50$

$216 = 4 \times 50 + 16$

$50 = 3 \times 16 + 2$

$16 = 8 \times 2 + 0$

gcd (482, 1180) = 2

How to write 2 as a function of 1180 and 482

$q_1 = 2$
$q_2 = 2$
$q_3 = 4$
$q_4 = 3$
$q_5 = 8$

$x_0 = 0, y_0 = 1$
$x_1 = 1, y_1 = 0$
$x_j = -q_{j-1}x_{j-1} + x_{j-2}$
$y_j = -q_{j-1}y_{j-1} + y_{j-2}$
$ax_n + by_n = gcd(a,b)$

$x_2 = -q_1 x_1 + x_0 = -2$
$x_3 = -q_2 x_2 + x_1 = -2 (-2) + 1 = 5$
$x_4 = -q_3 x_3 + x_2 = -4x5 + (-2) = -22$
$x_5 = -q_4 x_4 + x_3 = -3 (-22) + 5 = 71$

Compute y_5

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:

$ax + by = d$

$ar + bs = t$

Are we there yet?

- Solving linear equations
- CRT

Modulo Operation

Definition:

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

$$\underline{\text{where } 0 \le r \le n-1}$$

Example:

7 mod 3 = 1, 7 = 3 x 2 + 1

-7 mod 3 = 2, -7 = -3 x 3 + 2

Congrent Modulo n

$$a \equiv b \bmod n \Leftrightarrow a \bmod n = b \bmod n$$

a - b is a multiple of n
n | (a-b)
a = nk + b, for some k

- Examples:
- 32 ≡ 7 mod 5

Congruence Relation

Theorem

Congruence mod n is an equivalence relation:

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

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

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

$a \equiv c \pmod{n}$

Congruence Relation Properties

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
   $a \equiv b \pmod{mn}$

Linear Equation Modulo n

If **gcd(a, n) = 1**, the equation

$$ax \equiv 1 \bmod n$$

has a unique solution, $0 < x < n$. This solution is often represented as $a^{-1} \bmod n$

Proof: 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 $x_1-x_2=0$

How to compute x?
as + nt = 1, as = -t*n +1, so s is a solution

Examples

- Solve

$2x \equiv 1 \bmod 3$

$3x \equiv 1 \bmod 7$

$4x \equiv 1 \bmod 5$

$6x \equiv 3 \bmod 3$

Linear Equation Modulo (cont.)

If **gcd(a, n) = d**, the equation

$$ax \equiv b \bmod n$$

has a solution **iff d | b**.

Proof Sketch:
“=>” exists x such that
ax = qn + b; b = ax - qn
d divides a and n, so divides any linear combination, so d | b

“<=” d | b then b = dt, by theorem we have d = au + sn, so dt = a (ut) + s(nt) = b, so x = ut is a solution of $ax \equiv b \bmod n$

Examples

- Which equations have solutions?
- $6x \equiv 3 \mod 3$
- $6x \equiv 2 \mod 3$

- $6x \equiv 2 \mod 2$
- $6x \equiv 2 \mod 4$

- $482x \equiv 2 \mod 1180$
- $71 \times 482 + 1180 (-29) = 1$
- $71 \times 1 = 71$ is a solution

Solving Linear Equation Modulo

To solve the equation

$$ax \equiv b \bmod n$$

When gcd(a,n)=1, compute x = a^{-1} b mod n.
When gcd(a,n) = d >1, do the following

- If d does not divide b, there is no solution.
- Assume d|b. Solve the new congruence, get x_0

$$(a/d)x \equiv b/d \pmod{n/d}$$

- The solutions of the original congruence are x_0, x_0+(n/d), x_0+2(n/d), …, x_0+(d-1)(n/d) (mod n).

Examples

- $2x \equiv 3 \bmod 5$
- Compute 2^{-1}, by solving $2x \equiv 1 \bmod 5$
- 2^{-1} with respect to multiplication mod 5 is 3
- $x = 3 \times 3 \bmod 5$, $x = 4$

- $6x \equiv 2 \bmod 4$
- $3x \equiv 1 \bmod 2$, $x_0 = 1$
- Solution is $x_0 + 4/2$, $x_0 + 2 \times 4/2$ so on mod 4
- 3, 5, 7 solutions mod 4

Chinese Reminder Theorem

Theorem

Let m, and n be integers s.t. gcd(m, n) = 1.

$$x \equiv a \mod m$$

$$x \equiv b \mod n$$

There exists a unique solution modulo mn

Cristina Nita-Rotaru

Chinese Reminder Theorem

gcd(m, n) = 1, then there exist integers s and t such that ms +nt=1; Note that ms ≡ 1 mod n and nt ≡ 1 mod m

Idea is to show that x = bms + ant is a solution congruent to both eq.

(bms + ant) mod m ≡ ant mod m ≡ a mod m
(bms + ant) mod n ≡ bms mod n ≡ b mod n

Assume that there are two solutions x and y then we obtain

x ≡ y mod m and x ≡ y mod n, so x-y is a multiple of both m and n, so a multiple of mn

So x ≡ y mod mn

Example of CRT

Solve x ≡ 3 mod 7 and x ≡ 5 mod 15

Since 80 ≡ 3 mod 7 and 80 ≡ 3 mod 15, then 80 is a solution, solution is uniquely determined modulo 7 * 17 = 105

How to do it: list all numbers modulo that are 5 modulo15 then check which ones are 3 modulo 7.

Or solve the extended euclidian algorithm, get s and t, then compute the solution x = bms + amt

Chinese Reminder Theorem (CRT)

Theorem

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

$$x \equiv a_1 \bmod n_1$$

$$x \equiv a_2 \bmod n_2$$

$$\ldots$$

$$x \equiv a_k \bmod n_k$$

There exists a unique solution modulo

$n = n_1 \, n_2 \ldots n_k$

Are we there yet?

- Fermat's Little Theorem

The Euler Phi Function

Definition

Given an integer n, $\Phi(n)$ 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 Φ(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 $n = p_1^{e_1} p_2^{e2} \ldots p_k^{ek}$ then

$$\Phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\ldots(1 - \frac{1}{p_k})$$

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 · a mod p} 0< i < p is a permutation of the set {1, …, p-1}.
  - otherwise we have 0<n<m<p s.t. ma mod p = na mod p, and thus p| (ma - na) ⇒ p | (m-n), where 0<m-n < p)
- $a \times 2a \times \ldots \times (p-1)a = (p-1)!\, a^{p-1} \equiv (p-1)! \pmod{p}$

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

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 $a^{\Phi(n)-1} \bmod n$ is a multiplicative inverse of a mod 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

$$a^x \equiv a^y \pmod{n}.$$

Consequence of Euler's Theorem

Principle of Modular Exponentiation

Given a, n, x, y with $n \geq 1$ and $\gcd(a,n)=1$, if $x \equiv y \pmod{\phi(n)}$, then

$$a^x \equiv a^y \pmod{n}$$

Proof idea:

$a^x = a^{k\phi(n) + y} = a^y (a^{\phi(n)})^k$

by applying Euler's theorem we obtain

$a^x \equiv a^y \pmod{p}$

Groups

Definition

A *group* $(G, *)$ is a set G on which a binary operation is defined which satisfies the following axioms:

Closure: For all $a, b \in G, a * b \in G$.

Associative: For all $a, b, c \in G, (a * b) * c = a * (b * c)$.

Identity: $\exists$ e $\in G$ s.t. for all $a \in G, a * e = a = e * a$.

Inverse: For all $a \in G, \exists a^{-1} \in G$ s. t. $a * a^{-1} = a^{-1} * a = e$.

Example

$(Z_n, +)$ is a group, where + is addition modulo n

$(Z_{p, *})$ = is a group, where * is multiplication modulo p

Groups (cont.)

Definition:

A group $(G, *)$ is called an *abelian group* if operation $*$ is a commutative operation:

Commutative: For all $a, b \in G$, $a * b = b * a$.

Example:

(R, +) is an abelian group

Definition

A group G is *cyclic* if ∃ g ∈G s.t. any h ∈G can be writen $h = g^i$.

g is called group generator.

Example

Cyclic groups: $(Z_2, *)$, $(Z_3, *)$

Order of a Group

Definition

The *order* of a group G, ord(G), is defined as the number of elements in the group.

Definition

A group G is *finite,* if |G| = ord(G), is finite.

We can show that the order of (Z_n, *) is $\Phi(n)$

Example:

What is the order of (Z^*_7, *), (Z^*_{700}, *) ?

Order of an Element

Definition

The *order of an element g* from a finite group G, is the smallest power of *n* such that $g^n=e$, where *e* is the identity element.

Example:

What is the order of 2 in $(Z^*_5, *)$?

It is 4 because $2^4 \equiv 1 \bmod 5$

What is the order of 3 in $(Z^*_{10}, *)$?

It is 4 because $3^4 \equiv 1 \bmod 10$

OBS: order of an element modulo n =< $\Phi(n)$

Primitive Root

Definition

An integer g whose order modulo n is $\Phi(n)$ is called a primitive root modulo n.

Example

$(Z_7^*, *)$, $5^6 \equiv 1 \bmod 7$ and $\Phi(7) = 6$

$5^6 = 15625$

$(Z_8^*, *)$ does not have a primitive root

FACT

The group $G = \langle Z_n^*, * \rangle$ has primitive roots only if n is 2, 4, p^t or $2p^t$ where p is an odd integer.

Primitive Roots and Cyclic Groups

FACT

If a group (Z_n*, *) has a primitive root, it is cyclic. Each primitive root is a generator and can be used to create the whole set. $Z_n^* = \{g_1, g^2, \ldots g^{\Phi(n)}\}$

FACT

If the group (Z_n*, *) has any primitive root, the number of primitive roots is $\Phi(\Phi(n))$

OBSERVATION

(Z_n*, *) is cyclic if it has primitive roots

(Z_p*, *) is always cyclic

Discrete Logarithm

Definition

Let G = (Z_n^*, *) be a cyclic group with generator (primitive root) g. Then every element a of G can be written as $g^k \equiv a \mod n$.

k is called the index of a base g modulo n, or the discrete logarithm of a to base g modulo n.

Discrete logarithms behave similar with traditional logarithms.

$\log_g 1 \equiv 0 \mod \Phi(n)$

$\log_g xy \equiv (\log_g x + \log_g y) \mod \Phi(n)$

$\log_g x^k \equiv k \log_g y \mod \Phi(n)$