UNIVERSIDAD NACIONAL DE COLOMBIA

Introducción a la Criptografía y a la Seguridad de la Información

Sesión 5

Number Theory Background

Yoan Pinzón

Session 5

- **Number Theory Background**
  - ▷ Division Theorem
  - ▷ Congruent Modulo n
  - ▷ Equivalent Class Modulo n
  - ▷ Integer Modulo n ($\mathbb{Z}_n$)
  - ▷ Multiplicative Inverse
  - ▷ Factorization
  - ▷ GCD
  - ▷ Relatively Prime
  - ▷ Multiplicative Group of $\mathbb{Z}_n$
  - ▷ Euler's Theorem
  - ▷ Fermat's Little Theorem
  - ▷ EEA - Extended Euclidean Algorithm
  - ▷ PowerMod
  - ▷ CRT - Chinese Remainder Theorem
  - ▷ The Order of an Integer
  - ▷ Primitive Elements in $\mathbb{Z}_p^*$

Division Theorem

$\forall a, b \in \mathbb{Z}, \exists$ unique $q, r \in \mathbb{Z} : a = qb + r, 0 \leq r \leq |b|$.

- $q = \lfloor a/b \rfloor$ is called **quotient** of the division.
- $r = a \bmod b$ and is called **remainder** (or **residue**).

Example: $a = 36,\ b = 16$

$$a = qb + r$$

$$36 = 2 \cdot 16 + 4$$

$q = 2, r = 4$

$a\|b$ (read a divides b), if $\exists\, c \in \mathbb{Z} : b = a \cdot c$.

Divisor, GCD, Prime, Composite

Divisor: c is a common divisor of a, b if $c|a \wedge c|b$.

Greatest Common Divisor (GCD): $d = \gcd(a, b)$ if d is a common divisor of a and b, and $\forall c, c|a \wedge c|b \wedge c|d$, Note that $d \geq 1$.

The integer $p > 1$ is a **prime** if its only divisors are 1 and p.

An integer $a > 1$ that is not a prime is called a **composite number** (or a **composite**).

Integer 1 (one) is neither prime nor composite but a *unit*.

Integer 2 (two) is a prime (the only even one).

Congruent Modulo n

$$a \equiv b \pmod{n} \text{ iff } \begin{cases} n|(a-b) \\ a \bmod n = b \bmod n \end{cases}$$

Proof:

$$\begin{aligned} a \bmod n &= b \bmod n \\ a - kn &= b - k'n \\ a - b &= k''n \qquad \Rightarrow \quad n|(a-b) \end{aligned}$$

$a \bmod n =$
$a - n\lfloor a/n \rfloor =$
$a - nk$

$\square$

Example: $24 \equiv 9 \pmod{5}$

$$a = b \bmod n \quad \Rightarrow \quad a \equiv b \pmod{n}$$
$$a \equiv b \pmod{n} \quad \not\Rightarrow \quad a = b \bmod n$$

Equivalence Class Modulo n

$$[r]_n = \{r + kn : k \in \mathbb{Z}\}$$

Example:

$[0]_7 = \{\cdots, -21, -14, -7, 0, 7, 14, \cdots\}$
$[1]_7 = \{\cdots, -20, -13, -6, 1, 8, 15, \cdots\}$
$[2]_7 = \{\cdots, -19, -12, -5, 2, 9, 16, \cdots\}$
$[3]_7 = \{\cdots, -18, -11, -4, 3, 10, 17, \cdots\}$
$[4]_7 = \{\cdots, -17, -10, -3, 4, 11, 18, \cdots\}$
$[5]_7 = \{\cdots, -16, -9, -2, 5, 12, 19, \cdots\}$
$[6]_7 = \{\cdots, -15, -8, -1, 6, 13, 20, \cdots\}$

$a \in [b]_n$ is equivalent to writing $a \equiv b(\bmod n)$.

Integers Modulo n ($\mathbb{Z}_n$)

$$\mathbb{Z}_n = \{[r]_n : 0 \le r \le n-1\} = \{0, 1, 2, \cdots, n-1\}$$

Example:

$\mathbb{Z}_3 = \{0, 1, 2\}$
$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
$\mathbb{Z}_{14} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$
$\mathbb{Z}_{18} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17\}$

Multiplicative Inverse

$$x \in \mathbb{Z}_n \text{ s.t. } ax \equiv 1 \pmod{n}$$

x is denoted by a^-1

Example: $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, $3x \equiv 1 \pmod{4}$, $\boxed{x{=}3}$

Fact 1: $a \in \mathbb{Z}_n$; a is invertible iff $\gcd(a, n) = 1$

$$\begin{array}{lrcl} (\Leftarrow) & ax + ny & = & 1 \\ & n(-y) & = & ax - 1 \quad \rightarrow \quad n|(ax-1) \quad \rightarrow \quad ax \equiv 1 (\text{mod } n). \end{array}$$
$\square$

Exercise: in $\mathbb{Z}_9$ which integers are invertible and what are their inverses.

Factorization

$n \geq 2$ has a *unique* factorization as a product of distinct prime powers.

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},\ p_i = \text{prime},\ e_i \in \mathbb{Z}^+ \quad 1 \leq i \leq k$$

Example: 24

$$\begin{array}{r|l} 24 & 2 \\ 12 & 2 \\ 6 & 2 \\ 3 & 3 \\ 1 & \end{array}$$

$24 = 2^3 3^1$

GCD

$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$
$b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$

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

Example: Compute $gcd(210, 126)$

$$\begin{array}{r|l} 210 & 2 \\ 105 & 3 \\ 35 & 5 \\ 7 & 7 \\ 1 & \end{array} \qquad 210 = 2^1 3^1 5^1 7^1 \qquad \begin{array}{r|l} 126 & 2 \\ 63 & 3 \\ 21 & 3 \\ 7 & 7 \\ 1 & \end{array} \qquad 126 = 2^1 3^2 7^1$$

$\text{gcd}(210, 126) = 2^1 3^1 5^0 7^1 = 2 \cdot 3 \cdot 7 = 42$

Relatively Prime

Two integers a, b are called **relatively prime** if gcd$(a, b) = 1$

Example:

- 234 and 67 are relatively prime because gcd$(234, 67) = 1$
- 321 and 34 are relatively prime because gcd$(321, 34) = 1$
- 762 and 105 are NOT relatively prime because gcd$(762, 105) = 3$

Exercise: Are 123 and 45 relatively prime?

Multiplicative Group of $\mathbb{Z}_n$

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : \text{gcd}(a, n) = 1\}$$

$\phi(n)$=$|\mathbb{Z}_n^*|$= number of integers $[0, n-1]$ which are relatively prime to n

a) $\phi(p) = p - 1$ if p is prime

b) $\phi(nm) = \phi(n)\phi(m)$ if gcd$(n, m) = 1$

c) $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$ if $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$

Example: Find $\phi(21)$

$\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$, $\phi(21) = \phi(3)\phi(7) = 12$

Euler's Theorem

$$\text{if } a \in \mathbb{Z}_n^*,\ a^{\phi(n)} \equiv 1 \pmod{n}$$

Proof:

$g^{\phi(n)} \equiv 1 \pmod{n}$

$a \in \mathbb{Z}_n^* \Rightarrow \exists x : a \equiv g^x \pmod{n}$

$a^{\phi(n)} \equiv (g^x)^{\phi(n)} \pmod{n} \equiv (g^{\phi(n)})^x \equiv 1 \pmod{n}$

$\square$

Fermat's Little Theorem

$$\text{if } \gcd(a, p) = 1,\ a^{p-1} \equiv 1 \pmod{p}$$

p is prime.

Proof:

Using Euler's Theorem

$\square$

EEA - Extended Euclidean Algorithm

INPUT: $a, b \in \mathbb{Z}^+$, $a \geq b$
OUTPUT: (d, x, y), d=gcd(a, b), $x, y \in \mathbb{Z} : ax + by = d$

Pseudo-code:

```
procedure EEA(a,b)     { q ← ⌊a/b⌋ }
begin
    if b=0 then return (a,1,0)
    (d',x',y') ← EEA(b, a mod b)
    (d,x,y) ← (d',y',x' − qy')
    return (d,x,y)
end
```


EEA - Extended Euclidean Algorithm

Example

Compute EEA(372, 321)

a	b	q	d	x	y	
372	321	1	3	-44	51	$\triangleright$ $-44 \times 372 + 51 \times 321 = 3$
321	51	6	3	7	-44	$\triangleright$ $7 \times 321 + -44 \times 51 = 3$
51	15	3	3	-2	7	$\triangleright$ $-2 \times 51 + 7 \times 15 = 3$
15	6	2	3	1	-2	$\triangleright$ $1 \times 15 + -2 \times 6 = 3$
6	3	2	3	0	1	$\triangleright$ $0 \times 6 + 1 \times 3 = 3$
3	0	–	3	1	0	$\triangleright$ $1 \times 3 + 0 \times 0 = 3$

PowerMod - Modular Exponentiation

INPUT: $a, b, n \in \mathbb{Z}$
OUTPUT: $z = a^b \bmod n$

Pseudo-code:

```
procedure PowerMod(a, b, n)     { ⟨b_k, b_{k-1}, ..., b_0⟩_2 ← b,  z ← 1 }
begin
    for i ← k downto 0 do
        if b_i=1 then z ← (z^2 × a) mod  n
        else z ← z^2  mod  n
    od
return z
end
```


PowerMod - Modular Exponentiation

Example

Compute PowerMod(5,18,17)

$a = 5$
$b = 18_{10} = \langle 10010 \rangle_2$
$n = 17$

i	4	3	2	1	0
b_i	1	0	0	1	0
z	5	8	13	12	8

Then $5^{18} \bmod 17 = 8$

Exercise: Compute PowerMod(7,452,31)

CRT - Chinese Remainder Theorem

The following problem was posed by Sunzi [Sun Tsu] (4th century AD) in the book Sunzi Suanjing:

> *"There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the number?"*

CRT was commonly known as General Sun counting the soldiers or General Han counting the soldiers.

Oystein Ore mentions another puzzle with a dramatic element from Brahma-Sphuta-Siddhanta (Brahma's Correct System) by Brahmagupta (born 598 AD):

> *"An old woman goes to market and a horse steps on her basket and crashes the eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same happened when she picked them out three, four, five, and six at a time, but when she took them seven at a time they came out even. What is the smallest number of eggs she could have had?"*

Problems of this kind are all examples of CRT

CRT - Definition

Let $n_1, n_2, \ldots, n_k$ be *pairwise relatively prime* integers. If $a_1, a_2, \ldots, a_k$ are any integers, then the system of simultaneous congruences

$$x \equiv a_i \pmod{n_i} \quad \forall i \in \{1 \ldots k\}$$

has a unique solution modulo $N = n_1 n_2 \ldots n_k$

$$x = \sum_{i=1}^{k} N_i y_i a_i \bmod N$$

where N_i=N/n_i and y_i=$N_i^{-1} \bmod n_i$

Example

k=2, n_1=5, n_2=3

N=$n_1 n_2$=5×3=15

$\pi(x)$=(x mod 5, x mod 3) : $\mathbb{Z}_{15} \rightarrow \mathbb{Z}_5 \times \mathbb{Z}_3$

x	0	1	2	3	4	5	6	7
$\pi(x)$	(0,0)	(1,1)	(2,2)	(3,0)	(4,1)	(0,2)	(1,0)	(2,1)

x	8	9	10	11	12	13	14
$\pi(x)$	(3,2)	(4,0)	(0,1)	(1,2)	(2,0)	(3,1)	(4,2)

	0	1	2
0	0	10	5
1	6	1	11
2	12	7	2
3	3	13	8
4	9	4	14

$N_1 = N/n_1 = 15/5 = 3$
$N_2 = N/n_2 = 15/3 = 5$

$y_1 = N_1^{-1} \bmod n_1 = 3^{-1} \bmod 5 = 2$
$y_2 = N_2^{-1} \bmod n_2 = 5^{-1} \bmod 3 = 2$

$$\begin{aligned} x = \pi^{-1}(a_1, a_2) &= (N_1 y_1 a_1 + N_2 y_2 a_2) \bmod N \\ &= (3 \times 2a_1 + 5 \times 2a_2) \bmod 15 \\ &= (6a_1 + 10a_2) \bmod 15 \end{aligned}$$

for a_1=1 and a_2=2 we get

$x \equiv 1 \pmod 5$
$x \equiv 2 \pmod 3$

$$\begin{aligned} x = \pi^{-1}(1, 2) &= (6 \times 1 + 10 \times 2) \bmod 15 \\ &= (6 + 20) \bmod 15 \\ &= 26 \bmod 15 \\ &= 11 \end{aligned}$$

11 mod 5 = 1
11 mod 3 = 2

The Order of an Integer

Let $a \in \mathbb{Z}_n^*$.

$$\text{ord}(a) = \min(t : a^t \equiv 1 \pmod n\ )$$

Exercise: Find the order of 5 with the following moduli

i) 7
ii) 11
iii) 21

Primitive elements in $\mathbb{Z}_p^*$

for p=prime, α is called a **primitive element modulo p** if

$$\mathbb{Z}_p^* = \{\alpha^i \bmod p : i \in \mathbb{Z}_p^*\}$$

Example

For p=13 find all the possible *primitive elements modulo 13*.

t	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
2^t mod 13	2	4	8	3	6	12	11	9	5	10	7	1
3^t mod 13	3	9	1	3	9	1	3	9	1	3	9	1
4^t mod 13	4	3	12	9	10	1	4	3	12	9	10	1
5^t mod 13	5	12	8	1	5	12	8	1	5	12	8	1
6^t mod 13	6	10	8	9	2	12	7	3	5	4	11	1
7^t mod 13	7	10	5	9	11	12	6	3	8	4	2	1
8^t mod 13	8	12	5	1	8	12	5	1	8	12	5	1
9^t mod 13	9	3	1	9	3	1	9	3	1	9	3	1
10^t mod 13	10	9	12	3	4	1	10	9	12	3	4	1
11^t mod 13	11	4	5	3	7	12	2	9	6	8	10	1
12^t mod 13	12	1	12	1	12	1	12	1	12	1	12	1

a	1	2	3	4	5	6	7	8	9	10	11	12
ord(a)	1	**12**	3	6	4	**12**	**12**	4	3	6	**12**	2

Hence, the *primitive elements modulo 13* are 2, 6, 7 and 11.