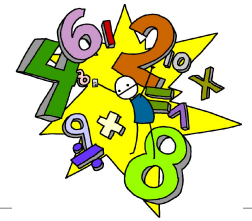
Chapter 2c

TOÁN HỌC DÙNG CHO MẬT MÃ

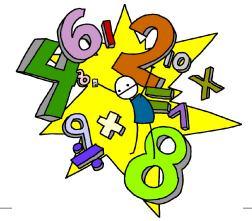
MATHEMATICS OF CRYPTOGRAPHY

Nội dung



- Số học số nguyên (Integer Arithmetic)
  - Phép chia hết
  - Giải thuật Euclid tìm gcd
- Số học đồng dư (Modular Arithmetic)
  - Các lớp đồng dư
  - Nghịch đảo cộng và nhân modulo n

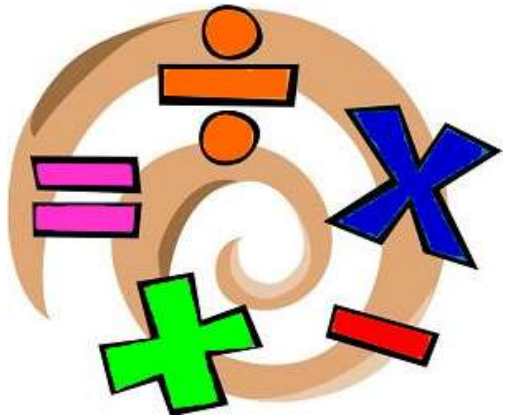
Nội dung



- Algebraic structures
  - Group và Field
  - GF(2) và GF(2^n)
- Số nguyên tố (prime)
  - Hàm Phi Euler
  - Định lý Fermat và Euler
- Các bài toán khó giải

Dẫn nhập

- Lý thuyết mật mã sử dụng và gắn liền với rất nhiều kiến thức toán học, bao gồm:
  - Lý thuyết số
  - Lý thuyết thông tin
  - Độ phức tạp tính toán
  - Thống kê
  - Tổ hợp.



Phần I : Integer Arithmetic

Số học số nguyên
Integer Arithmetic

- Tập các số nguyên

$$Z = \{...., -2,-1,0,1,2,...\}$$

- Tập các số nguyên không âm

$$Z+ = \{0,1,2,...\}$$

- Tập các số tự nhiên

$$N= \{0,1,2,...\}$$

- Tập các số tự nhiên khác không

$$N+ = N \setminus \{0\}$$

Tính chia hết của các số nguyên

- Tập Z là đóng kín với các phép toán +, - và * nhưng không đóng kín với phép chia
  - Phép cộng a+b
  - Phép trừ a – b
  - Phép nhân a * b

  } kết quả là 1 số nguyên $\in Z$
  - Nhưng phép chia a /b có thể không là 1 số nguyên

Tính chia hết của các số nguyên

- Cho a và b là các số nguyên (integer) với $b \neq 0$. Ta nói a chia hết cho b nếu tồn tại 1 số nguyên c sao cho:

$$a = bc$$

- Ký hiệu $b \mid a$ để chỉ a chia hết cho b.
- Ký hiệu $b \nmid a$ để chỉ a không chia hết cho b.
- a là bội số của b (multiple), b là ước số (divisor) của a
- Ví dụ: $2 \mid 6$, $3 \nmid 5$

Định lý phép chia của Euclid

- Đối với mọi số n, d ∈ Z\{0} luôn tồn tại duy nhất các số q, r ∈ Z sao cho

$$\mathbf{n = qd + r} \text{ với } 0 \leq r < |d|$$

- n là số bị chia (dividend), d là số chia (divisor), q là thương số (quotient) và r là số dư (remainder) ký hiệu là $R_d(n)$
- Ví dụ : $R_7(16) = 2$ (vì $16 = 2 \times 7+2$)

$R_7(-16) =$?? 5 (vì $-16 = -3 \times 7+5$)

$R_7(1) = R_7(8) = R_7(15) = R_7(22)... = 1.$

Lưu ý

- Khi chúng ra tính bằng máy tính hoặc máy tính tay, r và q ra số âm (negative) khi a là số âm. Làm thế nào để chúng ra có thể ngăn chăn điều này bởi vì r phải là số không âm?
- Giải pháp rất đơn giản, chúng ta giảm giá trị của q bởi 1 và chúng ta có thêm giá trị của n thêm r để làm cho nó dương.

$$-255 = (-\mathbf{23} \times 11) + (-\mathbf{2}) \quad \leftrightarrow \quad -255 = (-\mathbf{24} \times 11) + \mathbf{9}$$

Ước số chung lớn nhất (Greatest Common Divisor –gcd)

- Cho hai số a, b ∈ Z \{0}, c ∈ Z là ước số chung (common divisor) của a và b nếu c|a và c|b
- C được gọi là ước số chung lớn nhất (greatest common divisor), ký hiệu gcd(a, b), ***nếu nó là số nguyên lớn nhất được chia hết bởi cả a và b***.
- Ví dụ: gcd(12,18) =6, gcd(-18,27) = 9

Thuật toán Euclid tìm gcd

- Thuật toán dựa trên 2 lập luận:

  gcd (a, 0) = a

  gcd (a, b) = gcd (b, r),

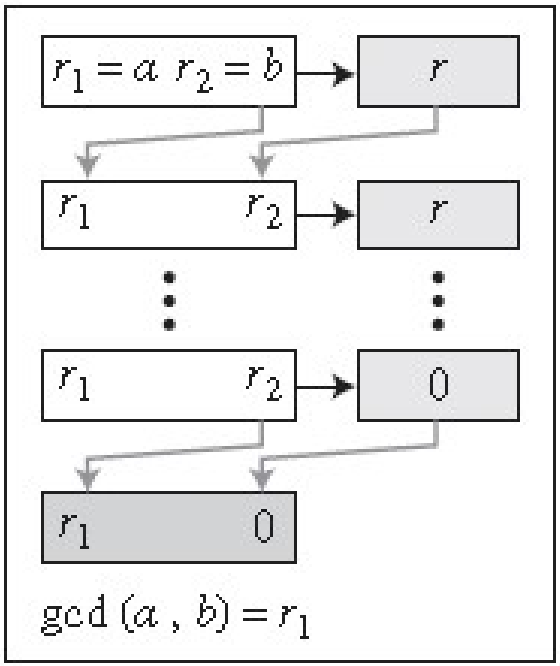
với r là phần dư của a chia cho b

Ví dụ:

$$\gcd(36, 10) = \gcd(10, 6) = \gcd(6, 4) = \gcd(4, 2) = \gcd(2, 0) = 2$$

→ để tính gcd(36,10), ta chỉ cần tìm gcd(2,0)

Thuật toán Euclid tìm gcd(a,b)



a. Process

```
r1 = a; r2 = b;   (Initialization)
while (r2 > 0)
  {
   q = r1 / r2;
   r = r1 - q * r2;
   r1 = r2; r2 = r;
  }

  gcd (a, b) = r1
```

b. Algorithm

Ví dụ: Tìm gcd(2740,1760)

q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	20	0	

➔ gcd (2740, 1760) = 20

Ví dụ: Tìm gcd(25,60)

q	r_1	r_2	r
0	25	60	25
2	60	25	10
2	25	10	5
2	10	5	0
	5	0	

- → gcd(25,60)=5

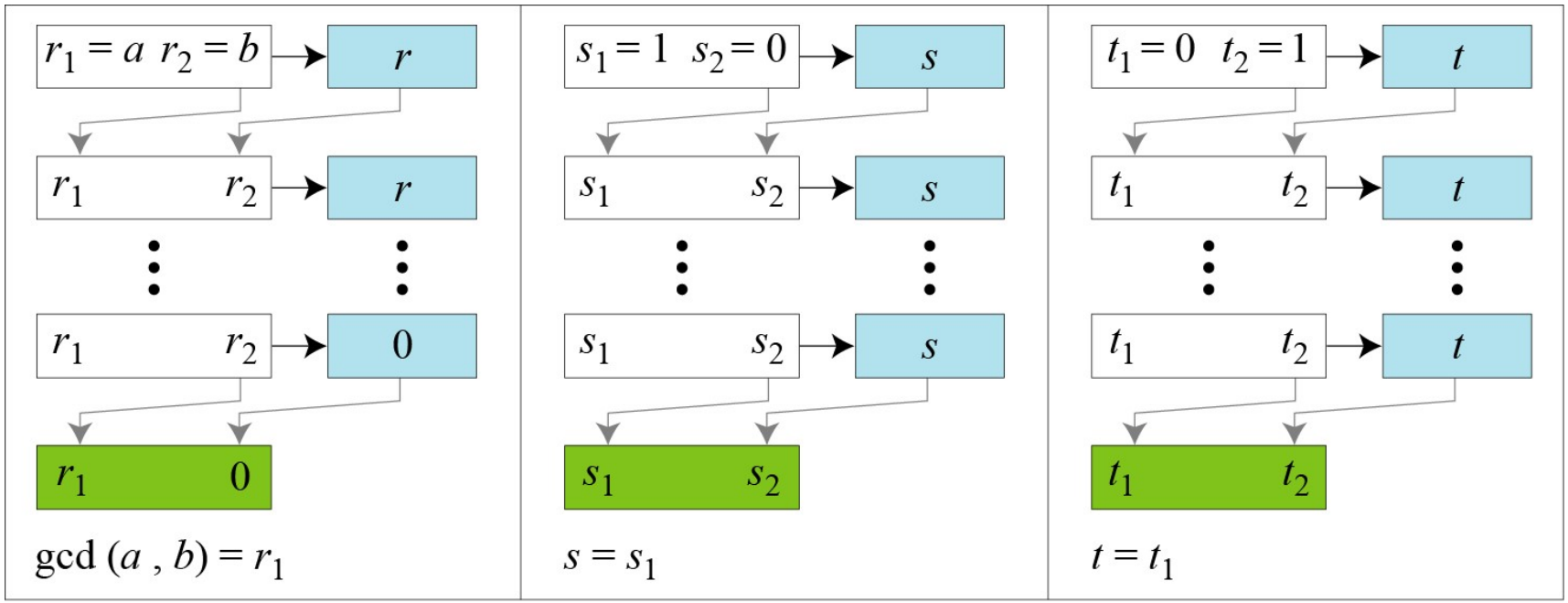
Thuật toán Euclid mở rộng (extended Euclidean algorithm)

- Cho 2 số nguyên a và b, tìm 2 số nguyên khác s và t sao cho:

$$s \times a + t \times b = \gcd(a, b)$$

- Thuật toán này vừa có thể tính được gcd(a,b) vừa tính được các giá trị s và t

Thuật toán Euclid mở rộng (extended Euclidean algorithm)



a. Process

Thuật toán Euclid mở rộng (extended Euclidean algorithm)

$r_1 \leftarrow a;$ $r_2 \leftarrow b;$
$s_1 \leftarrow 1;$ $s_2 \leftarrow 0;$
$t_1 \leftarrow 0;$ $t_2 \leftarrow 1;$ (Initialization)

while $(r_2 > 0)$
{
$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$
$r_1 \leftarrow r_2;$ $r_2 \leftarrow r;$ (Updating r's)

$s \leftarrow s_1 - q \times s_2;$
$s_1 \leftarrow s_2;$ $s_2 \leftarrow s;$ (Updating s's)

$t \leftarrow t_1 - q \times t_2;$
$t_1 \leftarrow t_2;$ $t_2 \leftarrow$ t; (Updating t's)

}
gcd $(a, b) \leftarrow r_1;$ $s \leftarrow s_1;$ $t \leftarrow t_1$

b. Algorithm

Ví dụ:
a = 161 và b = 28, tìm gcd (a, b) và giá trị s và t.

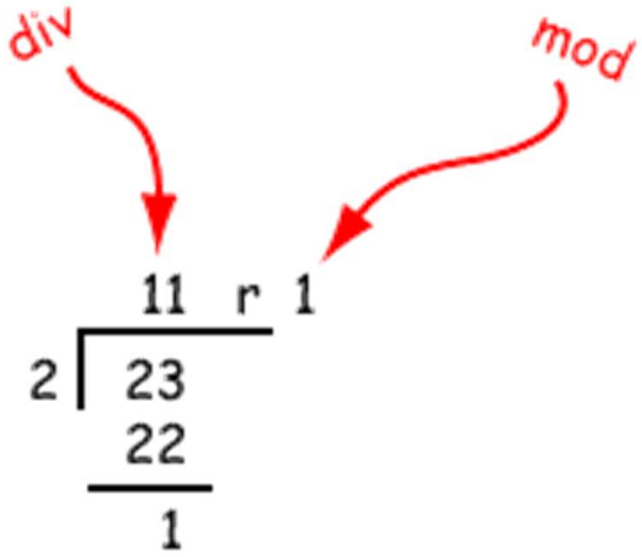
Giải: $r = r_1 - q \times r_2$; $s = s_1 - q \times s_2$; $t = t_1 - q \times t_2$

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
5	161	28	21	1	0	1	0	1	−5
1	28	21	7	0	1	−1	1	−5	6
3	21	7	0	1	−1	4	−5	6	−23
	7	0		**−1**	4		**6**	−23	

→ gcd (161, 28) = 7, s = −1 và t = 6.

Nguyên tố cùng nhau
(co-prime hay relatively prime)

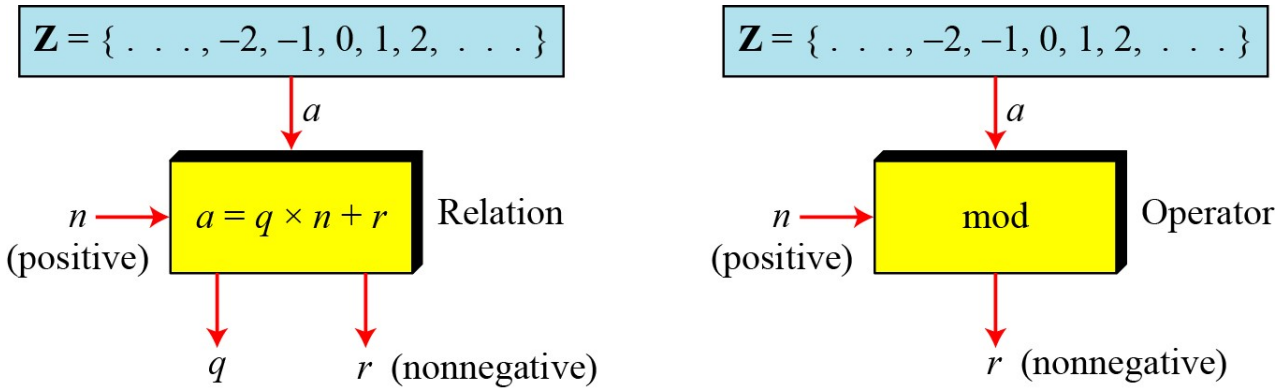
- Hai số nguyên a, b ∈ Z \{0} được gọi là **nguyên tố cùng nhau nếu gcd(a, b)=1**.
- Ví dụ: (5,8) , (9,14) là các cặp nguyên tố cùng nhau



Phần ii: Modular Arithmetic

Modulo Operator

- Phép modulo được ký hiệu là mod. Ngõ ra r được gọi là thặng dư (residue).



Đồng dư theo modular (modular congruence)

- Cho hai số a, b ∈ Z và n ∈ N. Số a được gọi là đồng dư (congruent) với b theo modulo n nếu $n \mid a - b$
- Ký hiệu **$a \equiv b \pmod{n}$**
- Ví dụ: $7 \equiv 12 \pmod 5$, $4 \equiv -1 \pmod 5$,

  $12 \equiv 0 \pmod 2$, $-2 \equiv 19 \pmod{21}$.

Tính chất của đồng dư modular n

- Với mọi số $n \in N$ và $a, b, c \in Z$, các tính chất sau luôn thỏa mãn:

1. $a \equiv a \pmod{n}$ (tính phản xạ)
2. Nếu $a \equiv b \pmod{n}$ thì $b \equiv a \pmod{n}$ (tính đối xứng)
3. Nếu $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ thì $a \equiv c \pmod{n}$ (tính bắc cầu)

Quan hệ tương đương (equivalence relation)

- Theo tính chất của quan hệ tương đương trên 1 tập nào đó thì tập đó được phân hoạch (partitions) thành 1 tập các lớp tương đương (equivalence class), được gọi là các lớp thặng dư (residue class).
- Quan hệ đồng dư theo modular n là quan hệ tương đương

Quan hệ tương đương (equivalence relation)

- Ký hiệu $R_n(a)$ để chỉ lớp đồng dư chứa tất cả các số x ∈ Z đồng dư với a theo modulo n
- **$R_n(a)$ còn được ký hiệu là a hay $a \pm nZ$**

$$R_n(a) := \{x \in \mathbb{Z} \mid a \equiv x \pmod{n}\}$$

- Ví dụ: $R_4(1)$ = {1, 5, 9, 13, 17,…}

Tập các thặng dư nhỏ nhất

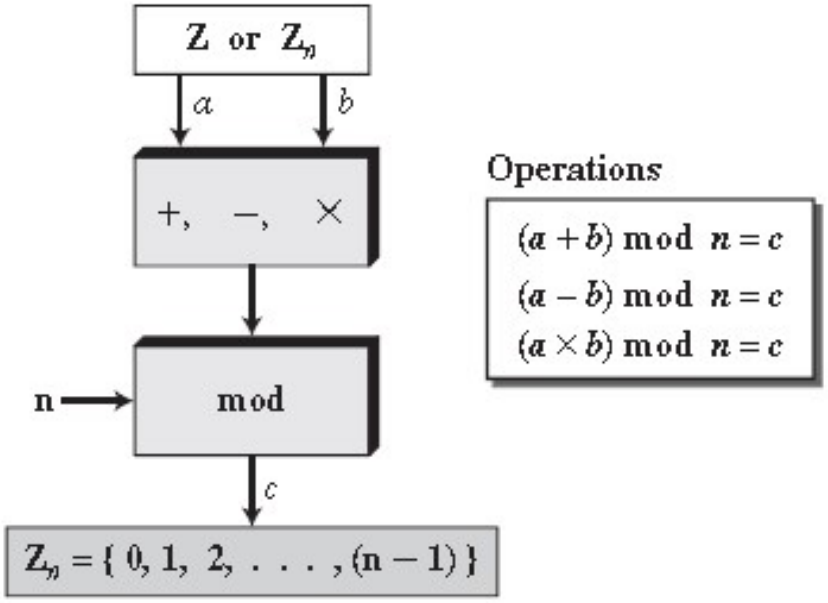
- Trong mỗi lớp đồng dư luôn có **1 phần tử không âm nhỏ nhất được gọi là least residue**. Trong lớp [0] least residue là 0, [1] least residue là 1,…
- Tập hợp tất cả các least residue modulo n

$$Z_n=\{0,1,2,3,\ldots, n-1\}$$

được gọi là set of all least residue modulo n

Các phép toán đồng dư

- 3 phép toán: Addtion,subtraction, và multiplication



Các phép toán đồng dư
Ví dụ:

- Cộng 7 với 4 trong Z_{15}
- Trừ 11 từ 7 trong Z_{13}
- Nhân 11 bởi 7 trong Z_{20}

→ Giải:

- $(14 + 7) \bmod 15 \rightarrow (21) \bmod 15 = 6$
- $(7 - 11) \bmod 13 \rightarrow (-4) \bmod 13 = 9$
- $(7 \times 11) \bmod 20 \rightarrow (77) \bmod 20 = 17$

Các phép toán đồng dư: Thuộc tính

First Property:	$(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
Second Property:	$(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$
Third Property:	$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

Các phép toán đồng dư
Ví dụ:

- $R_7(12 + 18) = R_7(R_7(12) + R_7(18)) = 2$

- $R_7(12 \cdot 18) = R_7(R_7(12) \cdot R_7(18))$

  $= R_7(5 \cdot 4) = R_7(20) = 6$

Các số nghịch đảo

- Khi thực hiện các phép toán số học modular, thường phải tìm nghịch đảo của 1 số tương ứng với phép toán.
  - Nghịch đảo cộng (additive inverse)
  - Nghịch đảo nhân (multiplicative inverse)

Nghịch đảo cộng
Additive Inverse

- Trong Z_n, hai số a và b là nghịch đảo cộng (additive inverse) của nhau nếu

$$a + b \equiv 0 \pmod{n}$$

Lưu ý

Trong phép toán đồng dư, mỗi số nguyên đều có một nghịch đảo cộng. Tổng số nguyên và nghịch đảo cộng của nó đồng dư với 0 modulo n.

Ví dụ

- Tìm tất cả các cặp nghịch đảo cộng trong Z_{10}.
- Có 6 cặp nghịch đảo cộng của nhau trong Z_{10} là (0, 0), (1, 9), (2, 8), (3, 7), (4, 6), and (5, 5).

Nghịch đảo nhân
multiplicative inverse

- Nếu tồn tại 1 số b ∈ Z_n sao cho

$$ab \equiv 1 (\text{mod } n)$$

thì b được gọi là nghịch đảo nhân của a modulo n

- Ký hiệu

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

Nghịch đảo nhân
multiplicative inverse

- ***Điều kiện để số a có nghịch đảo nhân khi và chỉ khi gcd(a, n)=1***
- Ví dụ: a=22, n=25

  Gcd(22,25)= 1 → a có nghịch đảo nhân

  $8 = 22^{-1} \pmod{25}$ vì $8.22 = 176 = 1 \pmod{25}$

  → 8 là nghịch đảo nhân của 22 modulo 25

Ví dụ nghịch đảo nhân

- Cho n = 5 và a = 2. Vì gcd(2, 5) = 1, do đó 2 sẽ có nghịch đảo nhân modulo 5

  → $3 = 2^{-1} \pmod 5$ vì $2 \cdot 3 \equiv 1 \pmod 5$.

- gcd(4, 15) = 1 vì vậy 4 có nghịch đảo nhân modulo 15.

  → Vì $4 \cdot 4 \equiv 1 \pmod{15}$ nên $4 = 4^{-1} \pmod{15}$

Cách tìm nghịch đảo nhân

- Cách 1: dùng giải thuật Euclid mở rộng

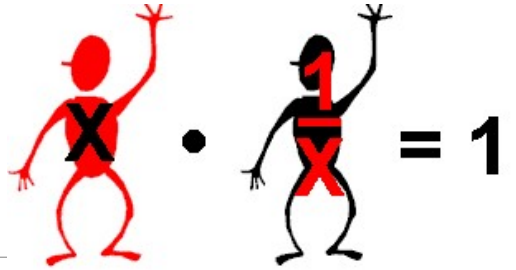
  $au + pv = 1$ với u,v số nguyên

  $u=a^{-1} \bmod p$

- Cách 2: dùng giải thuật tính số mũ nhanh (với p là số nguyên tố)

  $a^1 \equiv a^{p-2} \pmod p$

Nghịch đảo nhân multiplicative inverse



- Để tính nghịch đảo nhân modulo n, áp dụng giải thuật Euclid mở rộng:

  s x n + t x b = gcd(n,b) =1

- Thực hiện phép mod cả 2 vế

  (s x n + t x b) mod n = 1 mod n

  [(s x n) mod n] + [(txb) mod n] = 1 mod n

  0 + [(txb) mod n] = 1

➔ (t x b) mod n = 1 → t chính là nghịch đảo nhân của b

Ví dụ: Tìm nghịch đảo nhân của 23 trong Z_{100}.

$$t = t_1 - q \times t_2$$

q	r_1	r_2	r	t_1	t_2	t
4	100	23	8	0	1	–4
2	23	8	7	1	–4	19
1	8	7	1	–4	9	–13
7	7	1	0	9	–13	100
	1	0		–13	100	

- gcd(100, 23) là 1; nghịch đảo nhân của 23 là –13 hoặc 87.

Ví dụ: Tìm nghịch đảo nhân của 12 trong Z_{26}.

q	r_1	r_2	r	t_1	t_2	t
2	26	12	2	0	1	–2
6	12	2	0	1	–2	13
	2	0		–2	13	

- gcd(26, 2) là 2; nghịch đảo nhân không tồn tại

Ví dụ: Tìm nghịch đảo nhân của 7 trong Z_{160}

Các tập hợp nghịch đảo cộng & nhân

- Zn = {0,1,…,n-1}

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

- Nếu n là số nguyên tố thì $\mathbb{Z}_n \setminus \{0\} = \mathbb{Z}_n^*$
- $\mathbb{Z}_n^*$ là tập hợp tất cả các số thuộc Zn khả nghịch modulo n
- Mỗi phần tử của Zn đều có nghịch đảo cộng, nhưng chỉ có 1 số là có nghịch đảo nhân. Mỗi phần tử của $\mathbb{Z}_n^*$ đều có nghịch đảo nhân nhưng chỉ có 1 số là có nghịch đảo cộng.

Ví dụ một số tập hợp Zn và Zn*

$\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

$\mathbf{Z}_6^* = \{1, 5\}$

$\mathbf{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$\mathbf{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

$\mathbf{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$\mathbf{Z}_{10}^* = \{1, 3, 7, 9\}$

$Z_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

$Z_{13}* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

Phần IV

SỐ NGUYÊN TỐ (PRIME)

Nguyên tố và hợp số

- Số tự nhiên (natural number) 1 <n ∈ N được gọi là số nguyên tố (prime) nếu nó chỉ chia hết cho chính nó và cho 1.
- Số tự nhiên n ∈ N không phải là số nguyên tố thì được gọi là hợp số (composite)
- Tập hợp các số nguyên tố được ký hiệu là P
- Lưu ý : Số 1 không phải là số nguyên tố cũng không phải là hợp số

Hàm đếm các số nguyên tố

- Hàm đếm các số nguyên tố (prime counting function) $\pi(n)$ cho kết quả là số các số nguyên tố nhỏ hơn hay bằng $n \in N$

$$\pi(n) := |\{p \in P \mid p \leq n\}|$$

n	2	3	4	5	6	7	8	9	10	11	12	13	14	...
$\pi(n)$	1	2	2	3	3	4	4	4	4	5	5	6	6	...

Euler's Phi Function

- Dùng để đếm các số nhỏ hơn $n \in N$ mà nguyên tố cùng nhau với n

$$\phi(n)=|\{a \in \{0, \ldots, n-1\} | \gcd(a, n)=1\}|$$

- Ví dụ: $\phi(10) = 4$

Euler's Phi Function

1. $\phi(1)=0$
2. $\phi(p)=p-1$ nếu p là một nguyên tố
3. $\phi(m \times n)=\phi(m) \times \phi(n)$ nếu m và n là nguyên tố cùng nhau
4. $\phi(p^e)=p^e-p^{e-1}$ nếu p là một nguyên tố

Euler's Phi Function

- Kết hợp 4 quy tắc trên, nếu với mọi số nguyên n có thể phân tích thành thừa số (factorize) nguyên tố

$$n = \prod_i q_i^{k_i}$$

Thì

$$\phi(n) = \prod_i (q_i - 1) q_i^{k_i - 1}$$

- Ví dụ: $\phi(45) = \phi(3^2.5) = (3-1).3^{2-1}.(5-1).5^{1-1}=24$

Ví dụ: Giá trị của $\phi(240)$?

Giải

Chúng ta có thể viết $240 = 2^4 \times 3^1 \times 5^1$. thì

$$\phi(240) = (2\text{-}1) \text{ x } (2^{4\text{-}1}) \text{ x } (3\text{-}1) \times (3^{1\text{-}1}) \times (5\text{-}1)(5^{1\text{-}1})$$
$$= 64$$

Ví dụ: Chúng ta có thể nói $\phi(49) = \phi(7) \times \phi(7) = 6 \times 6 = 36$?

Giải

- Không. Vì 7 và 7 không là nguyên tố cùng nhau nên không áp dụng được luật 3.

- $49 = 7^2$, chúng ta cần luật thứ 4: $\phi(49) = 7^2 - 7^1 = 42$.

Ví dụ: Tính $\phi(187)$, với $187 = 17 \times 11$

Lưu ý

Độ khó của việt tìm $\phi(n)$ tùy thuộc vào độ khó của việc phân tích thừa số của n.

Định lý Little Fermat (1640)

- Nếu p là 1 số nguyên tố và a là số nguyên thì

$$a^{p-1} = 1 \mod p$$

- Hoặc

$$a^p \equiv a \mod p$$

- Ví dụ: cho p=5

➔ $3^4 = 81 = 1 \mod 5$

- **Ứng dụng**: dùng để tính nghịch đảo nhân nhưng không hiệu quả bằng giải thuật Euclid mở rộng

Vì $x \in Z_p \Rightarrow x \cdot x^{p-2} = 1 \Rightarrow x^{-1} = x^{p-2}$ in Z_p

Định lý Euler

- Định lý Euler được xem như trường hợp đặc biệt của định lý Fermat
- First Version

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

- Second Version

$$a^{k \times \phi(n) + 1} \equiv a \pmod{n}$$

Tìm nghịch đảo nhân dùng định lý Euler

- Định lý Euler có thể được dùng để tìm nghịch đảo nhân modulo 1 hợp số.

$$a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$$

Ví dụ:

- The answers to multiplicative inverses modulo a composite can be found without using the extended Euclidean algorithm if we know the factorization of the composite:

a. $8^{-1} \bmod 77 = 8^{\phi(77)-1} \bmod 77 = 8^{59} \bmod 77 = 29 \bmod 77$

b. $7^{-1} \bmod 15 = 7^{\phi(15)-1} \bmod 15 = 7^{7} \bmod 15 = 13 \bmod 15$

c. $60^{-1} \bmod 187 = 60^{\phi(187)-1} \bmod 187 = 60^{159} \bmod 187 = 53 \bmod 187$

d. $71^{-1} \bmod 100 = 71^{\phi(100)-1} \bmod 100 = 71^{39} \bmod 100 = 31 \bmod 100$

Example 9.17

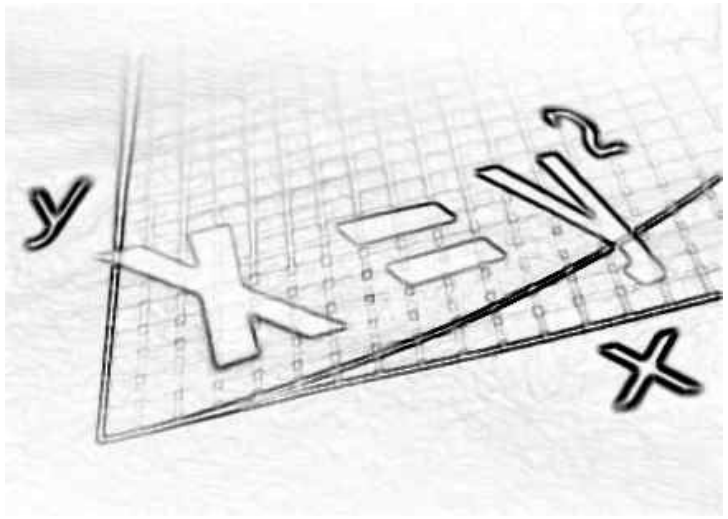
The answers to multiplicative inverses modulo a composite can be found without using the extended Euclidean algorithm if we know the factorization of the composite:

a. $8^{-1} \bmod 77 = 8^{\phi(77)-1} \bmod 77 = 8^{59} \bmod 77 = 29 \bmod 77$

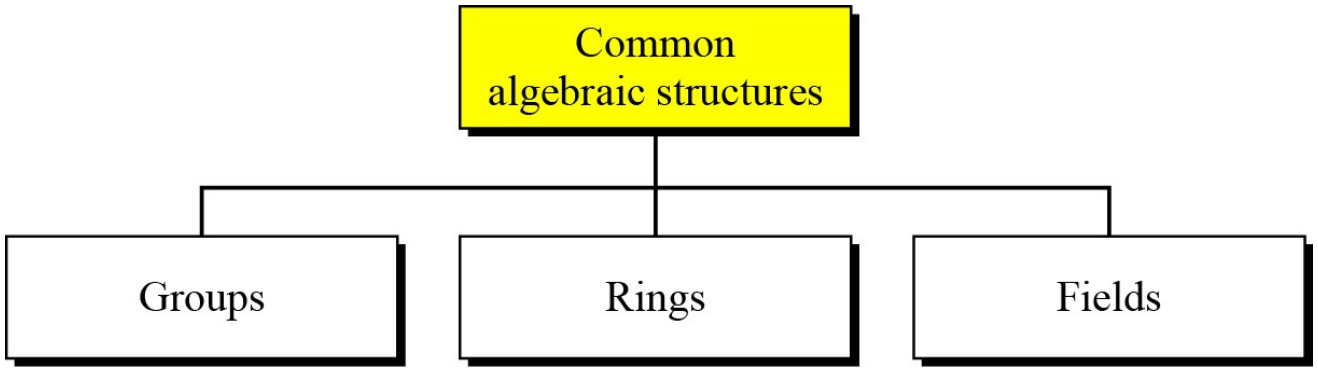
b. $7^{-1} \bmod 15 = 7^{\phi(15)-1} \bmod 15 = 7^{7} \bmod 15 = 13 \bmod 15$

c. $60^{-1} \bmod 187 = 60^{\phi(187)-1} \bmod 187 = 60^{159} \bmod 187 = 53 \bmod 187$

d. $71^{-1} \bmod 100 = 71^{\phi(100)-1} \bmod 100 = 71^{39} \bmod 100 = 31 \bmod 100$



PHẦN III: ALGEBRAIC STRUCTURES


Common
algebraic structures
Groups
Rings
Fields

Phần tử đồng nhất
Identity element

- Cho S là 1 tập hợp và $*$ là phép toán hai ngôi (binary operation) trên S. Phần tử $e \in S$ được gọi là phần tử đồng nhất nếu luôn có

$$e * a = a * e = a \quad \forall\, a \in S$$

Ví dụ: phần tử đồng nhất của phép cộng và phép nhân trong Z??

Groups

- **Group (G):** tập hợp các phần tử với 1 phép toán 2 ngôi "•" và thỏa mãn 4 thuộc tính sau:
  - **Closure**: nếu $a,b \in G$ thì $c=a \bullet b \in G$
  - **Associativity:** nếu $a,b \in G$ thì $(a \bullet b) \bullet c = a \bullet (b \bullet c)$
  - **Existence of identity**: $\forall a \in G$ luôn tồn tại 1 phần tử e được gọi là phần tử đồng nhất (identity element) sao cho $e \bullet a = a \bullet e = a$
  - **Existence of inverse**: $\forall a \in G$ luôn tồn tại 1 phần tử a' được gọi là nghịch đảo của a sao cho $a \bullet a' = a' \bullet a = e$

Nhóm giao hoán
Commutative group

- Còn được gọi là abelian group
- Là 1 group mà toán tử của nhóm thỏa mãn thêm thuộc tính commutativity.
  - **Commutativity:** $\forall a,b \in G$ thì $a \bullet b = b \bullet a$
- G = <Zn, +> có phải là nhóm giao hoán (commutative group) không?

➔ Yes

Finite Group/Subgroup

- Group được gọi là hữu hạn (finite) nếu số phần tử của nó là hữu hạn.
- Subgroup: tập con H của group G được gọi là subgroup của G nếu chính H cũng là 1 group với cùng phép toán của G.
  - Ví dụ: H = $<Z_{10}, +>$ có phải là subgroup của G=$<Z_{12},+>$?

Cyclic subgroup

- Nhóm con vòng (cyclic subgroup) : là subgroup của 1 group được tạo ra từ phép power của 1 phần tử nào đó
  - Power có nghĩa là lặp lại nhiều lần phép toán của nhóm.

$$a^n \rightarrow a \bullet a \bullet \ldots \bullet a \quad (n \text{ times})$$

Example 4.7

Four cyclic subgroups can be made from the group G = $<Z_6, +>$. They are H1 = $<\{0\}, +>$, H2 = $<\{0, 2, 4\}, +>$, H_3 = $<\{0, 3\}, +>$, and H4= G.

$0^0 \bmod 6 = 0$ — H1

$1^0 \bmod 6 = 0$
$1^1 \bmod 6 = 1$
$1^2 \bmod 6 = (1 + 1) \bmod 6 = 2$
$1^3 \bmod 6 = (1 + 1 + 1) \bmod 6 = 3$
$1^4 \bmod 6 = (1 + 1 + 1 + 1) \bmod 6 = 4$
$1^5 \bmod 6 = (1 + 1 + 1 + 1 + 1) \bmod 6 = 5$ — H4

$2^0 \bmod 6 = 0$
$2^1 \bmod 6 = 2$
$2^2 \bmod 6 = (2 + 2) \bmod 6 = 4$ — H2

$3^0 \bmod 6 = 0$
$3^1 \bmod 6 = 3$ — H3

$4^0 \bmod 6 = 0$
$4^1 \bmod 6 = 4$
$4^2 \bmod 6 = (4 + 4) \bmod 6 = 2$ — H2

$5^0 \bmod 6 = 0$
$5^1 \bmod 6 = 5$
$5^2 \bmod 6 = 4$
$5^3 \bmod 6 = 3$
$5^4 \bmod 6 = 2$
$5^5 \bmod 6 = 1$

Ví dụ

- Ba cyclic subgroup từ group G=<Z_{10}*, x>
- G chỉ có 4 phần tử là 1,3,7,9

$1^0 \bmod 10 = 1$ ← H1

$3^0 \bmod 10 = 1$
$3^1 \bmod 10 = 3$ ← H3
$3^2 \bmod 10 = 9$
$3^3 \bmod 10 = 7$

$7^0 \bmod 10 = 1$
$7^1 \bmod 10 = 7$
$7^2 \bmod 10 = 9$ ← H3
$7^3 \bmod 10 = 3$

$9^0 \bmod 10 = 7$
$91 \bmod 10 = 9$ ← H2

Cyclic group

- Nhóm vòng (cyclic group) là group mà chính nó cũng là cyclic subgroup.
  - Ví dụ H_4=G → G là 1 cyclic group.
- Phần tử tạo ra cyclic group được gọi là generator.

$$\{e, g, g^2, \ldots, g^{n-1}\}, \text{where } g^n = e$$

Ví dụ

- The group G = <Z6, +> is a cyclic group with two generators, $g = 1$ and $g = 5$.

- The group G = <Z_{10}*, ×> is a cyclic group with two generators, $g = 3$ and $g = 7$.

Bậc của nhóm (Order of the Group)

- Bậc của 1 nhóm hữu hạn |G| là số phần tử trong nhóm G.
- Bậc của G=<Zn*,x> là $\phi(n)$
- Ví dụ: bậc của nhóm G = <Z_{21}*, ×>?
  - |G| = ϕ (21) = ϕ (3) × ϕ (7) = 2 × 6 =12.
  - Z_{21}* ={1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20}

Bậc của phần tử
Order of an Element

- Bậc của phần tử a, ký hiệu ord(a) trong nhóm G là số nguyên nhỏ nhất i sao cho $a^i \cong e \pmod n$ với e là phần tử đồng nhất
- Bậc của phần tử là generator cũng là bậc của nhóm vòng mà nó tạo ra.

Ví dụ 1

- Tìm bậc của tất cả các phần tử trong G= $<Z_{10}^*, \times>$.
- Nhóm có $\phi(10) = 4$ phần tử, $Z_{10}^*=\{1,3,7,9\}$. Bậc của mỗi phần tử được tính bằng cách trial and error

a. $1^1 \equiv 1 \bmod (10) \rightarrow \text{ord}(1) = 1$.

b. $3^4 \equiv 1 \bmod (10) \rightarrow \text{ord}(3) = 4$.

c. $7^4 \equiv 1 \bmod (10) \rightarrow \text{ord}(7) = 4$.

d. $9^2 \equiv 1 \bmod (10) \rightarrow \text{ord}(9) = 2$.

Primitive root

- Trong nhóm G = $<Z_n*, \times>$, khi bậc của 1 phần tử bằng với $\phi(n)$, thì phần tử này được gọi là primitive root của nhóm.

$$\text{ord}(a) = \phi(n).$$

Primitive root của Z_{19}^* là 2,3,10,13,14,15

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Ví dụ: tìm primitive của $<Z_7^*, x>$

	$i = 1$	$i = 2$	$i = 3$	$i = 4$	$i = 5$	$i = 6$
$a = 1$	x: 1	x: 1	x: 1	x: 1	x: 1	x: 1
$a = 2$	x: 2	x: 4	x: 1	x: 2	x: 4	x: 1
Primitive root → $a = 3$	x: 3	x: 2	x: 6	x: 4	x: 5	x: 1
$a = 4$	x: 4	x: 2	x: 1	x: 4	x: 2	x: 1
Primitive root → $a = 5$	x: 5	x: 4	x: 6	x: 2	x: 3	x: 1
$a = 6$	x: 6	x: 1	x: 6	x: 1	x: 6	x: 1

Nhóm vòng
Cyclic Group

- Nếu g là primitive root trong nhóm thì g có thể tạo (generate) tập Z_n^* như sau:

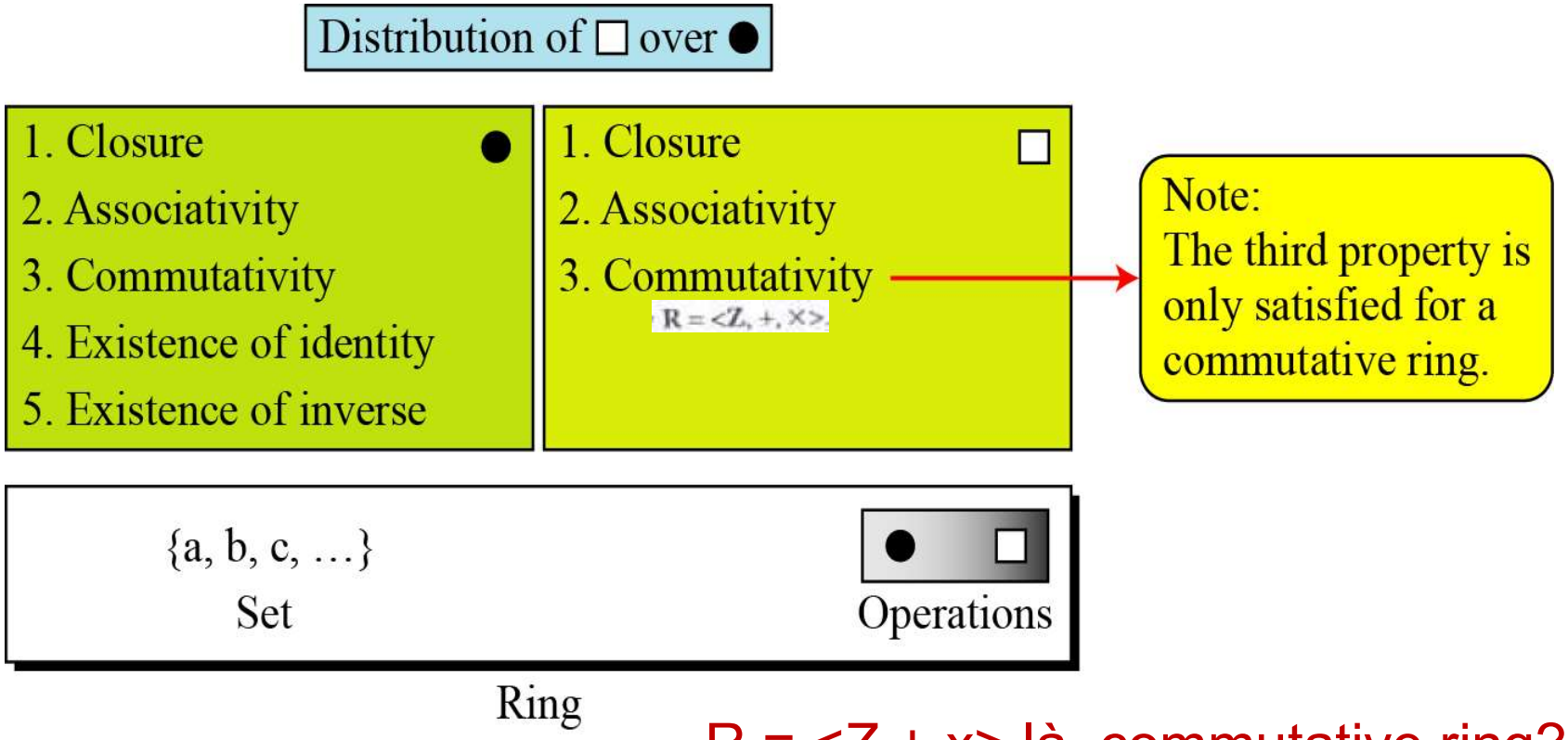
$$Z_n^* = \{g^1, g^2, g^3, \ldots, g^{\phi(n)}\}$$

The group $G = \langle Z_n^*, \times \rangle$ is a cyclic group if it has primitive roots.
The group $G = \langle Z_p^*, \times \rangle$ is always cyclic.

Ring

- **Ring** R=<{…}, •,□> có 2 phép toán
  - Phép toán thứ nhất • thỏa mãn cả 5 thuộc tính của nhóm giao hoán (abelian group)
  - Phép toán □ chỉ cần thỏa mãn 2 thuộc tính đầu nhưng phải có tính phân phối (distributivity) đối với phép toán thứ nhất •
  - ➔ ∀ a,b,c∈ R a □(b •c) = (a □b) •(a □c)
- **Commutative ring** là ring mà phép toán thứ hai thỏa mãn cả thuộc tính giao hoán (commutative)

Ring

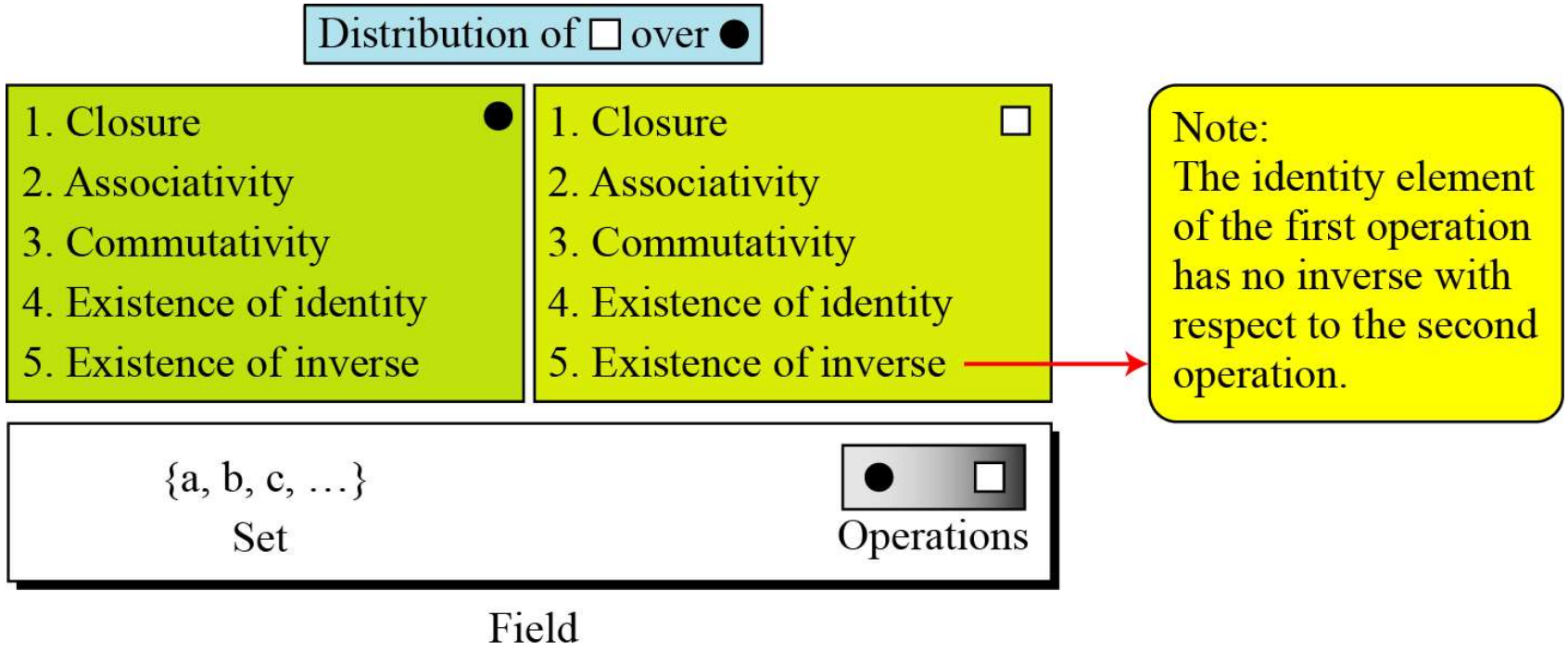


R = <Z,+,x> là commutative ring??

Field

- Field F= <{..}, ●,□> là 1 commutative ring mà phép toán thứ hai thỏa mãn cả 5 thuộc tính nhưng phần tử identity của phép toán thứ nhất không có nghịch đảo đối với phép toán thứ hai

Field


Distribution of □ over ●
1. Closure
2. Associativity
3. Commutativity
4. Existence of identity
5. Existence of inverse
1. Closure
2. Associativity
3. Commutativity
4. Existence of identity
5. Existence of inverse
Note:
The identity element of the first operation has no inverse with respect to the second operation.
{a, b, c, …}
Set
Operations
Field

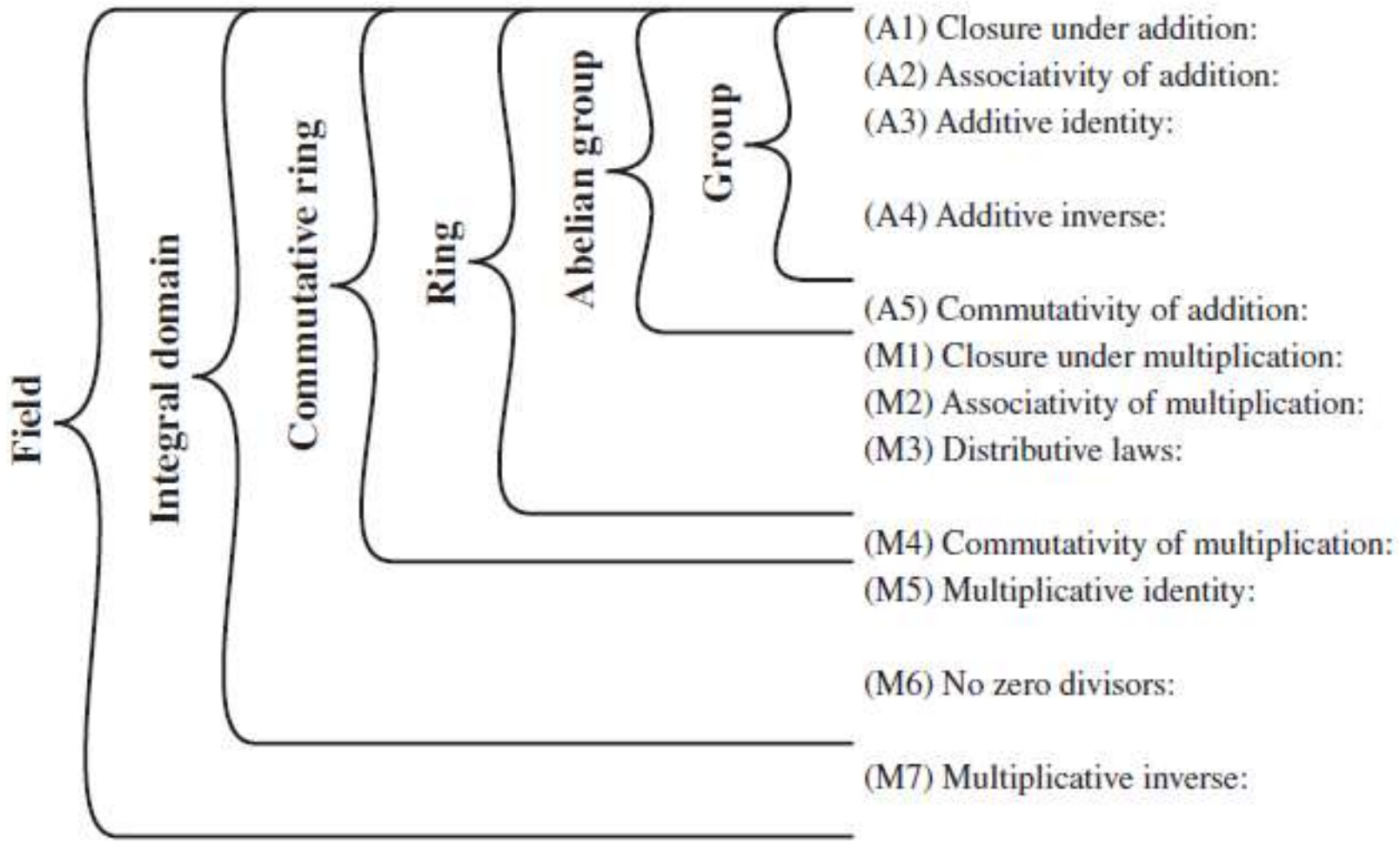


Figure 4.2 Groups, Ring, and Field

Finite field

- Finite field hay còn gọi là Galois field là 1 field mà số phần tử của nó là p^n với p là số nguyên tố (prime) và n là 1 số nguyên dương

Note

Một Galois field, GF(p^n), là một trường hữu hạn có p^n phần tử.

GF(p) field

- Khi n = 1 thì GF(p)

The simplest finite field is GF(2). Its arithmetic operations are easily summarized:

+	0	1
0	0	1
1	1	0

Addition

×	0	1
0	0	0
1	0	1

Multiplication

w	$-w$	w^{-1}
0	0	—
1	1	1

Inverses

In this case, addition is equivalent to the exclusive-OR (XOR) operation, and multiplication is equivalent to the logical AND operation.

Table 4.5 Arithmetic in GF(7)

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

(a) Addition modulo 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(b) Multiplication modulo 7

w	$-w$	w^{-1}
0	0	—
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

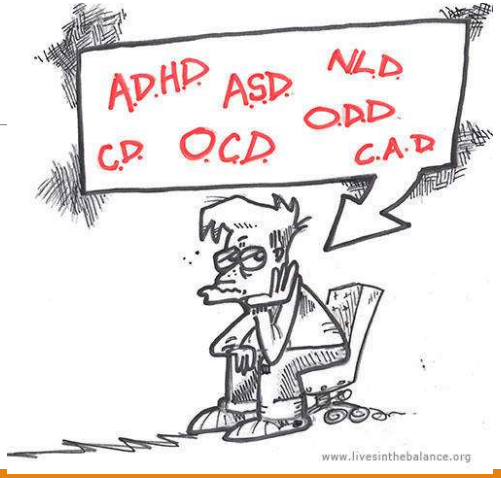
(c) Additive and multiplicative inverses modulo 7

1. GF(p) consists of p elements.
2. The binary operations + and × are defined over the set. The operations of addition, subtraction, multiplication, and division can be performed without leaving the set. Each element of the set other than 0 has a multiplicative inverse.

We have shown that the elements of GF(p) are the integers $\{0, 1, \ldots, p - 1\}$ and that the arithmetic operations are addition and multiplication mod p.

CÁC BÀI TOÁN KHÓ GIẢI

PHẦN V



- Phân tích thừa số nguyên tố
- Thặng dư bậc hai
- Logarithm rời rạc

Định lý số học cơ bản
Fundamental Theorem of Arithmetic

- Bất kỳ số dương nào lớn hơn 1 đều có thể biểu diễn duy nhất dưới dạng thừa số nguyên tố (prime factorization)

$$n = p_1^{e1} \times p_2^{e2} \times \cdots \times p_k^{ek}$$

  - Với $p_1, p_2, \ldots, p_k$ là các số nguyên tố
  - $e_1, e_2, .., e_k$ là các số nguyên dương

Thặng dư bậc hai
Quadratic Residuosity

- Phần tử x ∈ Z_n^* là thặng dư bậc hai modulo n (quadratic residue modulo n) nếu tồn tại 1 phần tử y ∈ Z_n^* sao cho x =y^2 (mod n) . Phần tử y được gọi là căn bậc hai của x modulo n (square root of x modulo n).
- Thặng dư bậc hai trong Z_n^* được ký hiệu QR_n

$$QR_n := \{x \in \mathbb{Z}_n^* \mid \exists y \in \mathbb{Z}_n^* : y^2 \equiv x \pmod{n}\}$$

Phân loại

- Xét 2 trường hợp thặng dư bậc hai modulo n với:
  - N là số nguyên tố
  - N là hợp số → bài toán thặng dư bậc hai (Quadratic residuosity problem **QRP**)

Thặng dư bậc hai modulo là số nguyên tố
Quadratic Residuosity modulo prime

- Mỗi phần tử trong Z_n^* hoặc là thặng dư bậc hai (quadratic residue) hoặc không thặng dư bậc hai (quadratic nonresidue)

  - Tập hợp tất cả số không thặng dư bậc hai trong Z_n^* là phần bù (complement) của QRn, ký hiệu QNR_n

$$QNR_n = Z_n^* \setminus QR_n$$

Ví dụ thặng dư bậc hai modulo prime

- Trong Z_7^* các phần tử {1, 2, 3, 4, 5, 6} có thể lũy thừa bậc hai như sau:

x	1	2	3	4	5	6
x^2	1	4	2	2	4	1

- Chỉ có 1,4,2 trong hàng thứ hai, nó chính là các thặng dư bậc hai
  - ➔ $QR_7 = \{1, 2, 4\}$
  - ➔ $QNR_7 = Z^*_7 \setminus QR_7 = \{3, 5, 6\}$

Ví dụ thặng dư bậc hai modulo là số nguyên tố

- Tìm QR19 và QNR19?

$$QR_{19} = \{1, 4, 5, 6, 7, 9, 11, 16, 17\}$$

$$QNR_{19} = \mathbb{Z}_{19}^* \setminus QR_{19} = \{2, 3, 8, 10, 12, 13, 14, 15, 18\}$$

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
x2	1	4	9	16	6	17	11	7	5	5	7	11	17	6	16	9	4	1

Thặng dư bậc hai với modulo là số nguyên tố

- Với 1 số nguyên tố lẻ p>2, luôn có

$$|QR_p| = \frac{p-1}{2}$$

- Với mọi số nguyên tố p> 2, Z_p^* được phân hoạch thành 2 nhóm con có kích cỡ bằng nhau QRp và QNRp (mỗi nhóm con chứa (p − 1)/2 phần tử)

Tiêu chuẩn Euler
Euler's criterion

- Cho p là 1 số nguyên tố. Đối với bất kỳ số x ∈ Z_p^* ,x ∈ QRp nếu và chỉ nếu

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

- Nếu tiêu chuẩn Euler không thỏa mãn thì

$$x^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

- Tiêu chuẩn Euler dùng để xác định xem 1 số x có thuộc QRp hay không?

Ví dụ

$QR_7 = \{1, 2, 4\}$

$QNR_7 = Z^*_7 \setminus QR_7 = \{3, 5, 6\}$

- Với x=2 $\in$ QR7 thì

$$x^{\frac{p-1}{2}} = 2^3 \bmod 7 = 1$$

- Với x = 5 $\in$ QNR_7 thì

$$x^{\frac{p-1}{2}} = 5^3 \bmod 7 = -1$$

Bài toán thặng dư bậc hai (Quadratic residuosity problem QRP)

- Cho n là một hợp số nguyên dương $n \in N$ và $x \in Z_n^*$. Bài toán QRP sẽ quyết định x có thuộc QRn hay không??
- Hiện vẫn chưa có giải thuật hiệu quả nếu đầu vào là 1 số $n \in N$ (tích của 2 số nguyên tố lớn) và $x \in Z_n^*$ có thể xác định được x có là thặng dư bậc hai modulo n hay không?

Bài toán thặng dư bậc hai (Quadratic residuosity problem QRP)

- Đã được chỉ rằng có thể tính được căn bậc hai của x nếu và chỉ nếu phân tích được thừa số của n.

→ Tính căn bậc hai trong Z_n^* cũng khó tương đương với bài toán phân tích số n.

Exponentiation và logarithm

Exponentiation: $y = a^x$ $\rightarrow$ **Logarithm:** $x = \log_a y$

Lũy thừa modulo
Modular Exponentiation

- Tính a^b (mod n)??
- Giải thuật đơn giản nhất là nhân a (mod n) b lần
- Giả sử b = 23

$$
\begin{aligned}
R_n(a^2) &= R_n(a \cdot a) \\
R_n(a^3) &= R_n(a \cdot R_n(a^2)) \\
R_n(a^4) &= R_n(a \cdot R_n(a^3)) \\
&\cdots \\
R_n(a^{23}) &= R_n(a \cdot R_n(a^{22}))
\end{aligned}
$$

- Có cách nào ngắn hơn không???

Lũy thừa modulo
Modular Exponentiation

$$
\begin{aligned}
R_n(a^2) &= R_n(a \cdot a) \\
R_n(a^4) &= R_n(R_n(a^2) \cdot R_n(a^2)) \\
R_n(a^5) &= R_n(a \cdot R_n(a^4)) \\
R_n(a^{10}) &= R_n(R_n(a^5) \cdot R_n(a^5)) \\
R_n(a^{11}) &= R_n(a \cdot R_n(a^{10})) \\
R_n(a^{22}) &= R_n(R_n(a^{11}) \cdot R_n(a^{11})) \\
R_n(a^{23}) &= R_n(a \cdot R_n(a^{22}))
\end{aligned}
$$

- Chỉ cần 7 lần nhân

Fast exponential algorithm
Square-and-multiply algorithm

- Sử dụng khai triển nhị phân của số mũ b để biến đổi phép tính a^b thành 1 chuỗi các phép bình phương và nhân.

$(a \in G, b = b_{k-1} \ldots b_1 b_0 \in \mathbb{N})$

$s \leftarrow 1$

for $i = k - 1$ down to 0 do

  $s \leftarrow s \cdot s$

  if $b_i = 1$ then $s \leftarrow s \cdot a$

return s

(a^b)

The square-and-multiply algorithm

- Tính 7^{22} (mod 11)
  - Tính b = $(22)_{10} = (10110)_2$.
  - Áp dụng giải thuật trên để tính như sau:

$$
\begin{aligned}
7^{(1)_2} &= 1^2 \cdot 7 \equiv 7 \pmod{11} \\
7^{(10)_2} &= 7^2 \equiv 5 \pmod{11} \\
7^{(101)_2} &= 5^2 \cdot 7 \equiv 3 \cdot 7 \equiv 10 \pmod{11} \\
7^{(1011)_2} &= (10)^2 \cdot 7 \equiv 7 \pmod{11} \\
7^{(10110)_2} &= 7^2 \equiv 5 \pmod{11}
\end{aligned}
$$

Discrete logarithm function

- P là 1 số nguyên tố (prime) và g là primitive root của Z_p^*. Hàm

$$\begin{aligned} \mathrm{Exp}_{p,g} : \mathbb{Z}_{p-1} &\longrightarrow \mathbb{Z}_p^* \\ x &\longmapsto g^x \end{aligned}$$

gọi là hàm discrete exponentiation của cơ số g.

- Vì Exp là song ánh nên hàm ngược của nó là:

$$\begin{aligned} \mathrm{Log}_{p,g} : \mathbb{Z}_p^* &\longrightarrow \mathbb{Z}_{p-1} \\ x &\longmapsto \log_g x \end{aligned}$$

Được gọi là hàm discrete logarithm

Discrete Logarithm Problem (DLP)

- Cho g là 1 *primitive root của Zp* và h là 1 phần tử khác 0 của Zp. Bài toán Discrete Logarithm là bài toán tìm số mũ (*exponent) *x sao cho*

$$g^x \equiv h \pmod{p}.$$

- Số *x được gọi là discrete logarithm của h cơ số g và được ký hiệu* $\log_g(h)$.

Discrete Logarithm Problem (DLP)

- Nếu tìm được 1 số mũ nguyên x sao cho $g^x = h$ thì sẽ có vô số lời giải vì theo định lý Fermat

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

→ Nếu x là lời giải của $g^x = h$ thì $x + k(p-1)$ *cũng là lời giải với mọi giá trị k vì*

$$g^{x+k(p-1)} = g^x \cdot (g^{p-1})^k \equiv h \cdot 1^k \equiv h \pmod{p}$$

Ví dụ

- Cho số nguyên tố *p = 56509, và g=2 là 1* primitive root của Zp*. Làm thế nào để tính *discrete* logarithm của h *= 38679?*
- *Lần lượt tính:*

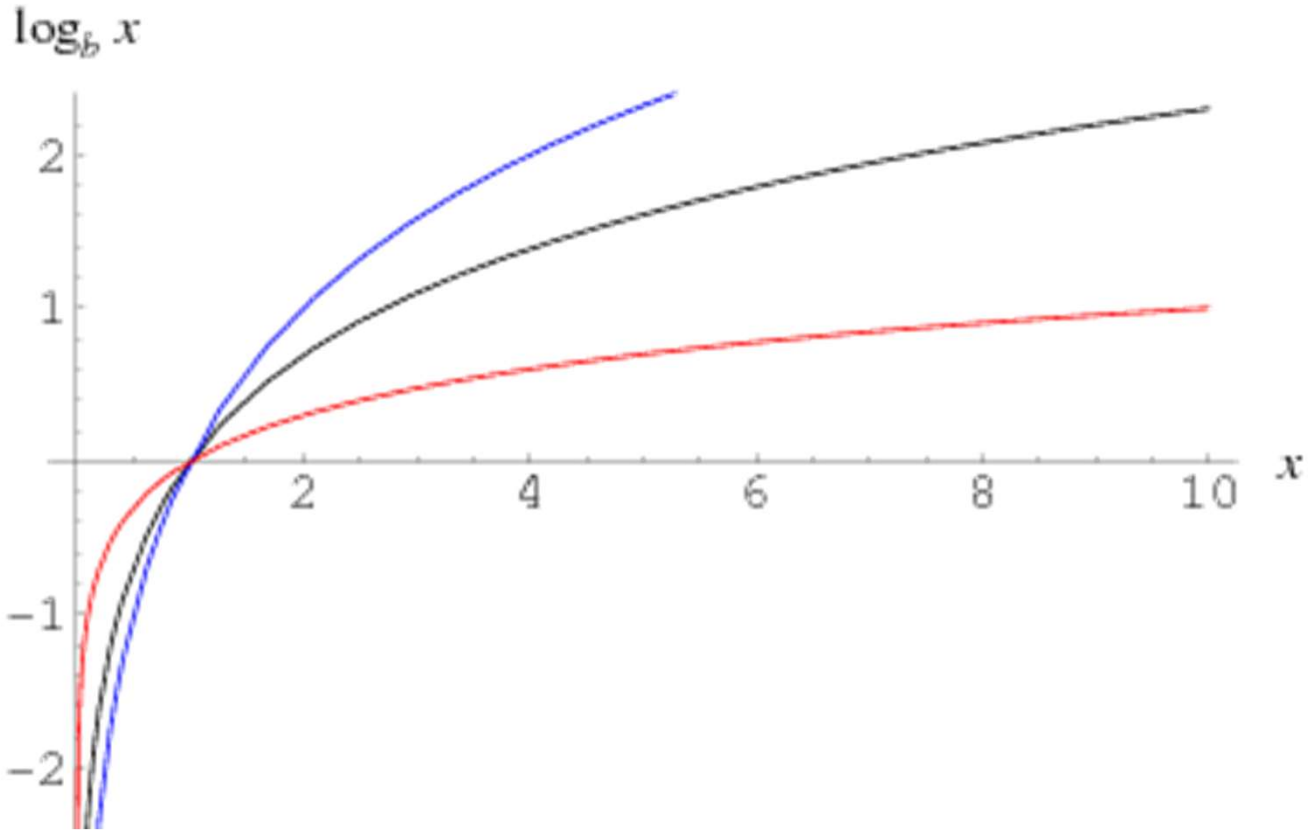
$$2^2,\ 2^3,\ 2^4,\ 2^5,\ 2^6,\ 2^7, \ldots \pmod{56509}$$

- Cho đến khi tìm thấy kết quả bằng với 38679. Việc tính toán này khó thực hiện bằng tay, nhưng nếu dùng máy tính thì dễ dàng tính được log*p(h) = 11235.*

Đặc điểm của Discrete logarithm

- Discrete logarithm khác nhiều so với continuous logarithm được dùng trong số thực hay phức.
  - Về mặt thuật ngữ thì như nhau, cả hai loại logarithm đều là nghịch đảo của lũy thừa (exponentiation)
  - Nhưng lũy thừa modulo *p thì khác xa với lũy thừa thông thường. Kết quả của lũy thừa modulo p thay đổi bất thường không theo quy luật như lũy thừa thông thường*

Continous logarithm



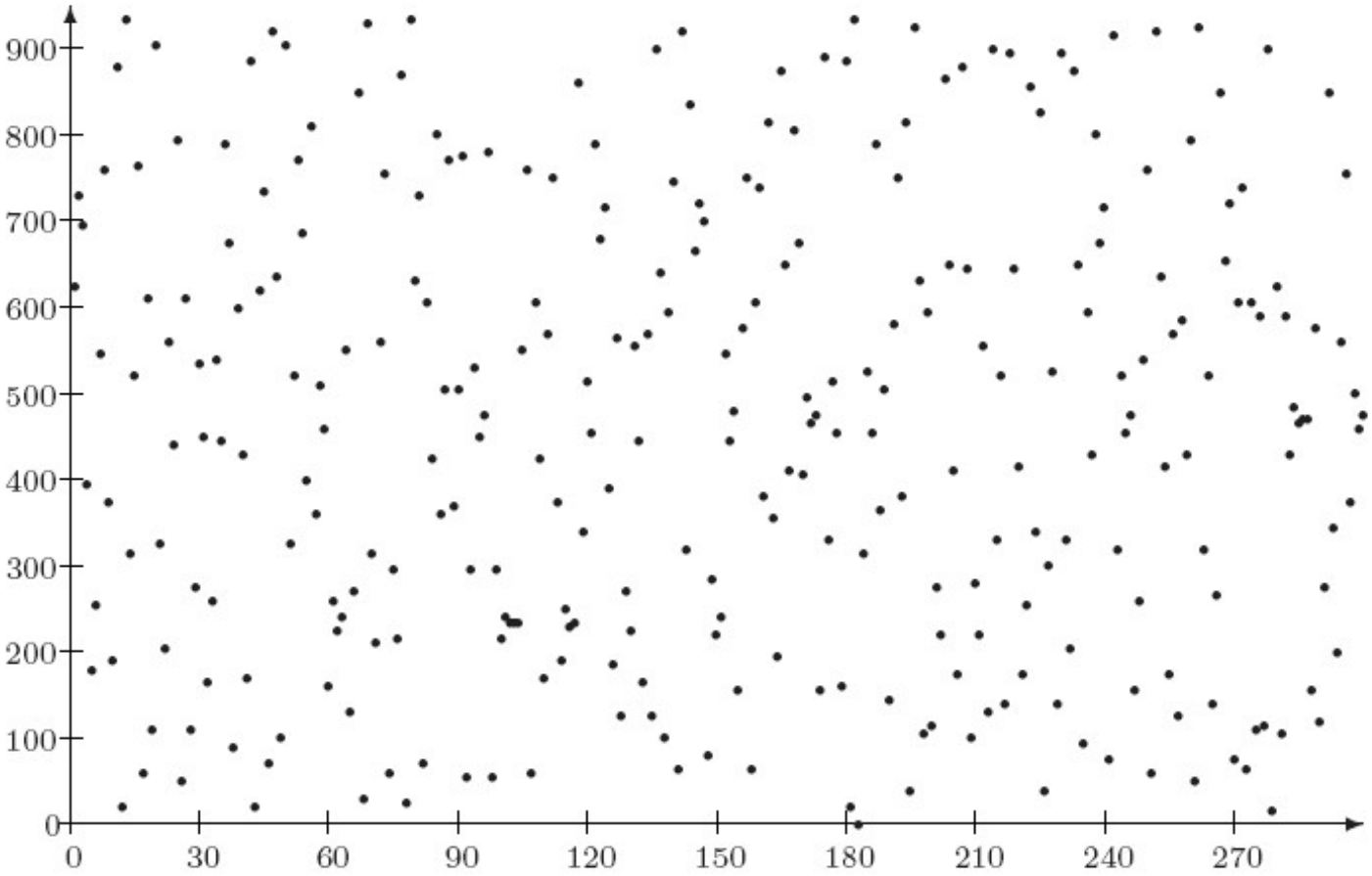


Figure 2.2: Powers 627^i mod 941 for $i = 1, 2, 3, \ldots$

Note

The discrete logarithm problem has the same complexity as the factorization problem.

Định lý số dư Trung hoa (Chinese Remainder Theorem)

$$\begin{cases} x \equiv a1 \pmod{n1} \\ x \equiv a2 \pmod{n2} \\ \dots \\ x \equiv ak \pmod{nk} \end{cases}$$

- Là hệ thống gồm k phương trình đồng dư với n1,...,nk
- Các giá trị n1, .., nk từng đôi một nguyên tố cùng nhau.
- Hệ thống có một nghiệm duy nhất x thuộc Zn

Giải thuật tìm số dư Trung Hoa
Chinese remainder algorithm (CRA)

- Đặt mi = n/ni với i =1,...,k,

  và yi = m^{-1}_i (mod ni)

Khi đó nghiệm x được tính như sau:

$$x \equiv \sum_{i=1}^{k} a_i m_i y_i \pmod{n}$$

Ví dụ

- Cho 1 hệ 3 phương trình đồng dư sau:

$x \equiv 5 (\mathrm{mod}\ 7)$

$x \equiv 3 \pmod{11}$

$x \equiv 11 \pmod{13}$

Hãy tìm nghiệm x

Ví dụ

- n1 =7, n2 =11, n3 =13 → tất cả các cặp đều nguyên tố cùng nhau
- a1 =5, a2 =3 và a3 =11
- Tính n =7 · 11 · 13 = 1001

→ Tính m1 = 1001/7 = 143

m2 = 1001/11 = 91

m3 = 1001/13 = 77

Ví dụ

- Tính $y_1 \equiv 143^{-1} (\text{mod } 7) = 5$

  $y_2 \equiv 91^{-1} (\text{mod } 11) = 4$

  $y_3 \equiv 77^{-1} (\text{mod } 13) = 12$

Tính $x = a_1 m_1 y_1 + a_2 m_2 y_2 + a_3 m_3 y_3$

$= 5 \text{x} 143 \text{x} 5 + 3 \text{x} 91 \text{x} 4 + 11 \text{x} 77 \text{x} 12$

$x = 14831$

Hệ 2 phương trình đồng dư

- Xét hệ 2 phương trình:

  x ≡ a1 (mod n1)

  x ≡ a2 (mod n2) với gcd(n1,n2)=1

Tính $$t \equiv n_2^{-1} \pmod{n_1}$$

Khi đó: u ≅ (a2 – a1)t (mod n2)

Giải thuật này ứng dụng rất nhiều trong hệ mật mã RSA

$$x = a_1 + un_2^1$$