TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN ĐIỆN TỬ VIỄN THÔNG
BỘ MÔN KỸ THUẬT ĐIỆN TỬ HÀNG KHÔNG VŨ TRỤ

LÝ THUYẾT MẬT MÃ - ET3310

CƠ SỞ TOÁN HỌC CỦA LÝ THUYẾT MẬT MÃ

Trình bày : Phạm Thương – ĐT10 K58
Email : thuonghust@gmail.com

NỘI DUNG

- ❖ Số học các số nguyên
- ❖ Số học Modulo
- ❖ Đồng dư tuyến tính
- ❖ Ma trận

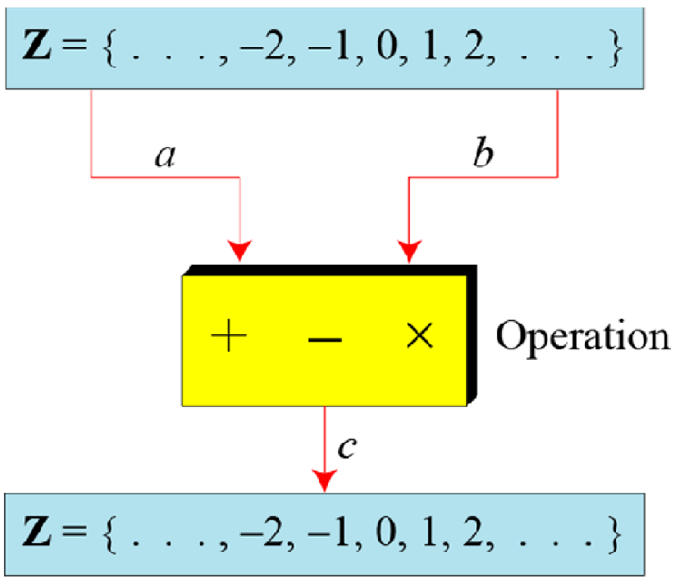
SỐ HỌC CÁC SỐ NGUYÊN

❖ **Tập các số nguyên**

- **Tập hợp các số nguyên: $Z = \{-\infty.....,-2,-1,0,1,2,....+\infty\}$**
- **Tập hợp các số nguyên không âm: $Z^{+}= \{0,1,2,..... +\infty\}$**

SỐ HỌC CÁC SỐ NGUYÊN

❖ Binary operations



- Tập hợp Z là đóng kín đối với các phép cộng, trừ và nhân, nhưng không đóng kín đối với phép chia.

- Ví dụ:

Add:	$5 + 9 = 14$	$(-5) + 9 = 4$	$5 + (-9) = -4$	$(-5) + (-9) = -14$
Subtract:	$5 - 9 = -4$	$(-5) - 9 = -14$	$5 - (-9) = 14$	$(-5) - (-9) = +4$
Multiply:	$5 \times 9 = 45$	$(-5) \times 9 = -45$	$5 \times (-9) = -45$	$(-5) \times (-9) = 45$

❖ Chia số nguyên

- Cho hai số nguyên bất kỳ a và n , n > 1

$$a = q*n + r$$

q là thương số
q = a div n

r là số dư, 0 ≤ r < n
r = a mod n

- Ví dụ

37 = 3*11 + 4 ⇒ 37 div 11 = 3
37 mod 11 = 4

Cho a = -1023, n = 13.
Tìm a div n, a mod n? ⇒ (-1023) div 13 = -79
(-1023) mod 13 = 4

SỐ HỌC CÁC SỐ NGUYÊN

❖ Phép chia hết

- **Biểu thức:** $a = q*n+r$
- **Nếu** $r = 0$**, suy ra a chia hết cho n, ký hiệu:** $n|a$**.**
- **Nếu** $r \neq 0$**, thì a không chia hết cho n, ký hiệu:** $n \nmid a$.

- Ví dụ:
  - ✓ $4|44$, $13|78$, $-6|24$, $11|(-33)$.
  - ✓ $11 \nmid (-32)$, $13 \nmid 27$, $-6 \nmid 23$, $4 \nmid 41$.

SỐ HỌC CÁC SỐ NGUYÊN

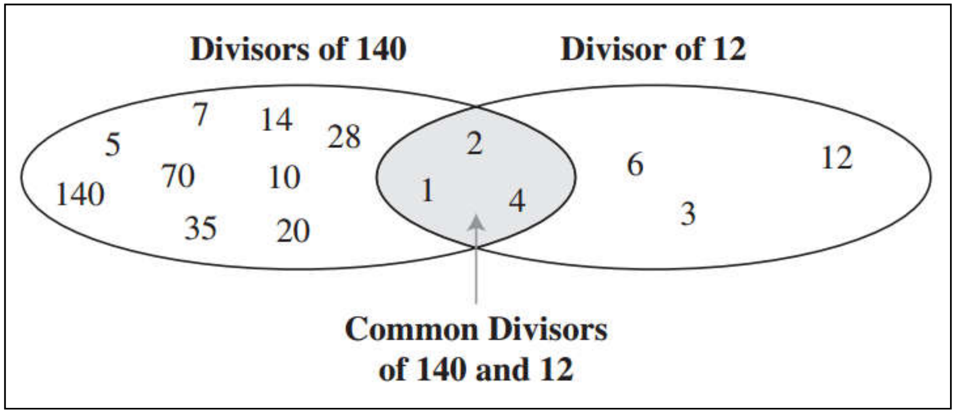
❖ Phép chia hết

➢ Một số tính chất:

- **Nếu $a|1$ thì $a = \pm 1$**
- **Nếu $a|b$ và $b|a$ thì $a = \pm b$**
- **Nếu $a|b$ và $b|c$ thì $a|c$**
- **Nếu $a|b$ và $a|c$ thì $a|(m*b+n*c)$ với m, n là hai số nguyên tùy ý.**

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

- Tìm UCLN của 140 và 12? (Ký hiệu gcd(140,12))

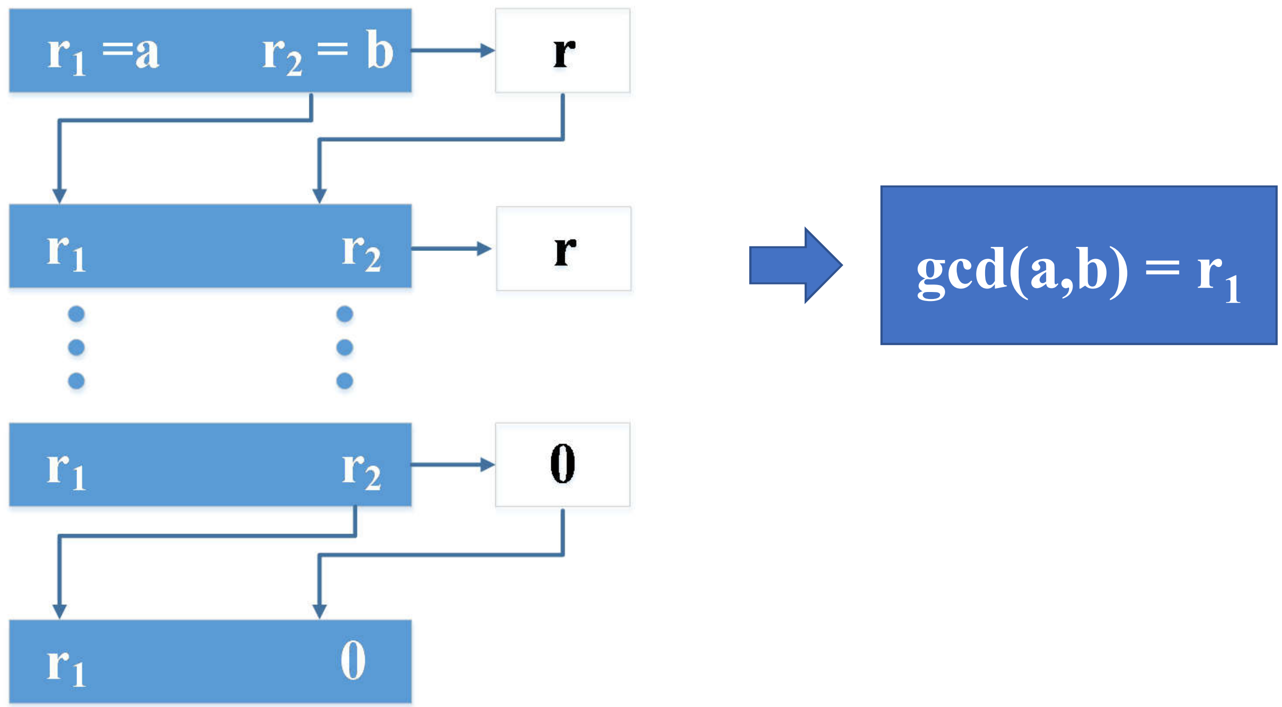


⇨ gcd(140,12)=4

Ký hiệu: d = gcd(a,b)

❖ Thuật toán Euclidean

- Mục đích: tìm gcd(a,b)



SỐ HỌC CÁC SỐ NGUYÊN

❖ Thuật toán Euclidean

gcd(a,0) = a

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

- 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**

SỐ HỌC CÁC SỐ NGUYÊN

❖ Thuật toán Euclidean

- Thực hành với MATLAB

- Viết chương trình tính UCLN của hai số nguyên: ucln.m

```
function y = ucln(a,b)
% Khoi tao
r1 = a;
r2 = b;
% Su dung vong lap while
while(r2>0)
    q = floor(r1/r2);% lam tron den so nguyen be gan nhat
    r = r1-q*r2; % Tinh so du
    r1=r2; % gan gia tri moi cho r1
    r2=r;  % gan gia tri moi cho r2
end
% y la uoc chung lon nhat cua a va b
y=r1;
```

Command Window

```
>> y = ucln(140,12)

y =

     4
```

SỐ HỌC CÁC SỐ NGUYÊN

❖ Số nguyên tố

- Một số nguyên a > 1 được gọi là số nguyên tố, nếu a không có ước số nào ngoài 1 và chính a và được gọi là hợp số , nếu không phải là số nguyên tố.
- Hai số a và b được gọi là nguyên tố với nhau, nếu chúng không có ước số chung nào khác 1, tức là nếu gcd(a,b) =1.
- Một số nguyên n > 1 bất kỳ đều có thể viết dưới dạng: $\boxed{\boldsymbol{n = p_1^{\alpha_1} * p_2^{\alpha_2} * \cdots * p_k^{\alpha_k}}}$

Trong đó p_1 , p_2 , … , p_k là các số nguyên tố khác nhau, α_1, α_2 , … , α_k là các số mũ nguyên dương.

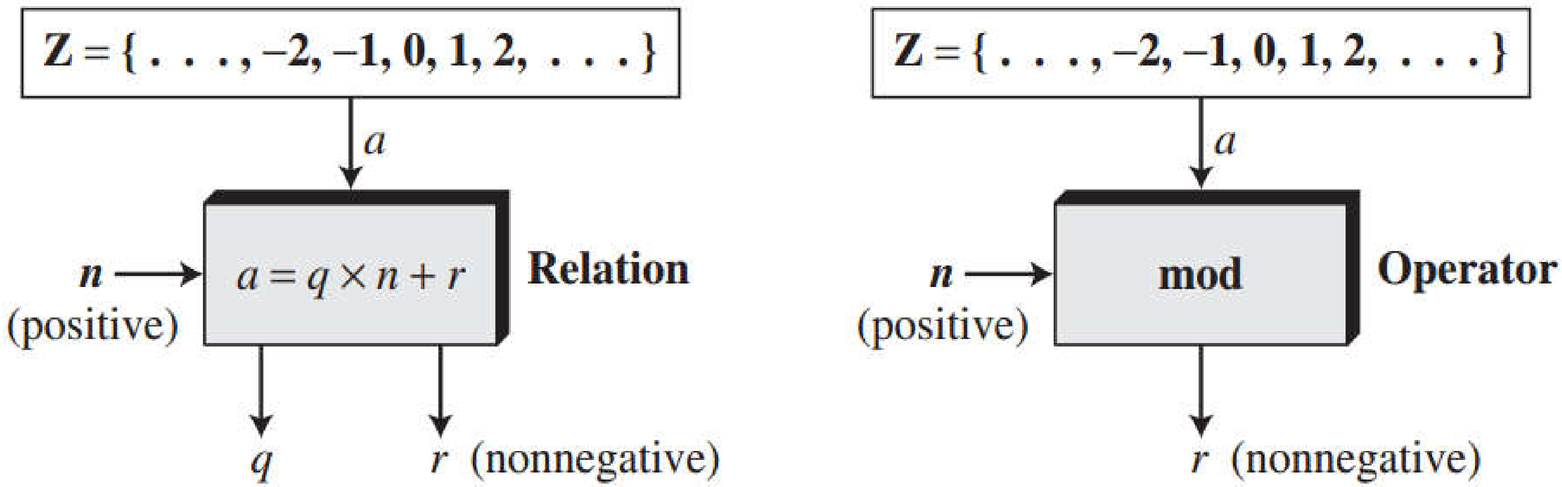
- Ví dụ: $1800 = 2^3*3^2*5^2$

NỘI DUNG

- ❖ Số học các số nguyên
- ❖ Số học Modulo
- ❖ Đồng dư tuyến tính
- ❖ Ma trận

SỐ HỌC MODULO

❖ **Toán tử Mod**



a mod n = r

SỐ HỌC MODULO

❖ Toán tử Mod

- Ví dụ:
  - 27 mod 5 = 2
  - 70 mod 7 = 0
  - -18 mod 14 = 10
  - -7 mod 10 = 3

SỐ HỌC MODULO

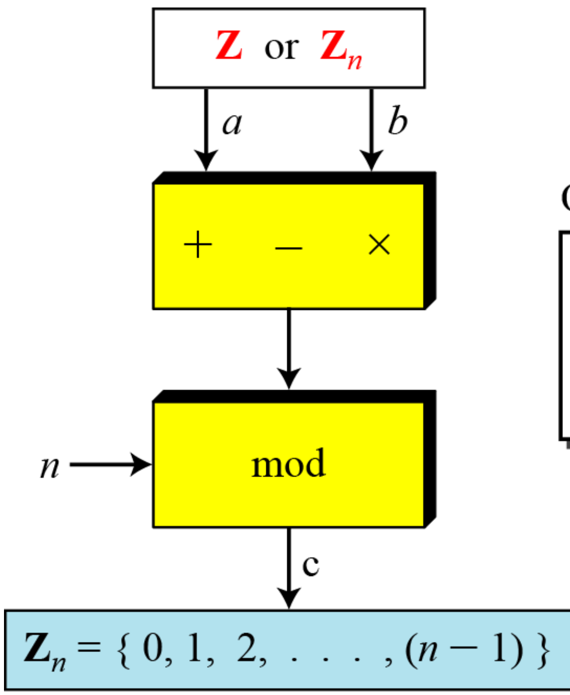
❖ Đồng dư - congruence

- Hai số nguyên a và b là đồng dư với nhau theo module n, và viết $a \equiv b \pmod{n}$, nếu $n|(a-b)$.
- Mỗi lớp tương đương được đại diện bởi một số duy nhất trong tập hợp: $Z_n = \{0, 1, 2, 3,...., n-1\}$ là số dư chung khi chia các số trong lớp đó cho n.
- Ví dụ: với $Z_{25} = \{0, 1, 2, ..., 24\}$,

15+14=29=4 (mod 25)

SỐ HỌC MODULO

❑ **Toán tử trong Z_n**



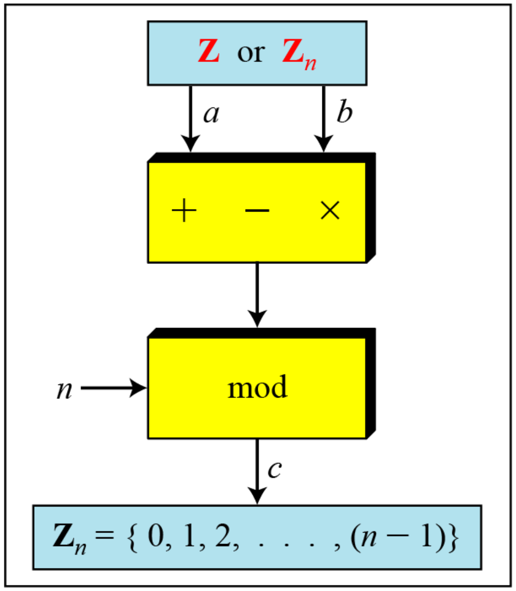
Operations

$$(a + b) \bmod n = c$$
$$(a - b) \bmod n = c$$
$$(a \times b) \bmod n = c$$

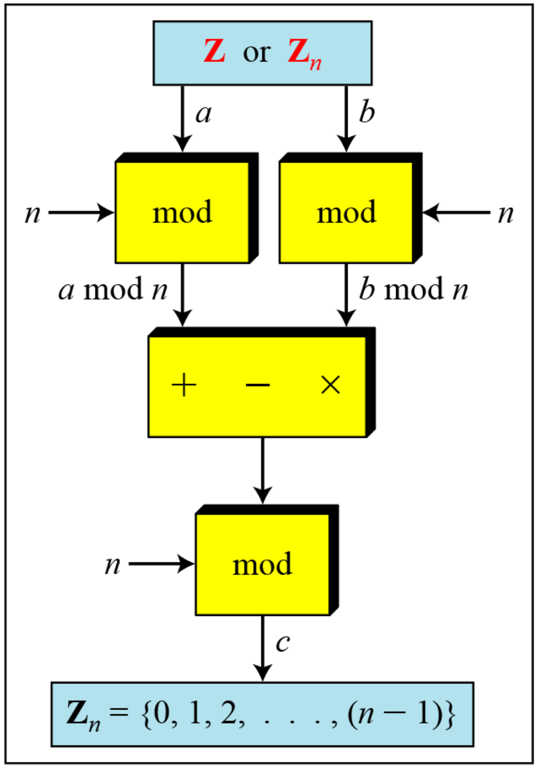
SỐ HỌC MODULO

❑ Toán tử trong Z_n

❖ Các tính chất



a. Original process



b. Applying properties

SỐ HỌC MODULO

❑ Toán tử trong Z_n

❖Các tính chất

1. (a+b) mod n = [(a mod n)+ (b mod n)] mod n

2. (a-b) mod n = [(a mod n) – (b mod n)] mod n

3. (a*b) mod n = [(a mod n) * (b mod n)] mod n

Ví dụ: (241*72) mod 23 = ((241 mod 23) * (72 mod 23)) mod 23

= (11 * 3)mod 23

= 33 mod 23 = 10

SỐ HỌC MODULO

❑ Nghịch đảo - Inverses

❖ Nghịch đảo cộng – Additive Inverses

Trong Z_n, a và b gọi là nghịch đảo cộng của nhau nếu:

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

- Trong số học modulo, mỗi một số nguyên có một nghịch đảo cộng.
- Tổng hai số nguyên là đảo cộng của nhau thì đồng dư với 0 trong modulo n
- Ví dụ: 11 là nghịch đảo cộng của 9 trong Z_{20} vì $(11+9)= 20 \equiv 0 \bmod 20$
- Trong tập Z_{10} có bao nhiêu cặp nghịch đảo cộng?

SỐ HỌC MODULO

❖ Nghịch đảo

➢ Nghịch đảo nhân – Multiplicate Inverses

- Cho $a \in Z_n$. Một số nguyên $x \in Z_n$ được gọi là nghịch đảo của a theo mod n, nếu :

$$a*x \equiv 1 \pmod{n}$$

- Nếu có số x như vậy thì ta nói a là khả nghịch, và ký hiệu x là $a^{-1} \bmod n$
- Số nguyên $a \in Z_n$ là khả nghịch khi và chỉ khi $gcd(n,a) = 1$

$$\text{vì } 22.8 = 176 \equiv 1 \pmod{25}$$

SỐ HỌC MODULO

❖ **Nghịch đảo**

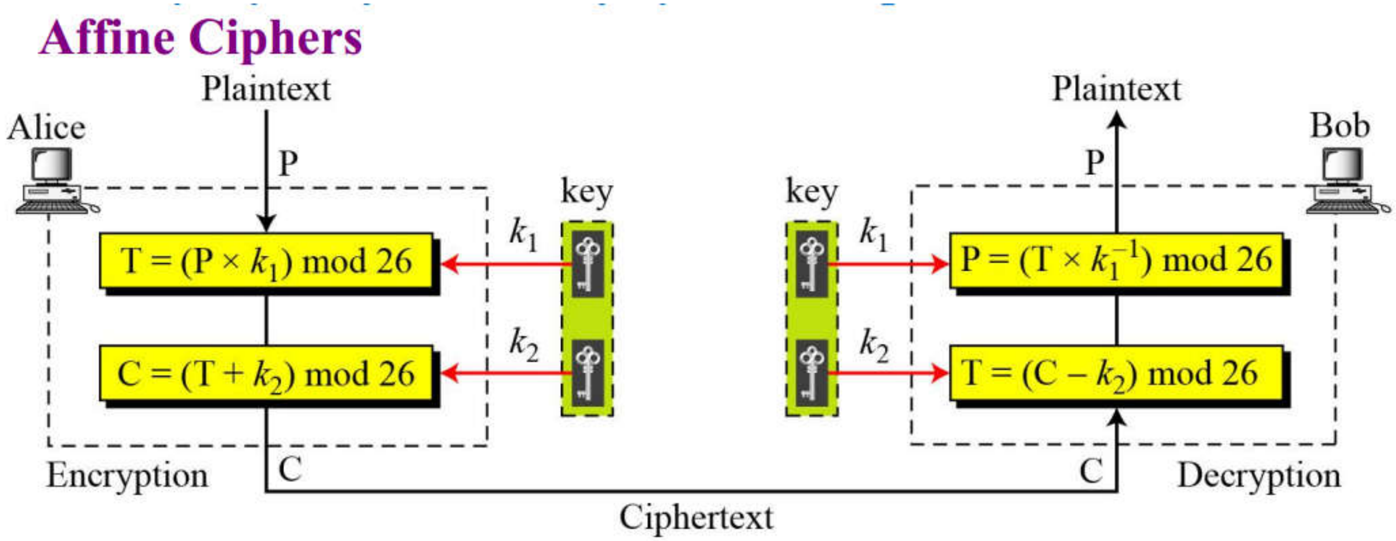
➢ **Nghịch đảo nhân – Multiplicate Inverses**

- Ví dụ: Tìm tất cả các cặp là nghịch đảo nhân của nhau trong Z_{11}.

  Có 7 cặp: (1,1), (2,6), (3,4), (5,9), (7,8), (9,9), (10,10)

❖ Nghịch đảo

➢ **Nghịch đảo nhân – Multiplicate Inverses**



$C = (P \times k_1 + k_2) \bmod 26$ $\qquad$ $P = ((C - k_2) \times k_1^{-1}) \bmod 26$

where k_1^{-1} is the multiplicative inverse of k_1 and $-k_2$ is the additive inverse of k_2

SỐ HỌC MODULO

❖ Nghịch đảo

➢ Nghịch đảo nhân – Multiplicate Inverses

- Có cặp **?** là nghịch đảo nhân của nhau trong Z_{26}.

  Có cặp 7 cặp:

  {(1,1), (3,9), (5,21), (7,15), (11,19), (17,23), (25,25)}.

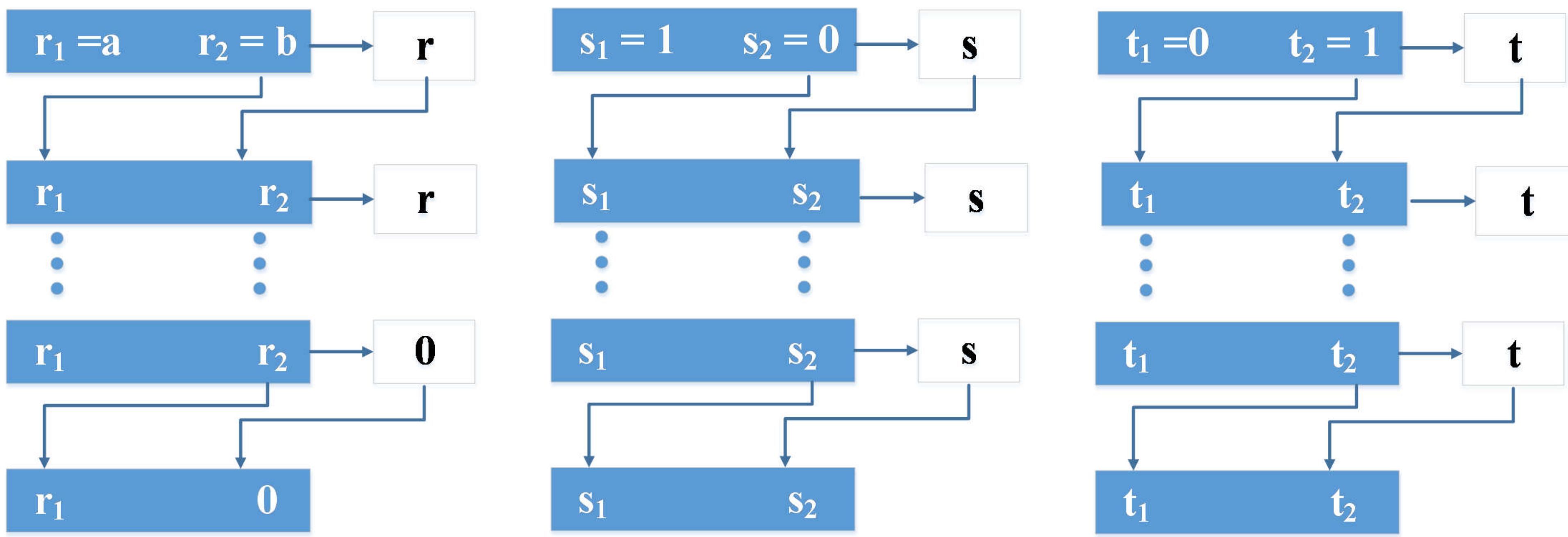
❖ Thuật toán Euclidean mở rộng

- Tính chất: Cho 2 số nguyên a và b, ta luôn tìm được 2 số nguyên s và t sao cho : $\mathbf{s \times a + t \times b = gcd(a,b)}$.
- Thuật toán Euclidean có thể tính đồng thời gcd(a,b) và giá trị ***s*** và ***t***.

SỐ HỌC MODULO

❖ **Thuật toán Euclidean mở rộng**

$$r = r_1 - q * r_2$$
$$s = s_1 - q * s_2$$
$$t = t_1 - q * t_2$$



$gcd(a,b) = r_1$ $s = s_1$ $t = t_1$

SỐ HỌC MODULO

❖ Thuật toán Euclidean mở rộng

- Ví dụ: Tìm gcd, s, t với (a,b) = (26,11)

Command Window

```
>> [d,s,t] = extendedEuclidean(26,11)

d =

     1


s =

     3


t =

    -7
```

MATLAB

extendedEuclidean.m

```
function [d,s,t] = extendedEuclidean(a,b)

% Khoi tao cac gia tri
r1 = a; r2 = b;

s1 = 1; s2 = 0;

t1=0; t2=1;
% While loop to calculate r, s, t
 while (r2>0)
     q = floor(r1/r2);

     r=r1-q*r2; r1=r2; r2=r;

     s = s1-q*s2; s1=s2; s2=s;

     t = t1-q*t2; t1=t2; t2=t;
     if (r1==1)
        break
     end
 end
     d = r1;  t = t1; s = s1;
end
```

SỐ HỌC MODULO

❖ Thuật toán Euclidean mở rộng

- Ví dụ: Cho: a=161, b=28.

Tìm gcd(a,b) và giá trị s và t?

$$\begin{aligned} r &= r_1 - q * r_2 \\ s &= s_1 - q * s_2 \\ t &= t_1 - q * t_2 \end{aligned}$$

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, $t = t_1 = 6$, $s = s_1 = -1$.

161*(-1) + 28*6 = gcd(161,28) = 7

SỐ HỌC MODULO

❖ Thuật toán Euclidean mở rộng

- Áp dụng thuật toán Euclidean để tìm nghịch đảo nhân của $\mathbf{b \in Z_n}$

\- Nếu b khả nghịch, **gcd(b,n)=1**, nên ta luôn tìm được s và t sao cho:

$$\boxed{\mathbf{s*n + t*b = 1}} \quad \mathbf{(*)}$$

$$(s*n + t*b) \bmod n = 1 \bmod n$$

$$[(s*n) \bmod n] + [(t*b) \bmod n] = 1 \bmod n$$

$$0 + [(t*b) \bmod n] = 1 \bmod n$$

$$(t \times b) \bmod n = 1$$

$$\Rightarrow \mathbf{t = b^{-1}}$$

➢ ***Như vậy, nghịch đảo nhân của $b \in Z_n$ thỏa mãn (*) là t.***

SỐ HỌC MODULO

❖ Thuật toán Euclidean mở rộng

- Áp dụng thuật toán Euclidean để tìm nghịch đảo nhân của ***b* ∈*Zn***

```
r1 = n;   r2 = b;
t1 = 0;   t2 = 1;

while (r2 > 0)
 {
  q = r1 / r2;

   r = r1 - q * r2;
   r1 = r2;   r2 = r;

   t = t1 - q * t2;
   t1 = t2;   t2 = t;

 }
  if (r1 = 1) then b^-1 = t1
```

SỐ HỌC MODULO

- Tập $\boldsymbol{Z_n} = \{0,1,2,\ldots,n-1\}$ thường được gọi là tập các thặng dư đầy đủ theo mod n.
- Tập các thặng dư thu gọn theo $mod\ n$ được định nghĩa là tập

$$Z_n^* = \{a \in \boldsymbol{Z_n}: \gcd(a, n) = 1\}$$

$\mathbf{Z}_6 = \{0, 1, 2, 3, 4, 5\}$	$\mathbf{Z}_6^* = \{1, 5\}$
$\mathbf{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$	$\mathbf{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$
$\mathbf{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$	$\mathbf{Z}_{10}^* = \{1, 3, 7, 9\}$

NỘI DUNG

- ❖ Số học các số nguyên
- ❖ Số học Modulo
- ❖ Đồng dư tuyến tính
- ❖ Ma trận

ĐỒNG DƯ TUYẾN TÍNH

- Phương trình đồng dư tuyến tính: là phương trình có dạng

$$ax \equiv b(\bmod n)$$

trong đó a, b, n là các số nguyên, n > 0, x là ẩn số

- Cách giải

 - Tính gcd(a,n)=d, nếu $d \nmid b$ thì phương trình vô nghiệm, nếu $d \mid b$ thì phương trình có d nghiệm. Các bước tìm nghiệm:

1. Chia cả hai vế cho d

2. Nhân cả hai vế với nghịch đảo của a/d, ta được nghiệm x_0

3.Các nghiệm còn lại $x = x_0 + k(\mathrm{n}/\mathrm{d})$ với k=0,1,.., (d-1)

ĐỒNG DƯ TUYẾN TÍNH

- Ví dụ: Tìm x trong phương trình đồng dư tuyến tính $\boldsymbol{3x \equiv 4(mod\ 5)}$

  ✓ Lời giải:

  - *Ta có: gcd(3,5) = 1, có 1|4.*
  - *Suy ra phương trình đã cho có 1 nghiệm.*

    Ta có: $3x \equiv 4 \pmod 5 \iff x \equiv (4*3^{-1}) \pmod 5$

  - *Lập bảng tìm nghịch đảo nhân của 3 trên modulo 5, sử dụng Euclidean mở rộng (tự lập bảng)* $\Rightarrow 3^{-1} (mod\ 5) = 2$

    $\Rightarrow x \equiv (4*3^{-1}) \pmod 5 \iff x \equiv (4*2) \pmod 5 \iff x \equiv 8 \pmod 5 \iff x = 3$

  - *Vậy phương trình đã cho có nghiệm:* $x = 3$.

NỘI DUNG

- ❖ Số học các số nguyên
- ❖ Số học Modulo
- ❖ Đồng dư tuyến tính
- ❖ Ma trận

MA TRẬN

❖ Định nghĩa

- Ma trận kích thước ***mxn*** *bao* gồm: ***m*n*** phần tử, ***m*** hàng và ***n*** cột
- Phần tử a_{ij} thuộc hàng i, cột j

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & & \vdots \\ \vdots & & a_{ij} \quad \ddots & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}_{mxn}$$

MA TRẬN

❖ Một số phép toán về ma trận

- Cộng hai ma trận
- Nhân (vô hướng) một số với ma trận với
- Phép nhân hai ma trận
- Ma trận chuyển vị

MA TRẬN

❖ Định thức

- Định thức của ma trận vuông A, kích thước $m\times m$ (kí hiệu là **det(A)**) là một số được tính theo:

1. Nếu m = 1, $\det(A) = a_{11}$

2. Nếu m > 1, $\det(A) = \sum_{i=1\ldots m} (-1)^{i+j} \times a_{ij} \times \det(A_{ij})$

Trong đó A_{ij} là ma trận A bỏ đi hàng i, cột j

- **Ma trận nghịch đảo nhân**: Ma trận vuông B được gọi là nghịch đảo của ma trận vuông A khi và chỉ khi: $A\times B=I$

MA TRẬN

❖ Ma trận thặng dư (Residue Matrices)

- Mật mã hóa thường sử dụng ma trận thặng dư: ma trận có các phần tử thuộc Z_n.
- Mọi phép toán trên ma trận thặng dư thì tương tự như trên ma trận số nguyên ngoại trừ việc các toán tử được thực trên trong số học modulo.
- Ma trận thặng dư vuông tồn tại nghịch đảo nhân khi và chỉ khi:

  gcd(det(A),n)=1.

MA TRẬN

- Ví dụ về nghịch đảo nhân ma trận thặng dư

  Ma trận A thuộc Z_{26}

$$\mathbf{A} = \begin{bmatrix} 3 & 5 & 7 & 2 \\ 1 & 4 & 7 & 2 \\ 6 & 3 & 9 & 17 \\ 13 & 5 & 4 & 16 \end{bmatrix} \qquad \mathbf{A}^{-1} = \begin{bmatrix} 15 & 21 & 0 & 15 \\ 23 & 9 & 0 & 22 \\ 15 & 16 & 18 & 3 \\ 24 & 7 & 15 & 3 \end{bmatrix}$$

$$\det(\mathbf{A}) = 21 \qquad \det(\mathbf{A}^{-1}) = 5$$

Bài 1. Cho một ma trận vuông A, tìm nghịch đảo A^{-1} trong module n.

❖ Ma trận: $A = \begin{pmatrix} 3 & 9 \\ 2 & 7 \end{pmatrix}$ trên module n = 17.

- Tìm det(A) = $\begin{vmatrix} 3 & 9 \\ 2 & 7 \end{vmatrix}$ **= 3**

  gcd(det(A), n) = gcd(3,17) = 1.

  Suy ra ma trận A tồn tại nghịch đảo trên module 17.

- $\mathbf{A^{-1}}$ **= (**det(A))$^{-1}$ *****B^T (mod 17). Với B^T là ma trận phụ đại số đã được chuyển vị.
  - ✓ Tính toán **(**det(A))$^{-1}$ **:** Tìm nghịch đảo nhân của det(A)= 3 trên module 17, sử dụng thuật toán Euclidean mở rộng. **(**det(A))$^{-1}$ mod 17 = 3^{-1}mod 17 = 6.
  - ✓ Tính ma trận phụ đại số đã được chuyển vị B^T (tự tính), $B^T = \begin{pmatrix} 7 & -9 \\ -2 & 3 \end{pmatrix}$.

Bài 1. Cho một ma trận vuông A, tìm nghịch đảo A^{-1} trong module n.

- Vậy: $A^{-1} = 6 * \begin{pmatrix} 7 & -9 \\ -2 & 3 \end{pmatrix} \pmod{17} = \begin{pmatrix} 42 & -54 \\ -12 & 18 \end{pmatrix} \bmod 17 = \begin{pmatrix} 8 & 14 \\ 5 & 1 \end{pmatrix}$

- Check again: $A * A^{-1} = \begin{pmatrix} 3 & 9 \\ 2 & 7 \end{pmatrix} * \begin{pmatrix} 8 & 14 \\ 5 & 1 \end{pmatrix} = \begin{pmatrix} 69 & 51 \\ 51 & 35 \end{pmatrix} \bmod 17 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbf{I}$

Bài 2. Problem with Hill cipher.

❖ **Encryption**: Plaintext P =“BACHKHOA”, Key: $K = \begin{bmatrix} 3 & 9 \\ 2 & 7 \end{bmatrix}$.

Encryption by Hill cipher, được bản mật ciphertext C = (P*K) mod 26.

- Kiểm tra khóa K thỏa mãn điều kiện tồn tại nghịch đảo nhân: gcd(det(K), 26) = 1.
- Plaintext: “BA CH KH OA” viết dưới dạng ma trận như sau:

$$\text{Plaintext} = \begin{bmatrix} B & A \\ C & H \\ K & H \\ O & A \end{bmatrix} \Rightarrow P = \begin{bmatrix} 1 & 0 \\ 2 & 7 \\ 10 & 7 \\ 14 & 0 \end{bmatrix}$$

✓ Lưu ý: ta có thể chèn thêm ký tự “Z” vào bản rõ khi chiều dài bản rõ khác số nguyên lần số hàng/cột của khóa.

Bài 2. Bài toán với Hill cipher

- Encrypt: C = (P*K) mod 26 = $\begin{bmatrix} 1 & 0 \\ 2 & 7 \\ 10 & 7 \\ 14 & 0 \end{bmatrix} * \begin{bmatrix} 3 & 9 \\ 2 & 7 \end{bmatrix}$mod 26

$$C = \begin{bmatrix} 3 & 9 \\ 20 & 67 \\ 44 & 139 \\ 42 & 126 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 3 & 9 \\ 20 & 15 \\ 18 & 9 \\ 16 & 22 \end{bmatrix} \Rightarrow Ciphertext = \begin{bmatrix} D & J \\ U & P \\ S & J \\ Q & W \end{bmatrix}$$

- Vậy bản mật được mật mã hóa là: ***"DJUPSJQW"***

Bài 2. Bài toán với Hill cipher

❖ **Decryption**: Ciphertext C = "DJUPSJQW", Key: K = $\begin{bmatrix} 3 & 9 \\ 2 & 7 \end{bmatrix}$. Giải mật mã hóa bằng Hill cipher, thu được bản rõ plaintext P = (C*K^{-1}) mod 26.

- Kiểm tra khóa K thỏa mãn tồn tại nghịch đảo nhân: gcd(det(K), 26) = 1, tính K^{-1}
- Ciphertext: "DJ UP SJ QW" viết dưới dạng ma trận như sau:

$$\text{Ciphertext} = \begin{bmatrix} D & J \\ U & P \\ S & J \\ Q & W \end{bmatrix} \Rightarrow \mathrm{C} = \begin{bmatrix} 3 & 9 \\ 20 & 15 \\ 18 & 9 \\ 16 & 22 \end{bmatrix}$$

Bài 2. Bài toán với Hill cipher

- Decrypt: P = (C*K^{-1}) mod 26 = $\begin{bmatrix} 3 & 9 \\ 20 & 15 \\ 18 & 9 \\ 16 & 22 \end{bmatrix} * \begin{bmatrix} 11 & 23 \\ 8 & 1 \end{bmatrix}$mod 26

$$C = \begin{bmatrix} 105 & 78 \\ 340 & 475 \\ 270 & 423 \\ 352 & 390 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 1 & 0 \\ 2 & 7 \\ 10 & 7 \\ 14 & 0 \end{bmatrix} \Rightarrow \ Plaintext = \begin{bmatrix} B & A \\ C & H \\ K & H \\ O & A \end{bmatrix}$$

- Vậy bản rõ được giải mật mã hóa là: ***"BACHKHOA"***

BÀI TẬP VỀ NHÀ THEO NHÓM

❖ NỘI DUNG: Bài tập của hai tập tài liệu:

Classical_CryptoSystem và Mathematics of Cryptography.

❖ HÌNH THỨC LÀM BÀI: báo cáo Word.

❖ HÌNH THỨC NỘP BÀI: Thông qua thư mục dropbox của nhóm trưởng.

❖ DEADLINE: Trước 23h59’, ngày 10/3/2017.

Thank you for attending!