

## Nội dung

- 1 Thuật toán Euclid
- 2 Thuật toán tính lũy thừa
- 3 Nhóm vòng và phần tử sinh



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

## Định nghĩa

- Ước chung của hai số nguyên  $a$  và  $b$  là số nguyên  $d$  thỏa mãn:

$$d \mid a \text{ và } d \mid b.$$

- Ta ký hiệu  $\text{gcd}(a, b)$  là ước chung **lớn nhất** của  $a$  và  $b$ .

## Ví dụ

- $\text{gcd}(12, 18) = 6$  vì  $6 \mid 12$  và  $6 \mid 18$  và không có số nào lớn hơn có tính chất này.
- $\text{gcd}(748, 2014) = 44$  vì

các ước của  $748 = \{1, 2, 4, 11, 17, 22, 34, 44, 68, 187, 374, 748\}$ ,  
các ước của  $2024 = \{1, 2, 4, 8, 11, 22, 23, 44, 46, 88, 92, 184, 253, 506, 1012, 2024\}$ .



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG



ĐẠI HỌC BÁCH KHOA HÀ NỘI  
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

## Nhập môn An Toàn Thông Tin

Nhắc lại một số thuật toán trong lý thuyết số

## Định nghĩa

- Ước chung của hai số nguyên  $a$  và  $b$  là số nguyên  $d$  thỏa mãn:

$$d \mid a \text{ và } d \mid b.$$

- Ta ký hiệu  $\text{gcd}(a, b)$  là ước chung **lớn nhất** của  $a$  và  $b$ .



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

## Định lý (Thuật toán Euclid)

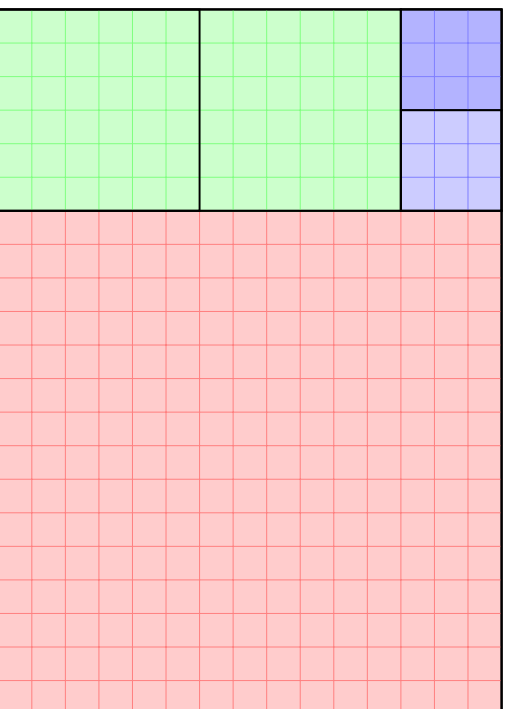
Xét  $a, b$  là hai số nguyên dương với  $a \geq b$ . Thuật toán sau đây tính  $\gcd(a, b)$  sau một số hữu hạn bước.

- 1 Đặt  $r_0 = a$  và  $r_1 = b$ .
- 2 Đặt  $i = 1$ .
- 3 Chia  $r_{i-1}$  cho  $r_i$ , ta được
$$r_{i-1} = r_i \cdot q_i + r_{i+1} \quad \text{với} \quad 0 \leq r_{i+1} < r_i.$$
- 4 Nếu  $r_{i+1} = 0$ , vậy thì
$$r_i = \gcd(a, b)$$

và thuật toán kết thúc.

- 5 Ngược lại,  $r_{i+1} > 0$ , vậy thì đặt  $i = i + 1$  và quay lại Bước 3.

$$\gcd(21, 15) = \gcd(15, 6) = \gcd(6, 3)$$



## Thuật toán Euclid (dạng đệ quy)

```
EUCLID( $a, b$ )  
  if  $b == 0$   
    return  $a$   
  else  
    return EUCLID( $b, a \bmod b$ )
```

## Định lý

Phép chia (Bước 3) của Thuật toán Euclid thực hiện nhiều nhất

$$\log_2(b) + 2 \text{ lần.}$$

## Thuật toán Euclid mở rộng

- *Input* : Cặp số nguyên dương  $(a, b)$
- *Output*: Bộ ba  $(d, x, y)$  thỏa mãn

$$d = \gcd(a, b) = ax + by.$$

EXTENDED-EUCLID( $a, b$ )

if  $b == 0$

return  $(a, 1, 0)$

else

$(d', x', y') = \text{EXTENDED-EUCLID}(b, a \bmod b)$

$(d, x, y) = (d', y', x' - \lfloor a/b \rfloor y')$

return  $(d, x, y)$



## Ví dụ

$$\begin{array}{r} a \quad b \quad \lfloor a/b \rfloor \quad d \quad x \quad y \\ 99 \quad 78 \quad 1 \end{array}$$

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào  $a$  và  $b$ , giá trị tính  $\lfloor a/b \rfloor$ , và giá trị trả về  $d, x, y$ .
- Bộ ba  $d, x, y$  được trả về trở thành bộ ba  $d', x', y'$  của mức tiếp theo từ công thức

$$x = y'$$

$$y = x' - \lfloor a/b \rfloor y'$$



## Thuật toán Euclid mở rộng

- Thuật toán Euclid có thể mở rộng để tìm thêm một số thông tin.
- Cụ thể, chúng ta mở rộng thuật toán để tính thêm hệ số  $x, y$  thỏa mãn
$$d = \gcd(a, b) = ax + by.$$
- Các hệ số  $x, y$  có thể âm hoặc bằng 0. Các hệ số này sẽ có ích sau này khi tích phân tử nghịch đảo trong số học modun.

## Tính đúng đắn của thuật toán

- Thuật toán tìm  $(d, x, y)$  thỏa mãn
$$d = \gcd(a, b) = ax + by$$
- Nếu  $b = 0$ , vậy thì
$$d = a = a \cdot 1 + b \cdot 0.$$
- Nếu  $b \neq 0$ , thuật toán EXTENDED-EUCLID sẽ tính  $(d', x', y')$  thỏa mãn

$$\begin{aligned} d' &= d = \gcd(b, a \bmod b) \\ &= bx' + (a \bmod b)y' \end{aligned}$$

- Và vậy thì

$$\begin{aligned} d &= b'x' + (a - b\lfloor a/b \rfloor)y' \\ &= ay' + b(x' - \lfloor a/b \rfloor y') \end{aligned}$$



## Ví dụ

$a$	$b$	$\lfloor a/b \rfloor$	$d$	$x$	$y$
99	78	1			
78	21	3			
21	15	1			

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào  $a$  và  $b$ , giá trị tính  $\lfloor a/b \rfloor$ , và giá trị trả về  $d, x, y$ .
- Bộ ba  $d, x, y$  được trả về trở thành bộ ba  $d', x', y'$  của mức tiếp theo từ công thức

$$x = y'$$

$$y = x' - \lfloor a/b \rfloor y'$$



## Ví dụ

$a$	$b$	$\lfloor a/b \rfloor$	$d$	$x$	$y$
99	78	1			
78	21	3			
21	15	1			
15	6	2			
6	3	2			

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào  $a$  và  $b$ , giá trị tính  $\lfloor a/b \rfloor$ , và giá trị trả về  $d, x, y$ .
- Bộ ba  $d, x, y$  được trả về trở thành bộ ba  $d', x', y'$  của mức tiếp theo từ công thức

$$x = y'$$

$$y = x' - \lfloor a/b \rfloor y'$$



## Ví dụ

$a$	$b$	$\lfloor a/b \rfloor$	$d$	$x$	$y$
99	78	1			
78	21	3			

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào  $a$  và  $b$ , giá trị tính  $\lfloor a/b \rfloor$ , và giá trị trả về  $d, x, y$ .
- Bộ ba  $d, x, y$  được trả về trở thành bộ ba  $d', x', y'$  của mức tiếp theo từ công thức

$$x = y'$$

$$y = x' - \lfloor a/b \rfloor y'$$



## Ví dụ

$a$	$b$	$\lfloor a/b \rfloor$	$d$	$x$	$y$
99	78	1			
78	21	3			
21	15	1			
15	6	2			

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào  $a$  và  $b$ , giá trị tính  $\lfloor a/b \rfloor$ , và giá trị trả về  $d, x, y$ .
- Bộ ba  $d, x, y$  được trả về trở thành bộ ba  $d', x', y'$  của mức tiếp theo từ công thức

$$x = y'$$

$$y = x' - \lfloor a/b \rfloor y'$$



## Ví dụ

$a$	$b$	$\lfloor a/b \rfloor$	$d$	$x$	$y$
99	78	1			
78	21	3			
21	15	1			
15	6	2			
6	3	2			
3	0	–	3	1	0

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào  $a$  và  $b$ , giá trị tính  $\lfloor a/b \rfloor$ , và giá trị trả về  $d, x, y$ .
- Bộ ba  $d, x, y$  được trả về trở thành bộ ba  $d', x', y'$  của mức tiếp theo từ công thức

$$x = y'$$

$$y = x' - \lfloor a/b \rfloor y'$$



## Ví dụ

$a$	$b$	$\lfloor a/b \rfloor$	$d$	$x$	$y$
99	78	1			
78	21	3			
21	15	1			
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	–	3	1	0

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào  $a$  và  $b$ , giá trị tính  $\lfloor a/b \rfloor$ , và giá trị trả về  $d, x, y$ .
- Bộ ba  $d, x, y$  được trả về trở thành bộ ba  $d', x', y'$  của mức tiếp theo từ công thức

$$x = y'$$

$$y = x' - \lfloor a/b \rfloor y'$$



## Ví dụ

$a$	$b$	$\lfloor a/b \rfloor$	$d$	$x$	$y$
99	78	1			
78	21	3			
21	15	1			
15	6	2			
6	3	2			
3	0	–			

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào  $a$  và  $b$ , giá trị tính  $\lfloor a/b \rfloor$ , và giá trị trả về  $d, x, y$ .
- Bộ ba  $d, x, y$  được trả về trở thành bộ ba  $d', x', y'$  của mức tiếp theo từ công thức

$$x = y'$$

$$y = x' - \lfloor a/b \rfloor y'$$



## Ví dụ

$a$	$b$	$\lfloor a/b \rfloor$	$d$	$x$	$y$
99	78	1			
78	21	3			
21	15	1			
15	6	2			
6	3	2	3	0	1
3	0	–	3	1	0

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào  $a$  và  $b$ , giá trị tính  $\lfloor a/b \rfloor$ , và giá trị trả về  $d, x, y$ .
- Bộ ba  $d, x, y$  được trả về trở thành bộ ba  $d', x', y'$  của mức tiếp theo từ công thức

$$x = y'$$

$$y = x' - \lfloor a/b \rfloor y'$$



Ví dụ

$a$	$b$	$\lfloor a/b \rfloor$	$d$	$x$	$y$
99	78	1			
78	21	3	3	3	-11
21	15	1	3	-2	3
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	-	3	1	0

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào  $a$  và  $b$ , giá trị tính  $\lfloor a/b \rfloor$ , và giá trị trả về  $d, x, y$ .
- Bộ ba  $d, x, y$  được trả về trở thành bộ ba  $d', x', y'$  của mức tiếp theo từ công thức

$$x = y'$$

$$y = x' - \lfloor a/b \rfloor y'$$

Ví dụ

$a$	$b$	$\lfloor a/b \rfloor$	$d$	$x$	$y$
99	78	1			
78	21	3			
21	15	1	3	-2	3
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	-	3	1	0

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào  $a$  và  $b$ , giá trị tính  $\lfloor a/b \rfloor$ , và giá trị trả về  $d, x, y$ .
- Bộ ba  $d, x, y$  được trả về trở thành bộ ba  $d', x', y'$  của mức tiếp theo từ công thức

$$x = y'$$

$$y = x' - \lfloor a/b \rfloor y'$$

Bài tập

Hãy tính giá trị

$$(d, x, y) = \text{EXTENDED-EUCLID}(899, 493).$$

Ví dụ

$a$	$b$	$\lfloor a/b \rfloor$	$d$	$x$	$y$
99	78	1	3	-11	14
78	21	3	3	3	-11
21	15	1	3	-2	3
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	-	3	1	0

- Mỗi dòng của bảng mô tả một mức đệ quy: các giá trị đầu vào  $a$  và  $b$ , giá trị tính  $\lfloor a/b \rfloor$ , và giá trị trả về  $d, x, y$ .
- Bộ ba  $d, x, y$  được trả về trở thành bộ ba  $d', x', y'$  của mức tiếp theo từ công thức

$$x = y'$$

$$y = x' - \lfloor a/b \rfloor y'$$

## Tính nghịch đảo theo modun

- *Input* : Số  $n > 0$  và số  $a \in \mathbb{Z}_n$  sao cho  $\gcd(a, n) = 1$
- *Output*: Số  $b$  thoả mãn  $a \cdot b \equiv 1 \pmod n$ .

MOD-INV ( $a, n$ )

$(d, x, y) = \text{EXTENDED-EUCLID}(a, n)$

$b = x \pmod n$

**return**  $b$



## Tính nghịch đảo

- Xét  $n > 1$ , nếu  $\gcd(a, n) = 1$  thì ta có
$$\gcd(a, n) = 1 = ax + ny$$
- Vậy  $ax \equiv 1 \pmod n$ . Tức là

$$x \equiv a^{-1} \pmod n$$



Ví dụ: Tính  $5^{-1} \pmod{12}$

$a$	$b$	$\lfloor a/b \rfloor$	$d$	$x$	$y$
5	12	0			
12	5	2			



Ví dụ: Tính  $5^{-1} \pmod{12}$

$a$	$b$	$\lfloor a/b \rfloor$	$d$	$x$	$y$
5	12	0			



Ví dụ: Tính  $5^{-1} \bmod 12$

$a$	$b$	$[a/b]$	$d$	$x$	$y$
5	12	0			
12	5	2			
5	2	2			
2	1	2			



Ví dụ: Tính  $5^{-1} \bmod 12$

$a$	$b$	$[a/b]$	$d$	$x$	$y$
5	12	0			
12	5	2			
5	2	2			
2	1	2			
1	0	–	1	1	0



Ví dụ: Tính  $5^{-1} \bmod 12$

$a$	$b$	$[a/b]$	$d$	$x$	$y$
5	12	0			
12	5	2			
5	2	2			



Ví dụ: Tính  $5^{-1} \bmod 12$

$a$	$b$	$[a/b]$	$d$	$x$	$y$
5	12	0			
12	5	2			
5	2	2			
2	1	2			
1	0	–			





Ví dụ: Tính  $5^{-1} \bmod 12$

$a$	$b$	$[a/b]$	$d$	$x$	$y$
5	12	0			
12	5	2			
5	2	2	1	1	-2
2	1	2	1	0	1
1	0	-	1	1	0



Ví dụ: Tính  $5^{-1} \bmod 12$

$a$	$b$	$[a/b]$	$d$	$x$	$y$
5	12	0	1	5	-2
12	5	2	1	-2	5
5	2	2	1	1	-2
2	1	2	1	0	1
1	0	-	1	1	0



Ví dụ: Tính  $5^{-1} \bmod 12$

$a$	$b$	$[a/b]$	$d$	$x$	$y$
5	12	0			
12	5	2			
5	2	2			
2	1	2	1	0	1
1	0	-	1	1	0

Ví dụ: Tính  $5^{-1} \bmod 12$

$a$	$b$	$[a/b]$	$d$	$x$	$y$
5	12	0			
12	5	2	1	-2	5
5	2	2	1	1	-2
2	1	2	1	0	1
1	0	-	1	1	0



# Tính lũy thừa nhanh

## Ví dụ

Giả sử ta muốn tính

$$3^{218} \pmod{1000}.$$

Đầu tiên, ta viết 218 ở dạng cơ số 2:

$$218 = 2 + 2^3 + 2^4 + 2^6 + 2^7.$$

Vậy thì  $3^{218}$  trở thành

$$3^{218} = 3^{2+2^3+2^4+2^6+2^7} = 3^2 \cdot 3^{2^3} \cdot 3^{2^4} \cdot 3^{2^6} \cdot 3^{2^7}.$$

Để ý rằng, để tính các mũ

$$3, 3^2, 3^{2^2}, 3^{2^3}, 3^{2^4}, \dots$$

# Thuật toán tính nhanh $a^b \pmod{n}$

Modular-Exponentiation( $a, b, n$ )

$$c = 0$$

$$d = 1$$

Biểu diễn  $b = \langle b_k, b_{k-1}, \dots, b_0 \rangle_2$

for  $i = k$  downto 0

$$c = 2c$$

$$d = (d \cdot d) \pmod{n}$$

if  $b_i == 1$  then

$$c = c + 1$$

$$d = (d \cdot a) \pmod{n}$$

return  $d$

# Nội dung

## 1 Thuật toán Euclid

## 2 Thuật toán tính lũy thừa

## 3 Nhóm vòng và phần tử sinh

## Ví dụ (tiếp)

Ta lập bảng

$i$	0	1	2	3	4	5	6	7
$3^{2^i} \pmod{1000}$	3	9	81	561	721	841	281	961

rồi tính

$$3^{218} = 3^2 \cdot 3^{2^3} \cdot 3^{2^4} \cdot 3^{2^6} \cdot 3^{2^7}$$

$$\equiv 9 \cdot 561 \cdot 721 \cdot 281 \cdot 961 \pmod{1000}$$

$$\equiv 489 \pmod{1000}.$$

# Thuật toán tính nhanh $a^b \pmod n$

Modular-Exponentiation( $a, b, n$ )

$c = 0$

$d = 1$

Biểu diễn  $b = \langle b_k, b_{k-1}, \dots, b_0 \rangle_2$

for  $i = k$  downto 0

$c = 2c$

$d = (d \cdot d) \pmod n$

if  $b_i == 1$  then

$c = c + 1$

$d = (d \cdot a) \pmod n$

return  $d$

- Giá trị của  $c$  bằng  $\langle b_k, b_{k-1}, \dots, b_{i+1} \rangle_2$
- và  $d = a^c \pmod n$ .

# Thuật toán đệ quy tính $a^b \pmod n$

Modular-Exponentiation( $a, b, n$ )

if  $b == 0$  then return 1

if  $b == 1$  then return  $a$

$r = \text{Modular-Exponentiation}(a, b/2, n)$

$r = r * r$

if  $b \bmod 2 == 1$  then  $r = r * a$

return  $r$

# Thuật toán tính nhanh $a^b \pmod n$

Modular-Exponentiation( $a, b, n$ )

$c = 0$

$d = 1$

Biểu diễn  $b = \langle b_k, b_{k-1}, \dots, b_0 \rangle_2$

for  $i = k$  downto 0

$c = 2c$

$d = (d \cdot d) \pmod n$

if  $b_i == 1$  then

$c = c + 1$

$d = (d \cdot a) \pmod n$

return  $d$

- Giá trị của  $c$  bằng  $\langle b_k, b_{k-1}, \dots, b_{i+1} \rangle_2$

Ví dụ  
Tính  $7^{560} \pmod{561}$

$i$	9	8	7	6	5	4	3	2	1	0
$b_i$	1	0	0	0	1	1	0	0	0	0
$c$	1	2	4	8	17	35	70	140	280	560
$d$	7	49	157	526	160	241	298	166	67	1

- Kết quả tính  $a^b \pmod n$  với

$a = 7, \quad b = 560 = (1000110000)_2$ , và  $n = 561$

- Kết quả cuối cùng bằng 1

## Nội dung

- 1 Thuật toán Euclid
- 2 Thuật toán tính lũy thừa
- 3 Nhóm vòng và phần tử sinh



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

## Cấp của một phần tử

Xét  $G$  là một nhóm (hữu hạn) với phần tử đơn vị 1.

**Định nghĩa**

**Cấp** của phần tử  $g \in G$ , ký hiệu  $o(g)$ , là số nguyên  $n \geq 1$  nhỏ nhất thoả mãn  $g^n = 1$ .



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

25 / 34

## Nhóm con

### Bài tập

Giả sử bạn biết  $\varphi(n)$ , hãy chỉ ra cách tính  $a^{-1} \pmod n$  cho mọi  $a \in \mathbb{Z}_n^*$  dùng thuật toán Modular-Exponentiation.

Gợi ý: Nhắc lại rằng  $a^{\varphi(n)} = 1 \pmod n$ .

**Định nghĩa**

Xét nhóm  $G$  và  $S \subseteq G$ . Khi đó  $S$  được gọi là **nhóm con** của  $G$  nếu  $S$  là một nhóm dưới phép toán của  $G$ .

**Ví dụ**

Xét  $G = \mathbb{Z}_{11}^*$  và  $S = \{1, 2, 3\}$ . Khi đó  $S$  không phải là nhóm con vì

- $2 \cdot 3 \pmod{11} = 6 \notin S$ , vi phạm tính chất đóng.
- $3^{-1} \pmod{11} = 4 \notin S$ , vi phạm tính khả nghịch.

Tuy nhiên  $\{1, 3, 4, 5, 9\}$  là một nhóm con. Bạn có thể kiểm tra!



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

22 / 34



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

24 / 34

## Nhóm con sinh bởi $g \in G$

### Định nghĩa

Cho phần tử  $g \in G$  có cấp  $n$ , ta đặt

$$\langle g \rangle = \{g^0, g^1, \dots, g^{n-1}\}.$$

Đây là một nhóm con của  $g$  và cấp của nó chính là  $o(g) = n$ .



## Nhóm con sinh bởi một phần tử

Xét  $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ .

$i$	0	1	2	3	4	5	6	7	8	9	10
$2^i \bmod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \bmod 11$	1	5	3	4	9	1	5	3	4	9	1

Khi đó

$$\langle 2 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$\langle 5 \rangle = \{1, 3, 4, 5, 9\}.$$



## Xác định cấp của phần tử

Xét  $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ .

$i$	0	1	2	3	4	5	6	7	8	9	10
$2^i \bmod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \bmod 11$	1	5	3	4	9	1	5	3	4	9	1

Cấp  $o(a)$  của phần tử  $a$  là số  $n \geq 1$  nhỏ nhất sao cho  $a^n = 1$ . Bởi vậy

- $o(2) = 10$
- $o(5) = 5$ .

## Cấp của nhóm con

### Mệnh đề

Cấp  $|S|$  của nhóm con  $S \subseteq G$  luôn là ước của cấp  $|G|$  của nhóm  $G$ .

### Mệnh đề

Cấp  $o(g)$  của  $g$  luôn là ước của  $|G|$ .

### Ví dụ

Nếu  $G = \mathbb{Z}_{11}^*$  thì

- $|G| = 10$
- $o(2) = 10$  là ước của 10
- $o(5) = 5$  là ước của 10



## Phần tử sinh

Xét  $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ .

$i$	0	1	2	3	4	5	6	7	8	9	10
$2^i \bmod 11$	1	2	4	8	5	10	9	7	3	6	1
$5^i \bmod 11$	1	5	3	4	9	1	5	3	4	9	1

Khi đó

$$\langle 2 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$\langle 5 \rangle = \{1, 3, 4, 5, 9\}.$$

- Liệu 2 có phải phần tử sinh?
- Liệu 5 có phải phần tử sinh?
- Nhóm  $\mathbb{Z}_{11}^*$  có phải nhóm vòng?



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

31 / 34

## Phần tử sinh

### Định nghĩa

Phần tử  $g \in G$  là một phần tử sinh (hoặc phần tử nguyên thủy) nếu  $\langle g \rangle = G$ .

### Mệnh đề

$g$  là phần tử sinh nếu và chỉ nếu  $o(g) = G$ .

### Định nghĩa

$G$  là nhóm vòng nếu nó có phần tử sinh.



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

30 / 34

## Logarit rời rạc

Xét  $G = \mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ . Ta biết rằng 2 là một phần tử sinh.

$i$	0	1	2	3	4	5	6	7	8	9	10
$2^i \bmod 11$	1	2	4	8	5	10	9	7	3	6	1

$a$	1	2	3	4	5	6	7	8	9	10
$\text{DLog}_{\mathbb{Z}_{11}^*, 2}(a)$	0	1	8	2	4	9	7	3	6	5



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

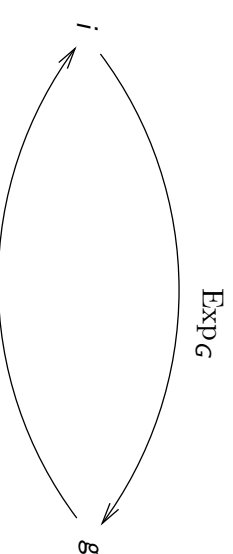
33 / 34

## Logarit rời rạc

Nếu  $G = \langle g \rangle$  là nhóm vòng thì với mọi phần tử  $a \in G$  có duy nhất số mũ  $i \in \{0, \dots, |G| - 1\}$  thoả mãn  $g^i = a$ . Ta gọi  $i$  là logarit rời rạc cơ sở  $g$  của  $a$  và ký hiệu

$$\text{DLog}_{G, g}(a)$$

Logarit rời rạc là hàm ngược của hàm mũ.



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

32 / 34



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG  
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY



soict.hust.edu.vn / fb.com/groups/soict

