

# BÀI GIẢNG AN TOÀN & BẢO MẬT THÔNG TIN CHƯƠNG 3-SỐ HỌC ĐỒNG DƯ

TS. NGUYỄN ĐÌNH DƯƠNG  
BỘ MÔN KHMT - KHOA CÔNG NGHỆ THÔNG TIN

Email: duongnd@utc.edu.vn

Ngày 03/07/2022

# Nội dung

## Số học đồng dư

- 1.2 Quan hệ đồng dư
- 1.3 The Euclidean Algorithm
- 1.4 Hàm số Euler
- 1.5 Một số định lí số học cơ bản

## Trao đổi

# Nội dung

## Số học đồng dư

- 1.2 Quan hệ đồng dư
- 1.3 The Euclidean Algorithm
- 1.4 Hàm số Euler
- 1.5 Một số định lí số học cơ bản

## Trao đổi

# 1. Số học đồng dư

## 1. 2. Quan hệ đồng dư

- What is the remainder when 51 is divided by 7? Answer: 2

We write  $51 \equiv 2 \pmod{7}$  and say "51 is congruent to 2 modulo 7"

This means that 51 and 2 have the same remainder when divided by 7.

In other words, 51 and 2 differ by a multiple of 7, or  $51 - 2 = 49$  is a multiple of 7.

- In general, if  $a, b$  and  $n$  are integers,

$$a \equiv b \pmod{n}, \quad "a \text{ is congruent to } b \text{ modulo } n"$$

means that

$a$  and  $b$  differ by a multiple of  $n$ , or  $a - b = kn$ , where  $k$  is some integer.

- We will be interested in **the smallest integer  $b \geq 0$  such that  $a - b = kn$ , where  $k$  is some integer.**

# 1. Số học đồng dư

## 1. 2. Quan hệ đồng dư

### Ví dụ 1.1

Tính

- a)  $52 \text{ mod } 8$     4
- b)  $41 \text{ mod } 5$     1
- c)  $84 \text{ mod } 4$     0
- d)  $-17 \text{ mod } 4$     -1
- e)  $145672 \text{ mod } 13$     7

# 1. Số học đồng dư

## 1. 2. Quan hệ đồng dư

- $28 \equiv 4 \pmod{8}$  and  $11 \equiv 3 \pmod{8}$ .

What happens when we add or subtract?

- $28 + 11 = 39 \equiv 7 \pmod{8}$ .

Also notice:  $28 \equiv 4 \pmod{8}$  and  $11 \equiv 3 \pmod{8}$  and  $3 + 4 = 7 \equiv 7 \pmod{8}$ .

- $28 - 11 = 17 \equiv 1 \pmod{8}$ .

Also notice:  $28 \equiv 4 \pmod{8}$  and  $11 \equiv 3 \pmod{8}$  and  $4 - 3 = 1 \equiv 1 \pmod{8}$ .

- **Tổng quát:** If  $a \equiv A \pmod{n}$  and  $b \equiv B \pmod{n}$ , then

- $a + b \equiv A + B \pmod{n}$
- $a - b \equiv A - B \pmod{n}$
- $a \times b \equiv A \times B \pmod{n}$

## Luyện tập

- ① Reduce 237288 modulo 5
- ② Reduce  $192 + 118$  modulo 5
- ③ Reduce  $192 - 118$  modulo 5
- ④ Reduce  $118 - 192$  modulo 5
- ⑤ Today is a Wednesday. What day of the week will it be
  - a) 100 days from now?
  - b) 365 days from now?
  - c) 1000 days from now?
- ⑥ Emily celebrated her 13th birthday on Wednesday, February 19th, 2014. On what day of the week was she born? (Don't forget about the leap years in 2004, 2008 and 2012!)

# 1. Số học đồng dư

## 1. 2. Quan hệ đồng dư

Đáp số:

- ①  $237288 \equiv 3 \pmod{5}$
- ②  $192 + 118 \equiv 0 \pmod{5}$
- ③  $192 - 118 \equiv 4 \pmod{5}$
- ④  $118 - 192 \equiv 1 \pmod{5}$
- ⑤
  - a) Friday
  - b) Thursday
  - c) Tuesday
- ⑥ Monday

# 1. Số học đồng dư

## 1. 2. Quan hệ đồng dư

### Định nghĩa 1.1

The number  $a$  is equivalent (congruent) to the number  $b$  modulo  $n$ , expressed by  $a \equiv b \pmod{n}$ , if  $a$  differs from  $b$  by an exact multiple of  $n$ .

### Bổ đề 1.1

*The following statements hold:*

- If  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n}$ , then  $a + c \equiv b + d \pmod{n}$ .
- If  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n}$ , then  $ac \equiv bd \pmod{n}$ .

### Ví dụ 1.2

a)  $321 \times 741 \equiv 1 \times 1 \equiv 1 \pmod{5}$

b)  $715^{10000} \equiv 1 \pmod{7}$ .

c)  $321^3 = 6^3 \pmod{7} = 36 \times 6 \pmod{7} = 6 \pmod{7}$ .

## Ví dụ 1.3

Reduce  $320^{984} \equiv 1 \pmod{7}$

We first write down the binary expression of 984, i.e.

$$984 = 512 + 256 + 128 + 64 + 16 + 8 = 2^9 + 2^8 + 2^7 + 2^6 + 2^4 + 2^3.$$

Note that  $320^{984} \equiv 5^{984} \pmod{7}$ . Moreover, we have the following:

- |  |  |
|--|--|
| <ul style="list-style-type: none"><li>• <math>5^2 = 25 \equiv 4 \pmod{7}</math></li><li>• <math>5^4 = 4 \times 4 \pmod{7} \equiv 2 \pmod{7}</math></li><li>• <math>5^8 = 2 \times 2 \pmod{7} \equiv 4 \pmod{7}</math></li><li>• <math>5^{16} = 4 \times 4 \pmod{7} = 2 \pmod{7}</math></li><li>• <math>5^{32} \equiv 4 \pmod{7}</math></li></ul> | <ul style="list-style-type: none"><li>• <math>5^{64} \equiv 2 \pmod{7}</math></li><li>• <math>5^{128} \equiv 4 \pmod{7}</math></li><li>• <math>5^{256} \equiv 2 \pmod{7}</math></li><li>• <math>5^{512} \equiv 4 \pmod{7}</math></li></ul> |
|--|--|

Hence

$$\begin{aligned}5^{984} &= 5^{512+256+128+64+16+8} \pmod{7} \\&\equiv 4 \times 2 \times 4 \times 2 \times 2 \times 2 \times 4 \pmod{7} \\&\equiv 1 \pmod{7}\end{aligned}$$

# 1. Số học đồng dư

## 1. 3. The Euclidean Algorithm

- Given two integers  $r_0$  and  $r_1$ , the Euclidean Algorithm finds the greatest common divisor of  $r_0$  and  $r_1$ , denoted by  $\gcd(r_0, r_1)$ .

Bổ đề 1.2

$$\gcd(r_0, r_1) = \gcd(r_1, r_0 \bmod r_1)$$

# 1. Số học đồng dư

## 1. 3. The Euclidean Algorithm (tiếp tục)

### Định lý 1.1 (The Euclidean Algorithm)

*Given two integers  $0 < b < a$ , we make a repeated application of the division algorithm to obtain a series of division equations, which eventually terminate with a zero remainder:*

$$a = bq_1 + r_1, 0 < r_1 < b$$

$$b = r_1q_2 + r_2, 0 < r_2 < r_1$$

...

$$r_{j-2} = r_{j-1}q_j + r_j, 0 < r_j < r_{j-1}$$

$$r_{j-1} = r_jq_{j+1}$$

*The greatest common divisor  $\gcd(a, b)$  of  $a$  and  $b$  is  $r_j$ , the last nonzero remainder in the division process.*

# 1. Số học đồng dư

## 1. 3. The Euclidean Algorithm

Ví dụ 1.4

Tính gcd (1970, 1966).

$$\begin{array}{llll} 1970 & = & 1 \times 1066 + 904 & \rightarrow \quad \text{gcd}(1066, 904) \\ 1066 & = & 1 \times 904 + 162 & \rightarrow \quad \text{gcd}(904, 162) \\ 904 & = & 5 \times 162 + 94 & \rightarrow \quad \text{gcd}(162, 94) \\ 162 & = & 1 \times 94 + 68 & \rightarrow \quad \text{gcd}(94, 68) \\ 94 & = & 1 \times 68 + 26 & \rightarrow \quad \text{gcd}(68, 26) \\ 68 & = & 2 \times 26 + 16 & \rightarrow \quad \text{gcd}(26, 16) \\ 26 & = & 1 \times 16 + 10 & \rightarrow \quad \text{gcd}(16, 10) \\ 16 & = & 1 \times 10 + 6 & \rightarrow \quad \text{gcd}(10, 6) \\ 10 & = & 1 \times 6 + 4 & \rightarrow \quad \text{gcd}(6, 4) \\ 6 & = & 1 \times 4 + 2 & \rightarrow \quad \text{gcd}(4, 2) \\ 4 & = & 2 \times 2 + 0 & \quad \text{Stop} \rightarrow \quad \text{gcd}(1970, 1966) = 2 \end{array}$$

# 1. Số học đồng dư

## 1. 3. The Euclidean Algorithm

- Now we show that the Euclidean Algorithm can be used to compute a multiplicative inverse.

### Định nghĩa 1.2

If  $ab \equiv 1 \pmod{p}$ , then  $b$  is called the multiplicative inverse of a module  $p$

# 1. Số học đồng dư

## 1. 3. The Euclidean Algorithm (tiếp tục)

### Định lý 1.2 (Multiplicative Inverse Algorithm)

Given two integers  $0 < b < a$ , consider the Euclidean Algorithm equations which yield  $\gcd(a, b) = r_j$ . Rewrite all of these equations except the last one, by solving for the remainders:

$$r_1 = a - bq_1$$

$$r_2 = b - r_1q_2$$

$$r_3 = r_1 - r_2q_3$$

...

$$r_{j-1} = r_{j-3} - r_{j-2}q_{j-1}$$

$$r_j = r_{j-2} - r_{j-1}q_j$$

Then, in the last of these equations,  $r_j = r_{j-2} - r_{j-1}q_j$ , replace  $r_{j-1}$  with its expression in terms of  $r_{j-3}$  and  $r_{j-2}$  from the equation immediately above it. Continue this process successively, replacing  $r_{j-2}, r_{j-3}, \dots$ , until we obtain the final equation

# 1. Số học đồng dư

## 1. 3. The Euclidean Algorithm

Multiplicative Inverse Algorithm ...

$$r_j = ax + by,$$

where  $x$  and  $y$  are integers. In the special case that  $\gcd(a, b) = 1$ , the integer equation reads

$$1 = ax + by.$$

Therefore we deduce

$$1 \equiv by \pmod{a}$$

so that the residue of  $y$  is the multiplicative inverse of  $b$ , mod  $a$ .

# 1. Số học đồng dư

## 1. 4. Hàm số Euler

### Số nguyên tố

- Số nguyên tố là một số lớn hơn 1, nhưng chỉ chia hết cho 1 và chính nó
- Số 2 là số nguyên tố đầu tiên và là số nguyên tố chẵn duy nhất
- Số lượng số nguyên tố là vô tận
- Hệ mật mã thường sử dụng số nguyên tố lớn cỡ 512 và thậm chí lớn hơn như vậy

#### Ví dụ 1.5

Sau đây là danh sách các số nguyên tố nhỏ hơn 200:

2	3	5	7	11	13	17	19	23	29	31	37	41	43
47	53	59	61	67	71	73	79	83	89	97	101	103	107
109	113	127	131	137	139	149	151	157	163	167	173	179	181
191	193	197	199										

# 1. Số học đồng dư

## 1. 4. Hàm số Euler

### Phân tích ra thừa số nguyên tố

- Một trong những bài toán cơ bản của số học là **phân tích  $a$  ra thừa số nguyên tố**, tức là viết nó dưới dạng tích của lũy thừa các số nguyên tố.
- Bài toán phân tích **khó hơn rất nhiều** so với bài toán nhân các số để nhận được tích.
- Theo lý thuyết số học, mọi số nguyên dương đều có **phân tích duy nhất** thành tích các lũy thừa của các số nguyên tố

$$a = p_1^{n_1} \times p_2^{n_2} \times \cdots \times p_m^{n_m}$$

#### Ví dụ 1.6

$$91 = 7 \times 13; \quad 3600 = 2^4 \times 3^2 \times 5^2$$

⊕ **Nhận xét:** Thông thường để tìm phân tích trên, ta thực hiện phép chia liên tiếp cho các số nguyên tố từ nhỏ đến lớn, rồi gộp thành lũy thừa.

# 1. Số học đồng dư

## 1. 4. Hàm số Euler

### Các số nguyên tố cùng nhau và GCD

- Hai số nguyên dương  $a$  và  $b$  không có ước chung nào ngoài 1, được gọi là **nguyên tố cùng nhau**

#### Ví dụ 1.7

8 và 15 là nguyên tố cùng nhau, vì ước của 8 là 1, 2, 4, 8, còn ước của 15 là 1, 3, 5, 15.

- Ngược lại GCD có thể tìm bằng cách trong các phân tích ra thừa số của chúng, tìm các **thừa số nguyên tố chung** và lấy **bậc lũy thừa nhỏ nhất** trong hai phân tích của hai số đó

#### Ví dụ 1.8

Ta có phân tích:  $300 = 2^1 \times 3^1 \times 5^2$  và  $18 = 2^1 \times 3^2$ .

$$\gcd(18, 300) = 2^1 \times 3^1 \times 5^0 = 6.$$

# 1. Số học đồng dư

## 1. 4. Hàm số Euler

### Hàm Euler

#### Ví dụ 1.9

Cho  $n = 10$ . Thực hiện phép chia các số nguyên khác cho  $n$ :

- Tập đầy đủ các phần dư là  $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
- Tập các phần dư nguyên tố với  $10$  là  $\{1, 3, 7, 9\} \rightarrow \Phi(n) = 4$ .
- Số các phần tử của tập rút gọn trên gọi là giá trị của hàm Euler  $\Phi(n)$ .

#### Định nghĩa 1.3

- Cho  $n$  là một số nguyên dương. Khi thực hiện phép tính đồng dư  $n$  của mọi số nguyên khác ta nhận được tập đầy đủ các phần dư:  $\{0, 1, 2, \dots, n - 1\}$
- Từ tập trên ta tìm tập  $A$  chỉ gồm các số nguyên tố cùng nhau với  $n$
- $\Phi(n) = |A|$

# 1. Số học đồng dư

## 1. 4. Hàm số Euler

### Hàm Euler

⊕ **Nhận xét:** Việc tìm  $\Phi(n)$  bằng việc đếm số các số nguyên tố cùng nhau với  $n$  và nhỏ hơn  $n$  tồn nhiều công sức !!!

- Có thể tính  $\Phi(p)$  dựa trên biểu thức phân tích ra thừa số của  $p$ :

- Nếu  $p$  là số nguyên tố, thì  $\Phi(p) = p - 1$
- Nếu  $p$  và  $q$  là hai số nguyên tố khác nhau thì  $\Phi(p \cdot q) = (p - 1) \cdot (q - 1)$
- Nếu  $p$  là số nguyên tố, thì  $\Phi(p^n) = p^n - p^{n-1}$
- Nếu  $s$  và  $t$  là hai số nguyên tố cùng nhau, thì  $\Phi(s \cdot t) = \Phi(s) \cdot \Phi(t)$

### Ví dụ 1.10

- $\Phi(37) = 37 - 1 = 36$
- $\Phi(21) = (3 - 1) \times (7 - 1) = 2 \times 6 = 12$
- $\Phi(72) = \Phi(8 \cdot 9) = \Phi(8) \cdot \Phi(9) = \Phi(2^3) \cdot \Phi(3^2) = (2^3 - 2^2) \cdot (3^2 - 3^1) = 24$

# 1. Số học đồng dư

## 1. 5. Một số định lí số học cơ bản

### Định lý 1.3 (Tồn tại phần tử nghịch đảo)

Nếu  $\gcd(a, n) = 1$  thì tồn tại duy nhất số  $b$  là phần tử nghịch đảo của  $a$ , tức là  $(ab) \equiv 1 \pmod{n}$ .

### Định lý 1.4 (Fermat nhỏ)

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

trong đó  $p$  là số nguyên tố và  $a$  là số nguyên bất kỳ khác bội của  $p$ , tức là  $\gcd(a, p) = 1$ .

#### ⊕ Nhận xét:

- Một phát biểu khác:  $a^p \equiv a \pmod{p}$
- Công thức trên luôn đúng nếu  $p$  nguyên tố và  $a$  nguyên dương nhỏ hơn  $p$ .

### Ví dụ 1.11

- $2^{7-1} \equiv 1 \pmod{7}$  ( $2^6 \bmod 7 = 64 \bmod 7 = 1$ )

# 1. Số học đồng dư

## 1. 5. Một số định lí số học cơ bản

### Định lý 1.5 (Định lí Euler)

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

với mọi cặp  $(a, n)$  nguyên dương nguyên tố cùng nhau, tức là  $\gcd(a, n) = 1$ .

⊕ **Nhận xét:** Với các số nguyên dương  $a, n, m$  bất kì

$$a^m \pmod{n} = (a \pmod{n})^m \pmod{n} = (a \pmod{n})^{m \pmod{\Phi(n)}} \pmod{n}$$

### Ví dụ 1.12

- Cho  $a = 3, n = 10$ . Ta có  $\Phi(10) = 4 \Rightarrow 3^4 = 81 \equiv 1 \pmod{10}$
- Cho  $a = 2, n = 11, \Phi(11) = 10 \Rightarrow 2^{10} = 1024 \equiv 1 \pmod{11}$
- Cho  $a = 4, n = 15, \Phi(15) = 8 \Rightarrow 4^8 \equiv 1 \pmod{15}$
- $45^{18} \pmod{20} = (45 \pmod{20})^{18 \pmod{\Phi(20)}} \pmod{20} = 5^2 \pmod{20} = 5$ .

# 1. Số học đồng dư

## 1. 5. Một số định lí số học cơ bản

- Với  $M$  lớn, để tăng tốc độ tính toán trong phép toán  $\mod M$  ta cần phân tích  $M$  thành tích của các số nhỏ hơn, từng cặp nguyên tố cùng nhau, tức là

$$M = m_1 \cdot m_2 \cdots m_k, \quad \gcd(m_i, m_j) = 1, \forall i \neq j$$

- Cơ sở của việc làm trên là nhờ định lý Phân dư Trung Hoa.

### Định lý 1.6 (Định lý phân dư Trung Hoa)

#### ① Tính toán theo modulo số lớn: Tìm $A \mod M$

- Tính  $a_i = A \mod m_i$ ;
- $A = \left( \sum_{i=1}^k a_i c_i \right) \mod M$ , trong đó  $\begin{cases} M_i = M/m_i \\ c_i = M_i \times (M_i^{-1} \mod m_i), & 1 \leq i \leq k \end{cases}$

# 1. Số học đồng dư

## 1. 5. Một số định lí số học cơ bản

Tính toán theo modulo số lớn

- Tính  $a_i = A \bmod m_i$ ;
- $A = \left( \sum_{i=1}^k a_i c_i \right) \bmod M$ , trong đó  $\begin{cases} M_i = M/m_i \\ c_i = M_i \times (M_i^{-1} \bmod m_i), \quad 1 \leq i \leq k \end{cases}$

Ví dụ 1.13

Tính  $17^8 \bmod 77$ , ở đây  $A = 17^8$ ,  $M = 77 = 7 \times 11 \Rightarrow m_1 = 7; m_2 = 11$ .

$$\text{Ta có } \begin{cases} M_1 = 11 \\ M_2 = 7 \end{cases} \Rightarrow \begin{cases} M_1^{-1} \bmod 7 = 11^{-1} \bmod 7 = 2 \\ M_2^{-1} \bmod 11 = 7^{-1} \bmod 11 = 8 \end{cases} \Rightarrow \begin{cases} c_1 = 11.2 = 22 \\ c_2 = 7.8 = 56 \end{cases}.$$

$$\text{Lại có } \begin{cases} a_1 = 17^8 \bmod 7 = (17 \bmod 7)^8 \bmod 7 = 3^8 \bmod 7 = \dots = 2 \\ a_2 = 17^8 \bmod 11 = (17 \bmod 11)^8 \bmod 11 = 6^8 \bmod 11 = \dots = 4 \end{cases}.$$

Vậy  $A = 17^8 \bmod 77 = (2.22 + 4.56) \bmod 77 = 268 \bmod 77 = 37$ .

# 1. Số học đồng dư

## 1. 5. Một số định lí số học cơ bản

Định lý phần dư Trung Hoa (tiếp ...)

- ② **Giải hệ phương trình modulo:** Tìm  $x$  thoả mãn  $a_i = x \pmod{m_i}$ ,  
 $\gcd(m_i, m_j) = 1, \forall i \neq j$ .

Theo Định lý phần dư Trung Hoa  $x$  chính là biểu thức cần tìm theo modulo số  $M = m_1 \cdot m_2 \cdots m_k$ .

### Ví dụ 1.14

Cho  $x \equiv 5 \pmod{7}$  và  $x \equiv 6 \pmod{11}$ . Tìm  $x$ .

Áp dụng Định lí phần dư Trung Hoa, ta tính

$$\begin{cases} 7^{-1} \pmod{11} = 8 \\ 11^{-1} \pmod{7} = 2 \end{cases} \Rightarrow x = (5 \cdot 2 \cdot 11 + 6 \cdot 7 \cdot 8) \pmod{(7 \cdot 11)} = 61 \pmod{77}.$$

# 1. Số học đồng dư

## 1. 5. Một số định lí số học cơ bản

### Căn nguyên thuỷ

- Theo Định lý Euler:  $a^{\Phi(n)} \equiv 1 \pmod{n}$  với  $\gcd(a, n) = 1$ .
- Nếu không có số mũ nguyên dương nào nhỏ hơn  $\Phi(n)$  thoả mãn hệ thức trên thì  $a$  gọi là **căn nguyên thuỷ** của  $n$ .

#### Ví dụ 1.15

- Xét xem  $a = 2$  có phải căn nguyên thuỷ của  $5$  không?

Ta có  $2 \pmod{5} = 2$ ;  $2^2 \pmod{5} = 4$ ;  $2^3 \pmod{5} = 3$ ;  $2^4 \pmod{5} = 1$ .

Mà  $m = \Phi(5) = 4 \Rightarrow m = \Phi(5)$  là số nguyên dương nhỏ nhất thoả mãn  $2^m \equiv 1 \pmod{5} \Rightarrow 2$  là căn nguyên thuỷ của  $5$ .

- Xét xem  $a = 3$  có phải căn nguyên thuỷ của  $8$  không?

Ta có  $3 \pmod{8} = 3$ ;  $3^2 \pmod{8} = 1$ ;  $3^3 \pmod{8} = 3$ ;  $3^4 \pmod{8} = 1$ .

Ở đây  $\Phi(8) = 4 \Rightarrow m = 2$  là số nguyên dương nhỏ nhất thoả mãn  $2^m \equiv 1 \pmod{8} \Rightarrow 3$  không là căn nguyên thuỷ của  $8$ .

# 1. Số học đồng dư

## 1. 5. Một số định lí số học cơ bản

### Logarit rời rạc

- Bài toán ngược của bài toán lũy thừa là tìm **logarit rời rạc** của một số modulo  $p$ , tức là tìm số nguyên  $x$  sao cho

$$a^x = b \pmod{p} \text{ hay } x = \log_a b \pmod{p}.$$

- Nếu  $a$  là căn nguyên thủy của  $p$  và  $p$  là số nguyên tố thì luôn luôn tồn tại logarit rời rạc.
- Tổng quát: nếu  $a$  là căn nguyên thủy của  $n$  và  $b$ ,  $n$  nguyên tố cùng nhau thì luôn luôn tồn tại  $x = \log_a b \pmod{n}$ .

# 1. Số học đồng dư

## 1. 5. Một số định lí số học cơ bản

### Logarit rời rạc

#### Ví dụ 1.16

- Tìm  $x = \log_2 3 \pmod{13}$ .

Thử lần lượt ta có  $2^0 \pmod{13} = 1$ ;  $2^1 \pmod{13} = 2$ ;  $2^2 \pmod{13} = 4$ ;  $2^3 \pmod{13} = 8$ ;  $2^4 \pmod{13} = 3$ .

Vậy  $\log_2 3 \pmod{13} = 4$ .

- Tìm  $x = \log_3 4 \pmod{13}$ .

Ta có  $3^0 \pmod{13} = 1$ ;  $3^1 \pmod{13} = 3$ ;  $3^2 \pmod{13} = 9$ ;  $3^3 \pmod{13} = 1 = 3^0 \pmod{13}$ .

không có nghiệm ! (**3 không là căn nguyên thuỷ của 13**).

# Nội dung

## Số học đồng dư

- 1.2 Quan hệ đồng dư
- 1.3 The Euclidean Algorithm
- 1.4 Hàm số Euler
- 1.5 Một số định lí số học cơ bản

## Trao đổi

# TRAO ĐỔI