TOÁN RỜI RẠC
DISCRETE MATHEMATICS

LÊ THỊ PHƯƠNG DUNG

L.T.P.D.

Thời gian thi cuối kỳ

- 14 giờ ngày 27/12/2020

L.T.D.D.

Nội dung

1. Mệnh đề và vị từ
2. Suy luận toán học
3. Phép đếm
4. Quan hệ
5. Đại số Bool
6. Lý thuyết chia và đồng dư

L.T.D.D.

Tài liệu tham khảo

- Kenneth Rosen, "Toán học rời rạc", bản dịch của NXB KH&KT, 2000
- Nguyễn Đức Nghĩa, Nguyễn Tô Thành, "Toán rời rạc", NXB ĐHQG Hà Nội, 2009
- ……..

L.T.D.D.

Chương 7: LÝ THUYẾT ĐỒNG DƯ

- **Quan hệ đồng dư**
- **Phương trình đồng dư bậc nhất một ẩn**
- **Hệ phương trình đồng dư**
- ***Phương trình đồng dư bậc cao một ẩn***

Quan hệ đồng dư

- Cho a và b là hai số nguyên, m là số nguyên dương. Khi đó a và b được gọi là đồng dư theo modulo m, ký hiệu $a \equiv b \ (mod\ m)$ nếu a và b có cùng số dư khi chia cho m. Ta có $a \equiv b \ (mod\ m)$ khi và chỉ khi $a - b \ \vdots\ m$
- VD: $16 \equiv 11 \ (mod\ 5)$; $-7 \equiv 5 \ (mod\ 3)$
- Cho a và b là hai số nguyên, m là số nguyên dương, các mệnh đề sau tương đương nhau
  - $a \equiv b \ (mod\ m)$
  - $a = b + mt \qquad (t \in \mathbb{Z})$
  - $a - b \equiv 0 \ (mod\ m)$
- **Các tính chất của đồng dư**

1. Nếu $a_i \equiv b_i \ (mod\ m), \forall i = 1,2, \dots, n$ thì
   - $a_1 a_2 \dots a_n \equiv b_1 b_2 \dots b_n (mod\ m)$
   - $a_1 + a_2 + \cdots + a_n \equiv b_1 + b_2 + \cdots + b_n \ (mod\ m)$

L.T.D.D.

Quan hệ đồng dư

2. $a \equiv b \ (mod\ m) \Leftrightarrow a \pm c \equiv b \pm c \ (mod\ m)$, với mọi $c \in \mathbb{Z}$
3. $a \equiv b \ (mod\ m) \Leftrightarrow a \equiv b + mk \ (mod\ m)$, với mọi $k \in \mathbb{Z}$
4. Nếu $a \equiv b \ (mod\ m)$ thì $a^n \equiv b^n \ (mod\ m)$, với n là số nguyên dương
5. Nếu $a \equiv b \ (mod\ m)$ thì $ac \equiv bc \ (mod\ m)$ với mọi $c \in \mathbb{Z}$. Trường hợp $(c, m) = 1$ ta có $a \equiv b \ (mod\ m) \Leftrightarrow ac \equiv bc \ (mod\ m)$
6. Nếu c là số nguyên dương thì $a \equiv b \ (mod\ m) \Leftrightarrow ac \equiv bc \ (mod\ mc)$
7. Nếu $d > 0$ là UC của a, b, m thì $a \equiv b \ (mod\ m) \Leftrightarrow \frac{a}{d} \equiv \frac{b}{d} \ (mod\ \frac{m}{d})$
8. Nếu d là UC của a, b và $(\mathrm{d}, \mathrm{m}) = 1$ thì $a \equiv b \ (mod\ m) \Leftrightarrow \frac{a}{d} \equiv \frac{b}{d} \ (mod\ m)$
9. Nếu $a \equiv b \ (mod\ m_i), \forall i = 1,2, \dots, n$ và $m = [m_1, m_2, \dots, m_n]$ thì $a \equiv b \ (mod\ m)$
10. Nếu $a \equiv b \ (mod\ m)$ và $d > 0$ là ước của m thì $a \equiv b \ (mod\ d)$
11. Nếu $a \equiv b \ (mod\ m)$ và d là UC của a, m thì d là ước của b
12. Nếu $a \equiv b \ (mod\ m)$ thì $(a, m) = (b, m)$

L.T.D.D.

Phương trình đồng dư bậc nhất một ẩn

- Cho $a, b, m \in \mathbb{Z}, m > 0$. Một phương trình có dạng $ax \equiv b \ (mod\ m)$, trong đó x là ẩn số nhận giá trị nguyên, được gọi là pt đồng dư bậc nhất một ẩn
- VD: $9x \equiv 6 \ (mod\ 15)$
- Xét phương trình $ax \equiv b \ (mod\ m)$ $(**)$ và đặt $\mathrm{d} = (a, m)$:
  - Nếu $\mathrm{d} \nmid b$ thì $(**)$ vô nghiệm
  - Nếu $d|b$ thì $(**)$ có d nghiệm không đồng dư theo modulo m. Nếu x_0 là một nghiệm của $(**)$ thì d nghiệm của $(**)$ được xác định như sau:

$$\begin{cases} x \equiv x_0 + \dfrac{m}{d}.0 \ (\mathrm{mod}\ m) \\ x \equiv x_0 + \dfrac{m}{d}.1 \ (\mathrm{mod}\ m) \\ \dots \\ x \equiv x_0 + \dfrac{m}{d}.(d-1) \ (\mathrm{mod}\ m). \end{cases}$$

Phương trình đồng dư bậc nhất một ẩn

- Giải phương trình $9x \equiv 6\ (mod\ 15)$
  - Ta có d = (9,15) = 3|6. Do đó pt có 3 nghiệm không đồng dư theo modulo 15. Ta thấy $x_0 = 4$ là một nghiệm của pt. Vậy 3 nghiệm của pt được xác định như sau:

$$\begin{cases} x \equiv 4 + \dfrac{15}{3}.0 \equiv 4 \pmod{15} \\ x \equiv 4 + \dfrac{15}{3}.1 \equiv 9 \pmod{15} \\ x \equiv 4 + \dfrac{15}{3}.(2) \equiv 14 \pmod{15}. \end{cases}$$

Phương trình đồng dư bậc nhất một ẩn

- Cách tìm nghiệm riêng x_0: Xét phương trình $ax \equiv b \ (mod\ m)$, d $= (a, m)|b$. Giả sử d=1, vì nếu d $\neq$ 1 thì ta chia a, b, m cho d ta được

$$\frac{a}{d}x \equiv \frac{b}{d} \ (mod\ \frac{m}{d})$$

  - TH1: Nếu $a\ |b$, vì $(a, m) = 1$ nên chia hai vế của pt cho a , ta được

$$x \equiv \frac{b}{a} \ (mod\ m)$$

  Khi đó, ta có $x_0 = \frac{b}{a}$ là một nghiệm của pt.

  - TH2: Nếu $a \nmid b$, vì (a, m) nên pt $ax \pm my = b$ luôn có nghiệm. Khi đó:

$$x_0 = \frac{b + my}{a}$$

  là một nghiệm của pt

L.T.D.D.

Phương trình đồng dư bậc nhất một ẩn

- VD: Giải pt $4x \equiv 12 \ (mod\ 7)$
  - $d = (4,7) = 1|12$. Do đó pt có một nghiệm theo modulo 7
  - Tìm nghiệm riêng: Vì $4\ |12$ nên ta được một nghiệm của pt là
  $$x_0 = \frac{b}{a} = \frac{12}{4} = 3$$
  - Vậy một nghiệm của pt là $x \equiv 3 \ (mod\ 7)$
- VD: Giải pt $3x \equiv 4 \ (mod\ 11)$
  - $d = (3,7) = 1|4$. Do đó pt có một nghiệm theo modulo 11
  - Tìm nghiệm riêng: Vì $3 \nmid 4$ nên một nghiệm riêng của pt là
  $$x_0 = \frac{b + my}{a} = \frac{4 + 11.1}{3} = 5$$
  - Vậy một nghiệm của pt là $x \equiv 5 \ (mod\ 11)$

L.T.D.D.

Phương trình đồng dư bậc nhất một ẩn

- Chú ý:
  - Pt đồng dư $ax \equiv b \ (mod\ m)$ có nghiệm khi và chỉ khi pt Diophante $ax + my = b$ có nghiệm
  - Nếu pt $ax + my = b$ có nghiệm thì ta dùng thuật toán Euclide để tìm hai số nguyên x_0, y_0 thỏa $ax_0 + my_0 = b$
  - Khi đó, x_0 là một nghiệm của pt đồng dư $ax \equiv b \ (mod\ m)$

L.T.D.D.

Hệ phương trình đồng dư

- Hệ phương trình sau đây được gọi là htp đồng dư bậc nhất một ẩn

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

- Nếu x_0 là một nghiệm của hpt thì mọi số nguyên x đồng dư với x_0 theo modulo $M = [m_1, m_2, \ldots, m_r]$ đều là nghiệm của hpt
- Tìm nghiệm của hpt đồng dư theo ***định lý Trung Quốc về phần dư***. Nếu hpt đồng dư có $m_1, m_2, \ldots, m_r$ là các số nguyên tố cùng nhau từng đôi thì hpt có duy nhất nghiệm theo modulo $\mathrm{M} = m_1 m_2 \ldots m_r$

L.T.D.D.

Hệ phương trình đồng dư

- Cách giải hpt đồng dư theo ***định lý Trung Quốc về phần dư***:
  - Đặt $M = m_1 m_2 \dots m_r$
  - Với mỗi $k \in \{1,2,\dots,r\}$
    - Đặt
$$M_k = \frac{M}{m_k} = m_1 m_2 \dots m_{k-1} m_{k+1} \dots m_r$$
    - Giải pt đồng dư $M_k y_k \equiv 1 \ (mod\ m_k)$
  - Khi đó: $x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r \ (mod\ M)$ là nghiệm của hpt

L.T.D.D.

Hệ phương trình đồng dư

- Đặt $M = m_1 m_2 \dots m_r$
- Với mỗi $k \in \{1,2,\dots,r\}$
  - Đặt $M_k = \frac{M}{m_k} = m_1 m_2 \dots m_{k-1} m_{k+1} \dots m_r$
  - Giải pt đồng dư $M_k y_k \equiv 1 \ (mod\ m_k)$
- $x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_r M_r y_r \ (mod\ M)$ là nghiệm

- VD: Tìm nghiệm của hpt đồng dư

$$\begin{cases} x \equiv 1 \pmod{12} \\ x \equiv 4 \pmod{5} \\ x \equiv 0 \pmod{7} \end{cases}$$

- Vì $m_1 = 12, m_2 = 5, m_3 = 7$ là các số nguyên tố sánh đôi thỏa mãn đk đl TQ
- Đặt $M = m_1 m_2 m_3 = 12.5.7 = 420;\ M_1 = 35; M_2 = 84; M_3 = 60$
- Giải các pt đồng dư
  - $35 y_1 \equiv 1 \ (mod\ 12)$ có nghiệm là $y_1 \equiv -1 \ (mod\ 12)$
  - $84 y_2 \equiv 1 \ (mod\ 5)$ có nghiệm là $y_2 \equiv -1 \ (mod\ 5)$
  - $60 y_3 \equiv 1 \ (mod\ 7)$ có nghiệm là $y_3 \equiv 2 \ (mod\ 7)$
- Vậy nghiệm của hpt là

$$x \equiv 1.35.(-1) + 4.84.(-1) + 0.60.2 \equiv 49 \ (mod\ 420)$$

L.T.D.D.