TOÁN RỜI RẠC
DISCRETE MATHEMATICS

LÊ THỊ PHƯƠNG DUNG

L.T.P.D.

Thời gian thi cuối kỳ

- 14 giờ ngày 27/12/2020

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.

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 6: LÝ THUYẾT CHIA

- Phép chia hết và chia có dư
- Ước chung lớn nhất và bội chung nhỏ nhất
- Số nguyên tố và hợp số
- Định lý căn bản của số học
- Phương trình nguyên

L.T.D.D.

Phép chia hết và chia có dư

- Cho hai số nguyên a và b $\neq 0$. Ta nói a chia hết cho b (ký hiệu $a \vdots b$) hoặc a là bội của b hoặc b chia hết a hoặc b là ước của a (ký hiệu $b|a$), nếu tồn tại số nguyên c sao cho $a = bc$
- Tính chất của phép chia hết:
  1. $b|a \Leftrightarrow \pm b| \pm a$
  2. Với $a \neq 0, a|a \wedge a|0$
  3. Với $a \in \mathbb{Z}, \pm 1|a$
  4. $a|b \wedge b|a \Leftrightarrow a = \pm b$
  5. $a|b \wedge b|c \Rightarrow a|c$
  6. $c|a \wedge c|b \Rightarrow c|(ax + by),\ \forall x, y \in \mathbb{Z}$
  7. $a|x \wedge b|y \Rightarrow ab|xy$
- Cho hai số nguyên a và b $\neq 0$. Khi đó, với cặp số nguyên q, r thỏa mãn $\mathrm{a} = \mathrm{bq} + \mathrm{r}$ và $0 \leq r < |b|$, ta nói a chia cho b dư r

L.T.D.D.

Ước chung lớn nhất và bội chung nhỏ nhất

- Cho $a_1, a_2, \dots, a_n$ là các số nguyên không đồng thời bằng 0
  - $d \in \mathbb{Z}$ là **UC** của $a_1, a_2, \dots, a_n$ nếu d là ước của $a_i, \forall i = \overline{1, n}$
  - $d \in \mathbb{Z}$ là **UCLN** của $a_1, a_2, \dots, a_n$, ký hiệu $d = (a_1, a_2, \dots, a_n)$, nếu d là UC của $a_1, a_2, \dots, a_n$ và d là bội của mọi UC của $a_1, a_2, \dots, a_n$
  - *VD:* $\pm 1, \pm 2, \pm 3, \pm 6$ *là các UC của* $18, -24, 30$ *và* $(18, -24, 30) = 6$
- **Tính chất**: *Cho* $a, b, c \in \mathbb{Z}$:
  - Giao hoán: $(a, b) = (b, a)$
  - Kết hợp: $(a, b, c) = \big((a, b), c\big) = \big(a, (b, c)\big)$
- Các số $a_1, a_2, \dots, a_n$ là **nguyên tố cùng nhau** nếu chúng có UCLN bằng 1
- VD: Các số $12, -7, 25$ là nguyên tố cùng nhau vì $(12, -7, 25) = 1$
- Các số $a_1, a_2, \dots, a_n$ là **nguyên tố sánh đôi** nếu $(a_i, a_j) = 1, \forall i \neq j$
- VD: Các số $12, -7, 25$ là nguyên tố sánh đôi vì
$$(12, -7) = (12, 25) = (-7, 25) = 1$$

L.T.D.D.

Ước chung lớn nhất và bội chung nhỏ nhất

- Tính chất của UCLN:
  - Nếu $(a_1, a_2, \dots, a_n) = d$ thì $\exists \alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{Z}$:
  $$d = \alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_n a_n$$
  - Nếu $m \in \mathbb{Z}_+$ thì $(ma_1, ma_2, \dots, ma_n) = m(a_1, a_2, \dots, a_n)$
  - Nếu $\mathrm{d} \in \mathbb{Z}_+$ là UC của $a_1, a_2, \dots, a_n$ thì $\left(\frac{a_1}{d}, \frac{a_2}{d}, \dots, \frac{a_n}{d}\right) = \frac{(a_1, a_2, \dots, a_n)}{d}$
  - Giả sử $\mathrm{d} \in \mathbb{Z}_+$ là UC của $\mathrm{a}_1, a_2, \dots, a_n$. Khi đó, $\mathrm{d} = (a_1, a_2, \dots, a_n)$ khi và chỉ khi $\left(\frac{a_1}{d}, \frac{a_2}{d}, \dots, \frac{a_n}{d}\right) = 1$
  - Nếu $\mathrm{b} \in \mathbb{Z}_+$ *là ước của* a thì $(\mathrm{a}, \mathrm{b}) = \mathrm{b}$, đặc biệt $(0, \mathrm{b}) = \mathrm{b}$
  - Nếu $\mathrm{c}|\mathrm{ab}$ và $(a, c) = 1$ thì $c|b$
  - Nếu $\mathrm{b}|\mathrm{a}$ và $\mathrm{c}|\mathrm{a}$ và $(\mathrm{b}, \mathrm{c}) = 1$ thì $\mathrm{bc}|\mathrm{a}$
  - Nếu $(\mathrm{a}, \mathrm{b}) = 1$ thì $(\mathrm{ac}, \mathrm{b}) = (\mathrm{c}, \mathrm{b})$
  - Nếu $(\mathrm{a}, \mathrm{b}) = (a, c) = 1$ thì $(\mathrm{a}, \mathrm{b}c) = 1$

L.T.D.D.

Ước chung lớn nhất và bội chung nhỏ nhất

- Giả sử a, b là hai số nguyên dương và $\mathrm{q}, \mathrm{r} \in \mathbb{Z}$ thỏa $\mathrm{a} = \mathrm{bq} + \mathrm{r}, 0 \leq r < b$. Khi đó, ta có $(\mathrm{a}, \mathrm{b}) = (\mathrm{b}, \mathrm{r})$
- Thuật toán Euclide tìm UCLN của hai số nguyên a, b. Vì $(\mathrm{a}, \mathrm{b}) = (|\mathrm{a}|, |\mathrm{b}|)$ nên có thể giả sử $\mathrm{a}, \mathrm{b} \in \mathbb{Z}_+$

$\mathrm{a} = \mathrm{bq} + \mathrm{r_0}$	$0 \leq r_0 < b$
$\mathrm{b} = \mathrm{r_0 q_0} + \mathrm{r_1}$	$0 \leq r_1 < r_0$
$\mathrm{r_0} = \mathrm{r_1 q_1} + \mathrm{r_2}$	$0 \leq r_2 < r_1$
$\vdots$	
$\mathrm{r_{n-2}} = \mathrm{r_{n-1} q_{n-1}} + \mathrm{r_n}$	$0 \leq r_n < r_{n-1}$
$\mathrm{r_{n-1}} = \mathrm{r_n q_n}$	

- Ta được: $(\mathrm{a}, \mathrm{b}) = (b, r_0) = (r_0, r_1) = \cdots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = r_n$
- Để tính UCLN của nhiều số nguyên $a_1, a_2, \dots, a_n$ ta tính $(a_1, a_2) = d_2$, $(d_2, a_3) = d_3, \cdots, (d_{n-1}, a_n) = d_n$. Khi đó, ta có $(a_1, a_2, \dots, a_n) = d_n$

L.T.D.D.

Ước chung lớn nhất và bội chung nhỏ nhất

VD: Tìm (51,45)

➨ Ta có $(51,45) = (45,6) = (6,3) = 3$

VD: Tìm (786,285)

➨ Ta có $(786,285) = (285,216) = (216,69) = (69,9) = (9,6) = (6,3) = 3$

VD: Bằng thuật toán Euclide hãy tìm UCLN d của $a = 786, b = 285$. Từ đó, tìm hai số $u, v \in \mathbb{Z}$ sao cho $au + bv = d$

$$\begin{aligned}
786 &= 2.285 + 216 \\
285 &= 1.216 + 69 \\
216 &= 3.69 + 9 \\
69 &= 7.9 + 6 \\
9 &= 1.6 + 3 \\
6 &= 2.3
\end{aligned}$$

$$\begin{aligned}
3 &= 9 - 6 \\
&= 9 - (69 - 7.9) = 8.9 - 69 \\
&= 8(216 - 3.69) - 69 = 8.216 - 25.69 \\
&= 8.216 - 25(285 - 216) = -25.285 + 33.216 \\
&= -25.285 + 33(786 - 2.285) = 33.786 - 91.285
\end{aligned}$$

Vậy $(786, 285) = 3 = 33.786 - 91.285$.

L.T.D.D.

Ước chung lớn nhất và bội chung nhỏ nhất

- Cho $a_1, a_2, \dots, a_n$ là các số nguyên khác 0.
  - $M \in \mathbb{Z}$ là **BC** của $a_1, a_2, \dots, a_n$ nếu M là bội của $a_i, \forall i = \overline{1, n}$
  - m $\in \mathbb{Z}_+$ là **BCNN** của $a_1, a_2, \dots, a_n$, ký hiệu $m = [a_1, a_2, \dots, a_n]$, nếu m là BC của $a_1, a_2, \dots, a_n$ và m là ước của mọi BC của $a_1, a_2, \dots, a_n$
  - *VD:* 60 *là BC của* $2, -3, 5$ *và* $[2, -3, 5] = 30$
- **Tính chất**: *Cho* $a, b, c \in \mathbb{Z} \backslash \{0\}$:
  - Giao hoán: $[a, b] = [b, a]$
  - Kết hợp: $[a, b, c] = \big[[a, b], c\big] = \big[a, [b, c]\big]$
- Để tính bội chung nhỏ nhất của nhiều số nguyên $a_1, a_2, \dots, a_n$ khác không, ta lần lượt tính $[a_1, a_2] = m_2, [m_2, a_3] = m_3, \cdots, [m_{n-1}, a_n] = m_n$. Khi đó ta có $[a_1, a_2, \dots, a_n] = m_n$

L.T.D.D.

Ước chung lớn nhất và bội chung nhỏ nhất

- Tính chất của BCNN:
  - Nếu m $\in \mathbb{Z}_+$ là BC của $a_1, a_2, \dots, a_n$ thì m $= [a_1, a_2, \dots, a_n]$ khi và chỉ khi $\left(\frac{m}{a_1}, \frac{m}{a_2}, \dots, \frac{m}{a_n}\right) = 1$
  - Với $k \in \mathbb{Z}_+$, ta có $[ka_1, ka_2, \dots, ka_n] = k[a_1, a_2, \dots, a_n]$
  - Nếu d $= (a_1, a_2, \dots, a_n)$ thì $\left[\frac{a_1}{d}, \frac{a_2}{d}, \dots, \frac{a_n}{d}\right] = \frac{[a_1, a_2, \dots, a_n]}{d}$
  - Nếu $a_1, a_2, \dots, a_n$ là số nguyên tố sánh đôi thì $[a_1, a_2, \dots, a_n] = a_1. a_2 \dots a_n$
- Giả sử a, b $\in \mathbb{Z}_+$, khi đó:

$$[a, \mathrm{b}] = \frac{\mathrm{ab}}{(a, b)}$$

VD: Tính $[21, 6]$

Ta có $(21, 6) = (6,3) = 3$. Suy ra $[21, 6] = \frac{21.6}{(21,6)} = \frac{21.6}{3} = 42$

L.T.D.D.

Số nguyên tố và hợp số

- Số nguyên $p > 1$ được gọi là số nguyên tố nếu p chỉ có hai ước dương là 1 và p
- Số nguyên $a > 1$ được gọi là hợp số nếu a không phải số nguyên tố
- VD: Số nguyên tố: 2,3,5,7,11,13; Hợp số: 4,6,8,9,10,12
- Giả sử số nguyên $a > 1$, khi đó ước dương bé nhất khác 1 của a là một số nguyên tố
- Nếu a là hợp số thì a có ít nhất một ước nguyên tố p thỏa $p \leq \sqrt{a}$
- **Sàng Erathosthene:**

1. B1: Liệt kê các số từ 2 đến n trong một bảng
2. B2: Tìm các số nguyên tố trong khoảng từ 2 đến $\sqrt{n}$
3. B3: Xóa tất cả các bội thực sự của các số nguyên tố này
4. B4: Các số còn lại trong bảng là các số nguyên tố cần tìm.

L.T.D.D.

Số nguyên tố và hợp số

- VD: Tìm các số nguyên tố không vượt quá 100

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

- Các số nguyên tố trong khoảng từ 2 đến $\sqrt{100}$ là: 2, 3, 5, 7
- Ta xóa các bội thực sự của ít nhất một trong các số nguyên tố trên

L.T.D.D.

Số nguyên tố và hợp số

- VD: Tìm các số nguyên tố không vượt quá 100
- Các số nguyên tố trong khoảng từ 2 đến $\sqrt{100}$ là: 2, 3, 5, 7
- Ta xóa các bội thực sự của ít nhất một trong các số nguyên tố trên
- Các số còn lại là các số nguyên tố cần tìm

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53				57			
61						67			
71		73						79	
		83						89	
						97			

Số nguyên tố và hợp số

- **Định lý căn bản của số học:** Giả sử a là một số nguyên lớn hơn 1. Khi đó a luôn phân tích được một cách duy nhất thành tích các thừa số nguyên tố
- Giả sử a là số nguyên lớn hơn 1. Khi đó, dạng phân tích a dưới dạng $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, trong đó $p_1, p_2, \cdots, p_k$
- VD: $28 = 2.2.7 = 2^2.7$; $1260 = 2.2.3.3.5.7 = 2^2.3^2.5.7$

Mệnh đề. *Giả sử dạng phân tích tiêu chuẩn của số nguyên $a > 1$ là $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Khi đó, số nguyên $d > 0$ là ước của a khi và chỉ khi dạng phân tích tiêu chuẩn của d là $d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$, trong đó $0 \leq \beta_i \leq \alpha_i$ với mọi $i = 1, 2, \ldots, k$.*

Dựa vào mệnh đề này ta có thể tìm ước chung lớn nhất và bội chung nhỏ nhất của hai số nguyên dương a và b. Ta viết dạng phân tích tiêu chuẩn của a và b như sau $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ và $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}$. Ta có

$$(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_n^{\gamma_n}, \text{ trong đó } \gamma_i = \min\{\alpha_i, \beta_i\}, i = 1, 2, \ldots, n$$

$$[a, b] = p_1^{\delta_1} p_2^{\delta_2} \ldots p_n^{\delta_n}, \text{ trong đó } \delta_i = \max\{\alpha_i, \beta_i\}\ i = 1, 2, \ldots, n.$$

Số nguyên tố và hợp số

Ví dụ. Với $a = 1960$ và $b = 2352$, ta có

$$a = 1960 = 2^3.5.7^2 = 2^3.3^0.5^1.7^2$$

$$b = 2352 = 2^4.3.7^2 = 2^4.3^1.5^0.7^2.$$

Vậy ta có

$$(a, b) = 2^3.3^0.5^0.7^2 = 392$$

$$[a, b] = 2^4.3^1.5^1.7^2 = 11760.$$

L.T.D.D.

Phương trình nghiệm nguyên (Diophante)

- Phương trình Diophante tuyến tính là phương trình dạng ax+by=c, trong đó a, b, c là các số nguyên, các biến x, y nhận giá trị nguyên
- Cách giải phương trình Diophante tuyến tính ax+by=c
  - Gọi d=(a,b).
  - Nếu d∤c thì pt không có nghiệm nguyên
  - Nếu d|c thì pt có vô số nghiệm nguyên. Nếu x_0, y_0 là một nghiệm của pt thì mọi nghiệm nguyên của pt có dạng

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t, \quad t \in \mathbb{Z}$$

- VD: Giải pt Diophante tuyến tính 14x+8y=200
  - $d = (14,8) = 2|200$. Vậy pt có vô số nghiệm
  - Ta có $14(-100) + 8(200) = 200$ nên $x_0 = -100,\ y_0 = 200$ là một nghiệm của pt
  - Vậy nghiệm tổng quát của pt đã cho là $x = -100 + 4t, y = 200 - 7t, t \in \mathbb{Z}$

L.T.D.D.