CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

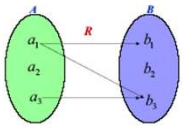
§1 Quan hệ.

1.1 Định nghĩa.

Một *quan hệ hai ngôi* từ tập A đến tập B là tập con của tích Đề các $R \subseteq A \times B$.

Chúng ta sẽ viết $a\ R\ b$ thay cho $(a, b) \in R$

Quan hệ từ A đến chính nó được gọi là quan hệ trên A

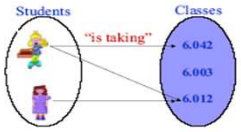


$R = \{ (a_1, b_1), (a_1, b_3), (a_3, b_3) \}$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

1.2 Thí dụ. A = tập sinh viên; B = các lớp học.

$R = \{(a, b) \mid$ sinh viên a học lớp $b\}$



CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

1.3 Định nghĩa. Quan hệ R trên A được gọi là *phản xạ* nếu:

$(a, a) \in R$ *với mọi* $a \in A$

1.4 Thí dụ. Trên tập $A = \{1, 2, 3, 4\}$, quan hệ:

$R_1 = \{(1,1), (1,2), (2,1), (2, 2), (3, 4), (4, 1), (4, 4)\}$ không phản xạ vì $(3, 3) \notin R_1$

$R_2 = \{(1,1), (1,2), (1,4), (2, 2), (3, 3), (4, 1), (4, 4)\}$ phản xạ vì $(1,1), (2, 2), (3, 3), (4, 4) \in R_2$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

- Quan hệ $\leq$ trên Z phản xạ vì $a \leq a$ với mọi $a \in Z$.

- Quan hệ" $\mid$ " ("ước số") trên Z^+ là phản xạ vì mọi số nguyên a là ước của chính nó .

1.5 Định nghĩa.

- Quan hệ R trên A được gọi là *đối xứng* nếu:

$$\forall a \in A, \forall b \in A, (a\ R\ b) \rightarrow (b\ R\ a)$$

- Quan hệ R được gọi là *phản xứng* nếu

$$\forall a \in A, \forall b \in A, (a\ R\ b) \wedge (b\ R\ a) \rightarrow (a = b)$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

1.6 Thí dụ.

- Quan hệ $R_1 = \{(1,1), (1,2), (2,1)\}$ trên tập $A = \{1, 2, 3, 4\}$ là đối xứng.
- Quan hệ $\leq$ trên **Z** không đối xứng. Tuy nhiên nó phản xứng vì

$$(a \leq b) \wedge (b \leq a) \rightarrow (a = b)$$

- Quan hệ" $\mid$ " ("ước số") trên Z^+ không đối xứng

Tuy nhiên nó có tính phản xứng vì

$$(a \mid b) \wedge (b \mid a) \rightarrow (a = b)$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

1.7 Định nghĩa. Quan hệ R trên A có tính *bắc cầu (truyền)* nếu

$$\forall a \in A, \forall b \in A, \forall c \in A, (a\ R\ b) \wedge (b\ R\ c) \rightarrow (a\ R\ c)$$

1.8 Thí dụ.

- Quan hệ $R = \{(1,1), (1,2), (2,1), (2, 2), (1, 3), (2, 3)\}$ trên tập $A = \{1, 2, 3, 4\}$ có tính bắc cầu.

- Quan hệ $\leq$ và "$\mid$"trên Z có tính bắc cầu

$$(a \leq b) \wedge (b \leq c) \rightarrow (a \leq c)$$

$$(a \mid b) \wedge (b \mid c) \rightarrow (a \mid c)$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

§2 Quan hệ tương đương.

2.1 Thí dụ.

Cho S = {sinh viên của lớp}, gọi

R = {(a,b): a có cùng họ với b}

Hỏi

R phản xạ? Yes

R đối xứng? Yes

R bắc cầu? Yes

Mọi sinh viên có cùng họ thuộc cùng một nhóm.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

2.2 Định nghĩa. Quan hệ R trên tập A được gọi là *tương đương* nếu nó có tính chất phản xạ, đối xứng và bắc cầu.

2.3 Thí dụ.

a) Cho R là quan hệ trên $\mathbb{R}$ sao cho aRb nếu $a-b$ nguyên. Khi đó R là quan hệ tương đương, Thật vậy

$-\forall a \in \mathbb{R}, a-a=0 \in \mathbb{Z}.$

$-\forall a,b \in \mathbb{R}, a-b \in \mathbb{Z} \to -(a-b)=b-a \in \mathbb{Z}.$

$-\forall a,b,c \in \mathbb{R},$

$$\begin{cases} a-b \in \mathbb{Z} \\ b-c \in \mathbb{Z} \end{cases} \to (a-b)+(b-c)=a-c \in \mathbb{Z}.$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

b) Cho n là số nguyên dương và R quan hệ trên Z được định nghĩa

$$\forall a,b \in \mathbb{Z}, aRb \leftrightarrow n \mid (a-b).$$

khi đó R là quan hệ tương đương.

- Phản xạ: $\forall a \in \mathbb{Z}, n \mid 0 \to n \mid (a-a) \to aRa.$
- Đối xứng: $\forall a,b \in \mathbb{Z}, aRb \to n \mid (a-b) \to n \mid (b-a) \to bRa$
- Bắc cầu:

$$\forall a,b,c \in \mathbb{Z}, \begin{cases} aRb \\ bRc \end{cases} \to \begin{cases} n \mid (a-b) \\ n \mid (b-c) \end{cases} \to n \mid ((a-b)+(b-c)) \to n \mid (a-c)$$

$\Rightarrow aRc.$

- Quan hệ tương đương này được gọi là *đồng dư modulo n* và chúng ta viết $a \equiv b \pmod{n}$ thay vì aRb

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

2.4 Định nghĩa. Cho R là quan hệ tương đương trên A và $a \in A$. *Lớp tương đương chứa* a được ký hiệu bởi $[a]$ hoặc $\overline{a}$ là tập hợp

$$[a]=\overline{a}=\{b \in \mathbb{Z} \mid aRb\}=\{b \in \mathbb{Z} \mid bRa\}.$$

Phần tử a được gọi là phần tử đại diện của $[a]$.

2.5 Tính chất lớp tương đương. Cho R là một quan hệ tương đương trên A, khi đó

a) $\forall a \in A, a \in [a].$

b) $A=\bigcup_{a \in A}[a].$

c) $aRb \leftrightarrow [a]=[b].$

d) $\forall a,b \in A, [a] \neq [b] \to [a] \cap [b] = \varnothing.$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

Chứng minh.

a) Suy ra từ định nghĩa lớp tương đương và tính phản xạ.

b) Mỗi $[a]$ là tập con của A, do đó

$$\bigcup_{a \in A}[a] \subset A.$$

Mặt khác theo (a), $A=\bigcup_{a \in A}\{a\} \subset \bigcup_{a \in A}[a].$

c) ($\to$) Lấy $c \in [a]$, ta có cRa và aRb, do tính bắc cầu cRb, do đó $c \in [b]$, kéo theo $[a] \subset [b]$. Chứng minh tương tự ta có $[b] \subset [a]$.

($\leftarrow$) Giả sử $[a]=[b]$, theo (a), $a \in [b]$ dẫn tới aRb.

d) Giả sử $[a] \cap [b] \neq \varnothing$, lấy $c \in [a] \cap [b]$, khi đó aRc và cRb, do tính bắc cầu aRb, theo (c) $[a]=[b]$.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

2.6 Lớp tương đương trên quan hệ $\equiv \pmod{n}$.

Lấy $a \in \mathbb{Z}$,

$$[a]=\overline{a}=\{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}=\{b \in \mathbb{Z} \mid n \mid (b-a)\}=$$

$$\{t \in \mathbb{Z} \mid tn=b-a\}=\{t \in \mathbb{Z} \mid b=tn+a\}=\{tn+a \mid t \in \mathbb{Z}\}$$

2.7 Thí dụ. Tìm các lớp tương đương modulo 8 chứa 0 và 3?

Giải. Lớp tương đương modulo 8 chứa 0 gồm tất cả các số nguyên a chia hết cho 8. Do đó

$$[0]_8=\{\ldots,-16,-8,0,8,16,\ldots\}$$

Tương tự

$$[3]_8=\{8t+3 \mid t \in \mathbb{Z}\}=\{\ldots,-13,-5,3,11,19,\ldots\}$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

2.8 Nhận xét.

a) Từ kết quả (b) và (d) của Tính chất 2.5, quan hệ tương đương trên A chia tập hợp A thành các tập con rời nhau mà mỗi tập con đó là một lớp tương đương.

b) Mỗi phần tử trong một lớp tương đương đều có thể làm phần tử đại diện cho lớp tương đương đó, điều này có thể có nhiều cách viết khác nhau cho một lớp tương đương. Chẳng hạn, trong quan hệ $\equiv (\text{mod } 8)$, $[4] = [36]$ vì $4 \equiv 36 (\text{mod } 8)$ (do $8|(36 - 4)$).

c) Trong quan hệ đồng dư modulo n, từ kết quả (c) của Tính chất 2.5, ta có $[a] = [a + tn]$ với mọi $t \in \mathbb{Z}$ (do $n|(a + tn - a)$). Suy ra có đúng n lớp tương đương trong quan hệ này, cụ thể là

$$[0], [1], \ldots, [n - 1].$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

§3 Vành $\mathbb{Z}_n$.

3.1 Định nghĩa. Tập hợp tất cả các lớp tương đương trong quan hệ đồng dư mod n được ký hiệu là $\mathbb{Z}_n$, vậy

$$\mathbb{Z}_n = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}.$$

3.2 Chú ý: Trong $\mathbb{Z}_n$ để đưa lớp tương đương $[a]$ có phần tử đại diện nằm trong khoảng từ 0 tới $n - 1$, ta thực hiện như sau:

$$\overline{a} = \overline{a - n\left[\frac{a}{n}\right]}.$$

Trong đó $\left[\frac{a}{n}\right]$ là phần nguyên lớn nhất không vượt quá $\frac{a}{n}$.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

3.3 Thí dụ. Trong $\mathbb{Z}_{48}$,

$$\overline{592} = \overline{592 - 48\left[\frac{592}{48}\right]} = \overline{592 - 48\times 12} = \overline{16}$$

$$\overline{-1293} = \overline{-1293 - 48\left[\frac{-1293}{48}\right]} = \overline{-1293 - 48(-27)} = \overline{3}.$$

Thực hành: Trong $\mathbb{Z}_{72}$,

$$\overline{5961} = ?;\ \overline{-3497} = ?$$

Đáp án: $\overline{57}; \overline{31}$.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

3.4 Phép toán trên $\mathbb{Z}_n$.

Trên $\mathbb{Z}_n$, ta định nghĩa các phép toán sau:

$$\forall \overline{a}, \overline{b} \in \mathbb{Z}_n, \overline{a} + \overline{b} = \overline{a+b}; \overline{a}.\overline{b} = \overline{ab}.$$

$$\forall k \in \mathbb{Z}, k.\overline{a} = \overline{ka}.$$

Ta chứng minh phép toán được định nghĩa tốt, nghĩa là không phụ thuộc vào cách lựa chọn phần tử đại diện. Giả sử $\overline{a} = \overline{b}, \overline{c} = \overline{d}$ khi đó

$$a = b + tn; c = d + kn (t, k \in \mathbb{Z}).$$

$$a + c = b + d + (t + k)n \to \overline{a+c} = \overline{b+d}.$$

$$ac = bd + (bk + td + tkn)n \to \overline{ac} = \overline{bd}.$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

3.5 Chú ý: Các phép toán thực hiện trên $\mathbb{Z}_n$ đều tương tự như trên $\mathbb{Z}$. Khác biệt là trên $\mathbb{Z}_n$ không có phép chia hay phân số.

3.6 Định nghĩa. $\mathbb{Z}_n$ với các phép toán được định nghĩa trong Định nghĩa 3.4 được gọi là vành $\mathbb{Z}_n$.

3.7 Tính khả nghịch trong vành $\mathbb{Z}_n$.

3.7.1 Định nghĩa. Phần tử $\overline{a} \in \mathbb{Z}_n$ được gọi là khả nghịch nếu tồn tại phần tử $\overline{b} \in \mathbb{Z}_n$, sao cho $\overline{a}.\overline{b} = \overline{1}$. Trong trường hợp này $\overline{b}$ được gọi là phần tử nghịch đảo của $\overline{a}$ và ta kí hiệu

$$\overline{b} = (\overline{a})^{-1}$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

3.7.2 Tính chất.

a) Nếu $\overline{a}$ khả nghịch thì phần tử nghịch đảo của nó là duy nhất.

b) $(\overline{a})^{-1}(\overline{b})^{-1} = (\overline{a}.\overline{b})^{-1}$.

Chứng minh. a) Nếu $(\overline{a})^{-1} = \overline{b} = \overline{c}; \overline{b} = \overline{b}.\overline{1} = \overline{b}.\overline{a}.\overline{c} = \overline{1}.\overline{c} = \overline{c}$.

b) $(\overline{a})^{-1}(\overline{b})^{-1}\overline{a}.\overline{b} = \overline{1} \to (\overline{a}.\overline{b})^{-1} = (\overline{a})^{-1}(\overline{b})^{-1}$.

3.7.3 Thí dụ. Trong $\mathbb{Z}_{15}$,

$$(\overline{4})^{-1} = \overline{4}\ \ (\overline{4}.\overline{4} = \overline{16} = \overline{1}).$$

$$(\overline{7})^{-1} = \overline{13}\ (\overline{7}.\overline{13} = \overline{91} = \overline{1}).$$

Phần tử $\overline{5}$ không khả nghịch trong $\mathbb{Z}_{15}$, vì không có phần tử nào trong $\mathbb{Z}_{15}$, nhân với $\overline{5}$ bằng $\overline{1}$.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

3.7.4 Định lý. $\bar{a}$ khả nghịch trong $\mathbb{Z}_n$ khi và chỉ khi $(a, n) = 1$.

Chứng minh. ($\rightarrow$) Giả sử $\bar{a}$ khả nghịch trong $\mathbb{Z}_n$ khi đó tồn tại $\bar{b}$ sao cho $\overline{ab} = \bar{1} \Rightarrow ba = 1 + tn \Rightarrow 1 = ba + (-t)n$. Theo Mệnh đề 5.7 chương 1 ta có $(a, n) = 1$.

($\leftarrow$) $(a,n) = 1 \rightarrow \exists p, q \in \mathbb{Z}, pa + qn = 1$

$\rightarrow \bar{1} = \overline{pa + qn} = \overline{pa} + \overline{qn} = \bar{p}.\bar{a}$ ($do \quad \overline{qn} = 0$).

3.7.5 Cách tìm phần tử nghịch đảo.

- Trường hợp $(a, n) \neq 1$, kết luận $\bar{a}$ không khả nghịch.
- Trường hợp $(a, n) = 1$, tìm p, q sao cho $pa + qn = 1$. Khi đó $\bar{p}$ nghịch đảo của $\bar{a}$.

(cách tìm p, q xem lại Thí dụ 4.10 chương 1)

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

3.7.6 Thí dụ. Tìm phần tử nghịch đảo của $\overline{17}$ trong $\mathbb{Z}132$.

$132 = 7\times17 + 13; 17 = 1\times13 + 4; 13 = 3\times4 + 1;$

$1 = 13 - 3\times4 = 13 - 3(17 - 1\times13) = -3\times17 + 4\times13 =$

$-3\times17 + 4(132 - 7\times17) = 4\times132 - 31\times17.$

$\rightarrow \left(\overline{17}\right)^{-1} = \overline{-31} = \overline{101}.$

Thực hành: Trong $\mathbb{Z}_{97}$, tìm nghịch đảo của $\overline{23}$.

Đáp án: $\overline{38}$.

3.7.7 Hệ quả. Nếu p là số nguyên tố thì mọi phần tử khác $\bar{0}$ trong $\mathbb{Z}_p$ đều khả nghịch.

Chứng minh. $a \in \{1, 2, ..., p-1\}, (a, p) = 1$.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

3.7.8 Giải phương trình $\bar{a}\,x = \bar{b}$ trong $\mathbb{Z}_n$.

Đặt $d = (a, n)$. Nếu b không chia hết cho d thì phương trình vô nghiệm. Trường hợp $d|b$, đặt

$$a_1 = \frac{a}{d}; b_1 = \frac{b}{d}; n_1 = \frac{n}{d};$$

Tính $(a_1)^{-1}$ trong $\mathbb{Z}_{n_1}$

Phương trình có d nghiệm như sau:

$$x = (\bar{a}_1)^{-1}\bar{b}_1 + t.\bar{n}_1, \quad t = \overline{0,1,...,d-1}.$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

3.7.9 Thí dụ. Giải các phương trình sau.

a) $\bar{2}(\bar{6}x + \overline{22}) = \overline{10}$ $(\mathbb{Z}_{92})$.

b) $\bar{3}\left(\bar{5}x - \overline{12}\right) = \overline{29}$ $(\mathbb{Z}_{85})$.

Giải. *a)* $\bar{2}(\bar{6}x + \overline{22}) = \overline{10} \rightarrow \overline{12}x = \overline{10} - \overline{44} = -\overline{34} = \overline{58}.$

$(12, 92) = 4; 4 \nmid 58.$

Phương trình vô nghiệm.

b) $\bar{3}\left(\bar{5}x - \overline{12}\right) = \overline{29}$ $(\mathbb{Z}_{85}) \rightarrow \overline{15}x = \overline{29} + \overline{36} = \overline{65}.$

$(15, 85) = 5; 5 \mid 65; \bar{a}_1 = \bar{3}; \bar{b}_1 = \overline{13}; n_1 = \overline{17}$

$(\bar{3})^{-1} = \bar{6}$ $(\mathbb{Z}_{17})$.

$x = \bar{6}.\overline{13} + t.\overline{17}$ $(t = 0,1,2,3,4) = \overline{78}; \overline{10}; \overline{27}; \overline{44}; \overline{61}.$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

Thực hành. Giải phương trình: $\bar{4}\left(\bar{7}x + \overline{52}\right) = \overline{16}$ $(\mathbb{Z}_{124})$.

Đáp án.

$\overline{28}x = \overline{56}; (28, 124) = 4, \left(\bar{7}\right)^{-1} = \bar{9}$ $(\mathbb{Z}_{31})$;

$x = \bar{9}.\overline{14} + t.\overline{31}$ $(t = 0,1,2,3) = \overline{2}, \overline{33}, \overline{64}, \overline{95}.$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

§4. Một số định lý về số học.

4.1 Định lý dư số trung hoa. Cho $n_1, n_2, ..., n_t$ là các số nguyên dương đôi một nguyên tố cùng nhau. Khi đó hệ đồng dư

$x \equiv a_1 \pmod{n_1}$

$x \equiv a_2 \pmod{n_2}$

.....

.....

$x \equiv a_t \pmod{n_t}$

(nghĩa là $\bar{x} = \bar{a}_i \left(\mathbb{Z}_{n_i}\right), \forall i = \overline{1,...,t}$)

Có nghiệm duy nhất đồng dư $n = n_1 n_2 ... n_t$.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

Chứng minh.

Tồn tại. Đặt $\overline{u_i} = n/n_i\ (\forall i = 1,\ldots,t)$. Theo Mệnh đề 5.5 chương 1 $(u_i, ni) = 1$. Suy ra $\overline{u_i}$ khả nghịch trong $\mathbb{Z}_{ni}$. Gọi $\overline{v_i}$ là phần tử nghịch đảo của $\overline{u_i}$ trong $\mathbb{Z}_{ni}$. Khi đó

$$\overline{a_i u_i v_i} = \overline{a}_i\ (\mathbb{Z}_{n_i});$$

$$\forall j \neq i, n_i \,|\, u_j \to \overline{u}_j = \overline{0}\ (\mathbb{Z}_{n_i}) \to \overline{a_j u_j v_j} = \overline{0}\ (\mathbb{Z}_{n_i}).$$

Đặt $x = a_1u_1v_1 + a_2u_2v_2 + \ldots + a_tu_tv_t$, khi đó

Duy nhất. Giả sử $\overline{x} = \overline{y} = \overline{a}_i\ (\mathbb{Z}_{n_i}), \forall i = \overline{1,\ldots,t}$. Khi đó

$$\forall i = \overline{1,\ldots,t},\ \overline{x-y} = \overline{0}\ (\mathbb{Z}_{n_i}) \to n_i \,|\, (x-y) \xrightarrow{5.6} n \,|\, (x-y)$$

$$\Rightarrow x \equiv y (\text{mod } n).$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

4.2 Thí dụ. Tìm tất cả giá trị x thỏa mãn hệ

$$x \equiv 4(\text{mod } 5); x \equiv 2(\text{mod } 8); x \equiv 6(\text{mod } 11).$$

Giải.

$$n = 5.8.11 = 440; u_1 = 8.11 = 88; u_2 = 5.11 = 55; u_3 = 5.8 = 40.$$

$$\left(\overline{88}\right)^{-1} = \left(\overline{3}\right)^{-1} = \overline{2}\ (Z_5); \left(\overline{55}\right)^{-1} = \left(\overline{7}\right)^{-1} = \overline{7}\ (Z_8); \left(\overline{40}\right)^{-1} = \left(\overline{7}\right)^{-1} = \overline{8}\ (Z_{11}).$$

$$\overline{x} = \overline{4.88.2 + 2.55.7 + 6.40.8} = \overline{3394} = \overline{314}\ (\mathbb{Z}_{440}) \Rightarrow x \in \left\{314 + 440t \,|\, t \in \mathbb{Z}\right\}.$$

Thực hành. Tìm tất cả giá trị x thỏa mãn hệ

$$x \equiv 3(\text{mod } 7); x \equiv 5(\text{mod } 9); x \equiv 4(\text{mod } 10).$$

Đáp án.

$$x \in \left\{374 + t.630 \,|\, t \in \mathbb{Z}\right\}.$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

4.3 Định lý Wilson. Nếu p là số nguyên tố thì

$$(p-1)! \equiv -1 (mod\ p).$$

Chứng minh. Nếu p = 2, 3 thì hiển nhiên đúng. Trường hợp $p > 3$, xét vành $\mathbb{Z}_p$. Ta có

$$\overline{a}^2 = \overline{1} \to (\overline{a}+\overline{1})(\overline{a}-\overline{1}) = 0 \to \overline{a} = \overline{1} \vee \overline{a} = \overline{-1} = \overline{p-1}.$$

Suy ra chỉ có $\overline{1}$ và $\overline{p-1}$ là có nghịch đảo trùng với nó. Từ số phần tử của $\{\overline{2}, \ldots, \overline{p-2}\}$ là số chẵn và mỗi phần tử trong tập hợp này có phần tử nghịch đảo khác nó. Do đó ta có thể chia tập hợp trên thành $(p-3)/2$ nhóm, trong đó mỗi nhóm bao gồm 1 phần tử và nghịch đảo của nó. Suy ra $\overline{2}\ldots.\overline{(p-2)} = \overline{1} \to \overline{(p-1)!} = -\overline{1}$, nghĩa là

$$(p-1)! \equiv -1 (mod\ p).$$

4.4 Thí dụ. Với p = 7, trong $\mathbb{Z}_7$ ta có,

$$\left(\overline{2}\right)^{-1} = \overline{4}; \left(\overline{3}\right)^{-1} = \overline{5} \to \overline{2}.\overline{3}.\overline{4}.\overline{5} = \overline{1}.$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

4.4 Định lý Wilson đảo. Cho n là số nguyên dương.

Nếu $(n-1)! \equiv -1 (mod\ n)$ thì n là số nguyên tố.

Chứng minh. Giả sử n không là số nguyên tố, khi đó $n = ab$, với $1 < a, b < n$. Ta có $a|(n-1)!$, từ giả thiết $(n-1)! \equiv -1 (mod\ n)$ dẫn tới $(n = ab)|[(n-1)!+1]$ suy ra $a|[(n-1)!+1]$. Kết hợp bên trên $a|[(n-1)!+1-(n-1)!]$ nghĩa là $a|1$. Điều này mâu thuẫn với giả thiết $a > 1$.

4.5 Thí dụ. 9! + 1 = 362881 không chia hết cho 9, vì vậy 9 không là số nguyên tố.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

4.6 Bổ đề. Cho p là số nguyên tố. Khi đó

$$p \,|\, C_p^k, \forall k = 1,\ldots,p-1.$$

Chứng minh. Xét vành $\mathbb{Z}p$. Ta có

$$\overline{C_p^k} = \left(\frac{p!}{(p-k)!k!}\right) \to \overline{(p-k)!k!}\ \overline{C_p^k} = \overline{p!} = \overline{0}.$$

$((p-k)!k!, p) = 1$ suy ra $\overline{(p-k)!k!}$ khả nghịch. Do đó

$$\overline{C_p^k} = \left(\overline{(p-k)!k!}\right)^{-1} \overline{(p-k)!k!}\ \overline{C_p^k} = \left(\overline{(p-k)!k!}\right)^{-1}.\overline{0} = \overline{0}.$$

Suy ra

$$p \,|\, C_p^k, \forall k = 1,\ldots,p-1.$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

4.7 Định lý Fermat nhỏ. Nếu p là số nguyên tố và a là số nguyên dương không chia hết cho p thì $a^{p-1} \equiv 1 (mod\ p)$.

Chứng minh. Xét $p > 2$ và $\mathbb{Z}_p$. Chọn b sao cho $\overline{a} = \overline{b}, 0 < b < p$ hiển nhiên $\overline{1}^p = \overline{1}$, giả sử $\overline{k}^p = \overline{k}$ $(0 < k < p-2)$. Khi đó

$$\left(\overline{(k+1)}\right)^p = \left(\sum_{i=0}^{p} C_p^i k^{p-i}\right) = \overline{C_p^0 k^p + C_p^p} = \overline{k^p + 1} = \overline{k+1} (\text{do } 4.6)$$

Bởi qui nạp $b^p \equiv b (\text{mod } p)$.

Mặt khác $(b, p) = 1$, do đó $\overline{b}$ khả nghịch. Suy ra

$$b^{p-1} \equiv 1 (\text{mod } p) \to a^{p-1} \equiv 1 (\text{mod } p),$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

Cách chứng minh 2. Xét tập con

$$A=\left\{\overline{a},\overline{2}\overline{a},...,\overline{(p-1)}\overline{a}\right\}\subset\mathbb{Z}_p\setminus\{\overline{0}\}.$$

Nếu $\overline{m}\overline{a}=\overline{n}\overline{a}$ thì do $(a,p)=1$ nên $\overline{a}$ khả nghịch. Suy ra,

$$\overline{m}\overline{a}=\overline{n}\,\overline{a}\rightarrow\overline{m}\,\overline{a}\,\overline{a}^{-1}=\overline{n}\,\overline{a}\,\overline{a}^{-1}\rightarrow\overline{m}=\overline{n}.$$

Do đó số phần tử của tập A bằng p -1 và bằng số phần tử của $\mathbb{Z}_p\setminus\{\overline{0}\}$, dẫn tới

$$A=\left\{\overline{a},\overline{2}\overline{a},...,\overline{(p-1)}\overline{a}\right\}=\mathbb{Z}_p\setminus\{\overline{0}\}=\left\{\overline{1},\overline{2},...,\overline{(p-1)}\right\}.$$

$$\rightarrow\overline{1}.\overline{2}.\ \ldots\ \overline{(p-1)}=\overline{(p-1)!}=\overline{a}.\overline{2}\overline{a}.\ldots\overline{(p-1)}\overline{a}=(\overline{a})^{p-1}\overline{(p-1)!}$$

Từ Định lý Wilson $\overline{(p-1)!}=\overline{-1}$, ta có

$$(\overline{a})^{p-1}=\overline{1}\rightarrow a^{p-1}\equiv 1(\text{mod }p).$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

4.8 Thí dụ. $p=7$ và $a=3$.

$$\overline{1}.\overline{3}=\overline{3};\overline{2}.\overline{3}=\overline{6};\overline{3}.\overline{3}=\overline{9}=\overline{2};\overline{4}.\overline{3}=\overline{12}=\overline{5};\overline{5}.\overline{3}=\overline{15}=\overline{1};\overline{6}.\overline{3}=\overline{18}=\overline{4}.$$

$$\rightarrow\left\{\overline{1}.\overline{3},\overline{2}.\overline{3},\overline{3}.\overline{3},\overline{4}.\overline{3},\overline{5}.\overline{3},\overline{6}.\overline{3}\right\}=\left\{\overline{3},\overline{6},\overline{2},\overline{5},\overline{1},4\right\}$$

4.9 Hệ quả. Cho p là số nguyên tố và a là số nguyên dương. Khi đó

$$\overline{a}^p\equiv a(\text{mod }p).$$

Chứng minh. Nếu p không là ước của a theo Định lý Fermat nhỏ ta có điều chứng minh. Trường hợp p là ước của a, khi đó

$$a\equiv 0(mod\ p)\rightarrow ap\equiv 0^p(mod\ p)\equiv 0(mod\ p)$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

4.10 Thí dụ. Rút gọn $15^{294}(mod\ 17)$.

Giải. $294=17.17+5$.

$15^{294}(mod\ 17)=(15^{17})^{17}.15^5(mod\ 17)=15^5(mod\ 17)=759375(mod\ 17)=2(mod\ 17)$.

Thực hành. Rút gọn $7^{296}(mod\ 13)$.

Đáp án. 10(mod 13).

4.11. Hệ quả. Nếu p là số nguyên tố và a là số nguyên dương không chia hết cho p thì trong $\mathbb{Z}_p$, $(\overline{a})^{-1}=(\overline{a})^{p-2}$.

Chứng minh. Theo Định lý Fermat nhỏ

$$(\overline{a})^{p-1}=\overline{1}\rightarrow(\overline{a})^{-1}=(\overline{a})^{-1}.\overline{1}=(\overline{a})^{-1}(\overline{a})^{p-1}=(\overline{a})^{p-2}.$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

4.12 Định lý Lagrange. Cho $p(x)=\overline{a}_nx^n+\overline{a}_{n-1}x^{n-1}+...+\overline{a}_0,(\overline{a}_n\neq\overline{0})$. với hệ số lấy trong $\mathbb{Z}_p$. Khi đó phương trình $p(x)=0$ có nhiều nhất là n nghiệm.

Chứng minh. Quy nạp theo n.

- $n=1$. Phương trình $\overline{a}_1x+\overline{a}_0=\overline{0}\rightarrow\overline{a}_1x=-\overline{a}_0\rightarrow x=\overline{a}_1^{-1}.(-\overline{a}_0)$. có 1 nghiệm.
- Giả sử mọi đa thức bậc $n-1$ có số nghiệm không vượt quá n -1 và $p(x)=\overline{a}_nx^n+\overline{a}_{n-1}x^{n-1}+...+\overline{a}_0,(\overline{a}_n\neq\overline{0})$ có nghiệm. Gọi $\overline{a}$ là một nghiệm của $p(x)$, $h(x)$ và $r(x)$ lần lượt là thương số và dư số trong phép chia $p(x)$ cho $(x-\overline{a})$. Do bậc của đa thức $(x-\overline{a})$ bằng 1 và bậc của $r(x)$ nhỏ hơn bậc của $(x-\overline{a})$ nên $r(x)$ là hằng số $\overline{u}$. Ta có

$$p(x)=h(x)(x-\overline{a})+\overline{u}\rightarrow\overline{0}=h(\overline{a})(\overline{a}-\overline{a})+\overline{u}=\overline{u}\rightarrow p(x)=h(x)(x-\overline{a}).$$

Bậc $h(x)$ là n - 1, theo qui nạp $h(x)$ có không quá n - 1 nghiệm, do đó $p(x)$ có không quá n nghiệm.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

4.13 Định lý Fermat về tổng của hai số chính phương.

Một số nguyên tố lẻ p biểu diễn được dưới dạng tổng của hai số chính phương, tức là $p=x^2+y^2$, với x,y là các số tự nhiên lớn hơn 0 khi và chỉ khi $p\equiv 1(mod\ 4)$.

4.14 Thí dụ. Các số nguyên tố lẻ 5, 13, 17, 29, 37, 41 đều đồng dư với 1 theo mô-đun 4, do đó chúng biểu diễn được dưới dạng tổng của hai số chính phương: $5=1^2+2^2$, $13=2^2+3^2$, $17=1^2+4^2$, $29=2^2+5^2$, $37=1^2+6^2$, $41=4^2+5^2$ v.v...

Để chứng minh định lý trên, ta cần các bổ đề sau:

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

4.15 Bổ đề. Tích của hai số, mà mỗi số là tổng của hai số chính phương, cũng là tổng của hai số chính phương.

Chứng minh. $(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2$.

4.16 Bổ đề. Nếu một số tự nhiên n mà chia hết cho số nguyên tố p và n lẫn p đều có thể biểu diễn thành tổng của hai số chính phương thì n/p cũng có thể biểu diễn thành tổng của hai số chính phương.

Chứng minh. Biểu diễn $n=a^2+b^2$, $p=c^2+d^2$, với a,b,c,d là các số tự nhiên. Do $(ac+bd)(ac-bd)=a^2c^2-b^2d^2=a^2(c^2+d^2)-(a^2+b^2)d^2=a^2.p-n.d^2$ chia hết cho p và p nguyên tố nên một trong hai số $(ac+bd)$ hoặc $(ac-bd)$ chia hết cho p.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

- Nếu $(ac - bd)$ chia hết cho p. Sử dụng Bổ đề 4.15, ta có

$$\frac{n}{p}=\frac{\left(a^2+b^2\right)}{p}=\frac{\left(a^2+b^2\right)\left(c^2+d^2\right)}{p^2}=\frac{\left(ad+bc\right)^2}{p^2}+\frac{\left(ac-bd\right)^2}{p^2}$$

Do n chia hết cho p và $(ac - bd)$ chia hết cho p nên $\frac{(ad+bc)^2}{p^2}$ là số nguyên dương, do đó $\frac{(ad+bc)^2}{p^2}$ là số chính phương.

- Nếu $(ac + bd)$ chia hết cho p. Sử dụng Bổ đề 4.15, ta có

$$\frac{n}{p}=\frac{\left(a^2+b^2\right)}{p}=\frac{\left(a^2+b^2\right)\left(c^2+d^2\right)}{p^2}=\frac{\left(ac+bd\right)^2}{p^2}+\frac{\left(ad-bc\right)^2}{p^2}$$

Do n chia hết cho p và $(ac + bd)$ chia hết cho p nên $\frac{(ad-bc)^2}{p^2}$ là số nguyên dương, do đó $\frac{(ad-bc)^2}{p^2}$ là số chính phương.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

4.17 Bổ đề. Cho n chia hết cho m, n biểu diễn thành tổng của hai số chính phương còn m không biểu diễn thành tổng của hai số chính phương thì tồn tại một ước dương lớn hơn 1 của n/m không thể biểu diễn thành tổng của hai số chính phương.

Chứng minh. Chứng minh bằng phản chứng. Giả sử mọi ước dương lớn hơn 1 của n/m đều có thể biểu diễn thành tổng của hai số chính phương. Phân tích $n/m = p_1p_2 \ldots pk$ là tích các số nguyên tố không nhất thiết đôi một khác nhau. Theo giả thiết $p_1, p_2, \ldots, p_k$ đều biểu diễn thành tổng của hai số chính phương, áp dụng Bổ đề 4.15 (k - 1) lần ta nhận được $p_1p_2 \ldots pk$ là tổng của hai số chính phương. Áp dụng Bổ đề 4.16 tới $m = (n/p_1p_2 \ldots pk)$ ta có m là tổng của của hai số chính phương. Điều mâu thuẫn này cho ta điều chứng minh.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

4.18 Bổ đề. Nếu a và b nguyên tố cùng nhau thì mọi ước dương lớn hơn 1 của $a^2 + b^2$ đều có thể biểu diễn thành tổng của hai số chính phương.

Chứng minh bằng phản chứng. Giả sử tồn tại các số tự nhiên a và b nguyên tố cùng nhau sao cho $a^2 + b^2$ có ít nhất một ước dương lớn hơn 1 không thể biểu diễn thành tổng của hai số chính phương. Trong các cặp số đó ta xét cặp (a, b) thỏa mãn tổng $(a+b)$ nhỏ nhất.

Xét x là ước dương lớn hơn 1 của $a^2 + b^2$ mà không thể biểu diễn thành tổng của 2 số chính phương. Dùng phép chia Euclide, biểu diễn $a = mx + c$, $b = nx + d$, trong đó c, d là số tự nhiên không vượt quá x - 1. nếu $c = d = 0$ thì x là ước chung của a và b vô lý với giả thiết a, b nguyên tố cùng nhau. Suy ra $c^2 + d^2 > 0$. Ta có

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

$$a^2+b^2=m^2x^2+2mxc+c^2+n^2x^2+2nxd+d^2$$
$$\rightarrow\left(a^2+b^2\right)-(m^2x+2mc+n^2x+2nd)x=c^2+d^2$$

Suy ra $c^2 + d^2$ chia hết cho x. Giả sử $(c, d) = 1$, nếu $c = 0$ thì $d = 1$ dẫn tới $x|1$vô lý. Vậy c và d khác 0, nhưng điều này mâu thuẫn với cách chọn $(a+b)$ nhỏ nhất bởi tổng $c+d < a+b$. Vậy $(c, d) = y > 1$.

Nếu y và x không nguyên tố cùng nhau, thì tồn tại số nguyên tố p sao cho y và x cùng chia hết cho p, suy ra

$$y=rp, x=sp, c=uy=urp, d=vy=vrp$$
$$\rightarrow a=mx+c=msp+urp=(ms+ur)p$$
$$b=nx+d=nsp+vrp=(ns+vr)p$$

Dẫn đến a, b chia hết cho p (mâu thuẫn với giả thiết a và b nguyên tố cùng nhau).Vậy y và x nguyên tố cùng nhau. Đặt

$$c_1=c/y; d_1=d/y.$$

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

Khi đó, c_1, d_1 nguyên tố cùng nhau và $(c_1)^2 + (d_1)^2$ chia hết cho x, nhưng $c_1 + d_1 < a + b$ mâu thuẫn với giả thiết về tổng $(a+b)$ là nhỏ nhất. Suy ra điều giả sử là sai. Ta có điều phải chứng minh.

Chứng minh định lý Fermat (4.13). Giả sử $p = 4k + 1$. Theo Định lý Fermat nhỏ (4.7), các số sau đây đều đồng dư với 1 theo mô-đun p: $1^{4k}, 2^{4k}, \ldots, (4k)^{4k}$. Xét hiệu giữa hai số liên tiếp:

$$i^{4k} - (i-1)^{4k} = (i^{2k} + (i-1)^{2k})(i^{2k} - (i-1)^{2k}),\ i = 2, \ldots, 4k.$$

Do p là số nguyên tố, nên ít nhất một trong hai số $(i^{2k} + (i - 1)^{2k})$ và $(i^{2k} - (i\text{-}1)^{2k})$ chia hết cho p.

Giả sử với mọi i, $(i^{2k} + (i - 1)^{2k}$ không chia hết cho p, suy ra: $(i^{2k} - (i\text{-}1)^{2k})$ chia hết cho p với mọi $i = 2, \ldots, 4k$. Như vậy các số sau đồng dư với nhau đôi một theo mô-đun p: $1^{2k}, 2^{2k}, \ldots, (4k)^{2k}$.

CHƯƠNG 2: VÀNH $\mathbb{Z}_n$ VÀ ĐỒNG DƯ

Suy ra trong $\mathbb{Z}_p$ ta có: $\overline{1}^{2k} = \overline{2}^{2k} = \overline{3}^{2k} = \ldots = (4k)^{2k}$.
do đó phương trình $x^{2k} - \overline{1} = 0$ trong $\mathbb{Z}_p$ có 4k nghiệm. Điều này mâu thuẫn với Định lý Lagrange (4.12). Suy ra tồn tại i sao cho $(i^{2k} + (i - 1)^{2k}$ chia hết cho p. Từ $(i, i - 1) = 1$, áp dụng Mệnh đề 5.5 $k - 1$ lần cho $(i - 1)$, ta nhận được $(i, (i - 1)^k) = 1$.

Tiếp tục áp dụng Mệnh đề 5.5 k -1 lần cho i ta có $(i^k, (i - 1)^k) = 1$. Theo Bổ đề 4.18, p là tổng của hai số chính phương.

Cho chiều đảo, giả sử $p = a^2 + b^2$. Từ p là số lẻ, a phải là số chẵn và b phải là số lẻ. Suy ra $p = (2u)^2 + (2v + 1)^2 = 4(u^2 + v^2 + v) + 1$.