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

4.19 Định lý Wolstenholme. Cho $p > 3$ là số nguyên tố. Khi đó

$$a)\ \frac{1}{1^2}+\frac{1}{2^2}+\ldots+\frac{1}{(p-1)^2}=\frac{m}{n}$$

$(m,n \in \mathbb{N}, (m,n)=1) \Rightarrow m \vdots p.$

$$b)\ \frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{(p-1)}=\frac{m}{n}$$

$(m,n \in \mathbb{N}, (m,n)=1) \Rightarrow m \vdots p^2.$

$c)\ C_{2p-1}^{p-1} \equiv 1 (\mathrm{mod}\ p^3).$

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

Chứng minh.

$$a)\ \frac{1}{1^2}+\frac{1}{2^2}+\ldots+\frac{1}{(p-1)^2}=\frac{m}{n}$$

$$\rightarrow m = n\left(\frac{1}{1^2}+\frac{1}{2^2}+\ldots+\frac{1}{(p-1)^2}\right)$$

Xét trong $\mathbb{Z}_p$.

$$\overline{m}=\overline{n\left(\frac{1}{1^2}+\frac{1}{2^2}+\ldots+\frac{1}{(p-1)^2}\right)}=$$

$$\overline{n}.\left(\left(\overline{1}\right)^{-1}\right)^2+\left(\left(\overline{2}\right)^{-1}\right)^2+\ldots+\left(\left(\overline{p-1}\right)^{-1}\right)^2$$

Do phần tử nghịch đảo là duy nhất và mọi phần tử khác $\overline{0}$ của $\mathbb{Z}_p$ đều khả nghịch nên

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

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

$$\Rightarrow \overline{m}=\overline{n}.\left(\left(\overline{1}\right)^2+\left(\overline{2}\right)^2+\ldots+\left(\overline{p-1}\right)^2\right)=\overline{n}.\overline{\left(\frac{(p-1)p(2p-1)}{6}\right)}$$

Do $p > 3$ nên $(p, 6) = 1$, vì vậy $\overline{6}$ khả nghịch. Suy ra

$$\overline{m}==\overline{n}.\left(\overline{6}\right)^{-1}\overline{(p-1)p(2p-1)}=\overline{0}.$$

$$\Rightarrow m \vdots p.$$

$$b)\ m=n\left(\frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{(p-1)}\right), \text{ trong } \mathbb{Z}p.$$

$$\overline{m}=\overline{n\left(\frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{(p-1)}\right)}=\overline{n}.\left(\left(\overline{1}\right)^{-1}+\left(\overline{2}\right)^{-1}+\ldots+\left(\overline{p-1}\right)^{-1}\right)=$$

$$\overline{n}.\left(\overline{1+2+\ldots+(p-1)}\right)=\overline{n}\overline{\left(\frac{p(p-1)}{2}\right)}$$

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

Do $p > 3$ nên $(p, 2) = 1$, vì vậy $\overline{2}$ khả nghịch. Suy ra

$$\overline{m}==\overline{n}.\left(\overline{2}\right)^{-1}\overline{(p-1)p}=\overline{0}\Rightarrow m \vdots p.$$

đặt $m_1 = m : p$, $(m_1, n) = 1$. Mặt khác

$$2\frac{m}{n}=2\left(\frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{(p-1)}\right)=$$

$$\left(\frac{1}{1}+\frac{1}{p-1}\right)+\left(\frac{1}{2}+\frac{1}{p-2}\right)+\ldots+\left(\frac{1}{p-1}+\frac{1}{p-(p-1)}\right)=$$

$$\left(\frac{p}{1(p-1)}\right)+\left(\frac{p}{2(p-2)}\right)+\ldots+\left(\frac{p}{(p-1)[p-(p-1)]}\right)=p\sum_{i=1}^{p-1}\frac{1}{i(p-i)}$$

$$\Rightarrow 2m_1=n\sum_{i=1}^{p-1}\frac{1}{i(p-i)}$$

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

Xét trong $\mathbb{Z}_p$. Ta có $\overline{p-i}=\overline{-i}$, suy ra

$$\overline{m}_1=\left(\overline{2}\right)^{-1}\overline{n\left(\frac{1}{1(p-1)}+\frac{1}{2(p-2)}+\ldots+\frac{1}{(p-1)[p-(p-1)]}\right)}=$$

$$\left(\overline{2}\right)^{-1}\overline{n}.\left(\left(\overline{1}\right)^{-1}\left(\overline{p-1}\right)^{-1}+\left(\overline{2}\right)^{-1}\left(\overline{p-2}\right)^{-1}+\ldots+\left(\overline{p-1}\right)^{-1}\left(\overline{p-(p-1)}\right)^{-1}\right)=$$

$$\left(\overline{2}\right)^{-1}\overline{n}\left(\left(\overline{1}\right)^{-2}+\left(\overline{2}\right)^{-2}+\ldots+\left(\overline{p-1}\right)^{-2}\right)=$$

$$-\left(\overline{2}\right)^{-1}\overline{n}\left(\left(\overline{1}\right)^{2}+\left(\overline{2}\right)^{2}+\ldots+\left(\overline{p-1}\right)^{2}\right)=$$

$$-\left(\overline{2}\right)^{-1}\overline{n}\overline{\left(\frac{p(p-1)(2p-1)}{6}\right)}=-\left(\overline{2}\right)^{-1}\overline{n}\left(\overline{6}\right)^{-1}\overline{p(p-1)(2p-1)}=\overline{0}.$$

$$\Rightarrow m_1 \vdots p \rightarrow m \vdots p^2.$$

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

$$c)\ C_{2p-1}^{p-1}\equiv 1(\mathrm{mod}\ p^3)\Leftrightarrow C_{2p-1}^{p-1}-1\equiv 0(\mathrm{mod}\ p^3)\Leftrightarrow p^3\,\middle|\,(C_{2p-1}^{p-1}-1).$$

$$C_{2p-1}^{p-1}-1=\frac{(p+1)(p+2)\ldots(p+(p-1))-(p-1)!}{(p-1)!}$$

Xét khai triển đa thức.

$$f(x)=(x+1)(x+2)\ldots.(x+(p-1))-(p-1)!=$$

$$x^{p-1}+s_{p-2}x^{p-2}+\ldots+s_2x^2+s_1x.$$

$$s_1=(p-1)!\left(\frac{1}{1}+\frac{1}{2}+\ldots+\frac{1}{p-1}\right);$$

$$s_2=(p-1)!\left(\begin{array}{l}\frac{1}{1.2}+\frac{1}{1.3}+\ldots+\frac{1}{1.(p-1)}+\frac{1}{2.3}+\frac{1}{2.4}+\\ +\ldots+\frac{1}{2.(p-1)}+\ldots+\frac{1}{(p-2)(p-1)}\end{array}\right)$$

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

$$(p-1)!\left(C_{2p-1}^{p-1}-1\right)=f(p)=p^{p-1}+...+s_2p^2+s_1=$$

$$Ap^3+p^2(p-1)!\begin{pmatrix}\frac{1}{1.2}+\frac{1}{1.3}+...+\frac{1}{1.(p-1)}+\frac{1}{2.3}+\frac{1}{2.4}+\\+...+\frac{1}{2.(p-1)}+...+\frac{1}{(p-2)(p-1)}\end{pmatrix}+$$

$$+p(p-1)!\left(\frac{1}{1}+\frac{1}{2}+...+\frac{1}{p-1}\right);$$

Áp dụng câu (b)

$$(p-1)!\left(\frac{1}{1}+\frac{1}{2}+...+\frac{1}{p-1}\right)\vdots p^2$$

$$\Rightarrow p(p-1)!\left(\frac{1}{1}+\frac{1}{2}+...+\frac{1}{p-1}\right)\vdots p^3$$

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

Mặt khác, trong $\mathbb{Z}_p$.

$$\overline{(p-1)!\begin{pmatrix}\frac{1}{1.2}+\frac{1}{1.3}+...+\frac{1}{1.(p-1)}+\frac{1}{2.3}+\frac{1}{2.4}+\\+...+\frac{1}{2.(p-1)}+...+\frac{1}{(p-2)(p-1)}\end{pmatrix}}=$$

$$\overline{(p-1)!}\begin{pmatrix}(\overline{1})^{-1}(\overline{2})^{-1}+(\overline{1})^{-1}(\overline{3})^{-1}+...+(\overline{1})^{-1}(\overline{p-1})^{-1}+(\overline{2})^{-1}(\overline{3})^{-1}+\\+(\overline{2})^{-1}(\overline{4})^{-1}+...+(\overline{2})^{-1}(\overline{p-1})^{-1}+...+(\overline{p-2})^{-1}(\overline{p-1})^{-1}\end{pmatrix}=$$

$$\overline{(p-1)!}\begin{pmatrix}\overline{1.2+1.3+...+1(p-1)+2.3+2.4+...+2.(p-1)+}\\\overline{+...+(p-2)(p-1)}\end{pmatrix}$$

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

Ta có

$$1+2+...+k=\frac{k(k+1)}{2};1^2+2^2+...+k^2=\frac{k(k+1)(2k+1)}{6};$$

$$1^3+2^3+...+k^3=\frac{k^2(k+1)^2}{4}$$

suy ra

$$1.2+1.3+...+1(p-1)+2.3+2.4+...+2.(p-1)+...+(p-2)(p-1)=$$

$$1\left(\frac{(p-1)p}{2}-1\right)+2\left(\frac{(p-1)p}{2}-(1+2)\right)+...+$$

$$+(p-2)\left(\frac{(p-1)p}{2}-(1+2+...+(p-2))\right)=$$

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

$$\sum_{i=1}^{p-2}i\left(\frac{(p-1)p}{2}-\frac{i(i+1)}{2}\right)=$$

$$\frac{1}{2}\left[(p-1)p\sum_{i=1}^{p-2}i-\sum_{i=1}^{p-2}i^3-\sum_{i=1}^{p-2}i^2\right]=$$

$$\frac{1}{2}\left((p-1)p\frac{(p-2)(p-1)}{2}-\frac{(p-2)^2(p-1)^2}{4}-\frac{(p-2)(p-1)(2p-3)}{6}\right)=$$

$$\frac{(p-1)(p-2)p(3p-1)}{24}$$

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

ta có $(24, p)=1$, kết hợp các kết quả trên ta có

$$\overline{(p-1)!\begin{pmatrix}\frac{1}{1.2}+\frac{1}{1.3}+...+\frac{1}{1.(p-1)}+\frac{1}{2.3}+\frac{1}{2.4}+\\+...+\frac{1}{2.(p-1)}+...+\frac{1}{(p-2)(p-1)}\end{pmatrix}}=$$

$$(\overline{24})^{-1}\overline{(p-1)(p-2)p(3p-1)}=\overline{0}$$

$$\Rightarrow(p-1)!\begin{pmatrix}\frac{1}{1.2}+\frac{1}{1.3}+...+\frac{1}{1.(p-1)}+\frac{1}{2.3}+\frac{1}{2.4}+\\+...+\frac{1}{2.(p-1)}+...+\frac{1}{(p-2)(p-1)}\end{pmatrix}\vdots p$$

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

$$(p-1)!\left(C_{2p-1}^{p-1}-1\right)\vdots p^3\Rightarrow\overline{(p-1)!}\,\overline{C_{2p-1}^{p-1}-1}=\overline{0}\ (\mathbb{Z}_{p^3}).$$

từ $((p-1)!, p^3)=1$, $\overline{(p-1)!}$ khả nghịch trong $\mathbb{Z}_{p^3}$. Suy ra

$$\overline{C_{2p-1}^{p-1}-1}=\left(\overline{(p-1)!}\right)^{-1}\overline{(p-1)!}\,\overline{C_{2p-1}^{p-1}-1}=\left(\overline{(p-1)!}\right)^{-1}.\overline{0}=\overline{0}$$

$$\Rightarrow\overline{C_{2p-1}^{p-1}}=\overline{1}\ (\mathbb{Z}_{p^3})\Rightarrow C_{2p-1}^{p-1}\equiv1(\text{mod } p^3).$$

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

4.20 Định lý Euler.

4.20.1 Định nghĩa. Cho n là số nguyên. $\phi(n)$ được gọi là hàm phi-Euler được định nghĩa là số các số nguyên dương không vượt quá n và nguyên tố cùng nhau với n.

4.20.2 Thí dụ.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

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

4.20.2 Định nghĩa. Một hệ *reduced residue* (mod n) là một tập hợp gồm $\phi(n)$ phần tử, mỗi phần tử trong hệ nguyên tố cùng nhau với n và hai phần tử phân biệt trong hệ không đồng dư (mod n) với nhau.

4.20.3 Thí dụ. các {1, 2, 4, 5, 7, 8}, {-2, -1, 1, 2, 4, 5} đều là hệ reduced rescidue mod 9.

4.20.4 Mệnh đề. Nếu $\{a_1, a_2, ..., a_{\phi(n)}\}$ là hệ reduced rescidue và u là số nguyên dương thỏa $(u, n) = 1$ thì $\{ua_1, ua_2, ..., ua_{\phi(n)}\}$ cũng là hệ reduced rescidue.

Chứng minh. $\forall i, (a_i, n) = 1 \wedge (u, n) = 1 \Rightarrow \xrightarrow{5.5} (ua_i, n) = 1.$

$$ua_i \equiv ua_j (\text{mod } n) \Rightarrow \overline{ua_i} = \overline{ua_j} (\mathbb{Z}_n) \Rightarrow \overline{u}^{-1}\overline{ua_i} = \overline{u}^{-1}\overline{ua_j}$$

$$\Rightarrow \overline{a}_i = \overline{a}_j \Rightarrow a_i \equiv a_j (\text{mod } n) \Rightarrow i = j.$$

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

4.20.5 Thí dụ. {1, 2, 4, 5, 7, 8} là hệ reduced rescidue mod 9, (11, 9) = 1, do đó {11, 22, 44, 55, 77, 88} là hệ reduced rescidue mod 9.

4.20.6 Nhận xét. Nếu $\{a_1, a_2, ..., a_{\phi(n)}\}$ là hệ reduced rescidue mod n thì $\{\overline{a}_1, \overline{a}_2, ..., \overline{a}_{\phi(n)}\}$ tập các phần tử khả nghịch của $\mathbb{Z}_n$.

4.20.7 Định lý Euler. Cho n là số nguyên dương. Nếu $(a, n) = 1$ thì

$$a^{\phi(n)} \equiv 1 (\text{mod } n).$$

Chứng minh. Gọi $\{u_1, u_2, ..., u_{\phi(n)}\}$ là hệ reduced rescidue, khi đó theo (4.20.4) $\{au_1, au_2, ..., au_{\phi(n)}\}$ là hệ reduced rescidue. Theo 4.20.6

$$\{\overline{u}_1, \overline{u}_2, ..., \overline{u}_{\phi(n)}\} = \{\overline{au}_1, \overline{au}_2, ..., \overline{au}_{\phi(n)}\}$$

$$\Rightarrow \overline{u}_1\overline{u}_2...\overline{u}_{\phi(n)} = \overline{a}^{\phi(n)}\overline{u}_1\overline{u}_2...\overline{u}_{\phi(n)}$$

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

$\overline{u}_1\overline{u}_2...\overline{u}_{\phi(n)}$ khả nghịch, do đó

$$\overline{1} = \left(\overline{u}_1\overline{u}_2...\overline{u}_{\phi(n)}\right)^{-1}\overline{u}_1\overline{u}_2...\overline{u}_{\phi(n)} = \overline{a}^{\phi(n)}\overline{u}_1\overline{u}_2...\overline{u}_{\phi(n)}\left(\overline{u}_1\overline{u}_2...\overline{u}_{\phi(n)}\right)^{-1} = \overline{a}^{\phi(n)}$$

$$\Rightarrow a^{\phi(n)} \equiv 1 (\text{mod } n).$$

4.20.8 Hệ quả. Cho n là số nguyên dương. Nếu $(a, n) = 1$ thì

$$\overline{a}^{-1} = \overline{a}^{(\phi(n)-1)} (\mathbb{Z}_n).$$

4.20.9 Thí dụ. a) Trong $\mathbb{Z}_9$,

$$\left(\overline{4}\right)^{-1} = \left(\overline{4}\right)^{\phi(9)-1} = \left(\overline{4}\right)^{6-1} = \overline{1024} = \overline{7}.$$

b) Trong $\mathbb{Z}_9$, tính $\left(\overline{7}\right)^{259}$.

$$261 = \phi(9) \times 43 + 3 \Rightarrow \left(\overline{7}\right)^{261} = \left(\left(\overline{7}\right)^{\phi(9)}\right)^{43}\left(\overline{7}\right)^3 = \overline{343} = \overline{1}.$$

Thực Hành. Tính $\left(\overline{11}\right)^{572}$ $(\mathbb{Z}_7)$.

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

§5 Hàm số học.

5.1 Định nghĩa.

a) Hàm số đi từ tập con của $\mathbb{N}$ vào $\mathbb{N}$ được gọi là *hàm số học*.

b) Hàm số $f : D \subset \mathbb{N} \to \mathbb{N}$ được gọi là *nhân tính* nếu

$$(m, n) = 1 \Rightarrow f(mn) = f(m)f(n).$$

5.2 Thí dụ. Hàm $g(a) = a$ là hàm nhân tính vì $g(mn) = mn = g(m)g(n)$

Hàm $h(a) = 1$, $\forall a$ là hàm nhân tính vì $h(ab) = 1 = h(a)h(b)$.

5.3 Mệnh đề. Cho f là hàm nhân tính và $n = p_1^{a_1}p_2^{a_2}...p_t^{a_t}$ với các p_i là số nguyên tố. Khi đó

$$f(n) = f(p_1)^{a_1}f(p_2)^{a_2}...f(p_t)^{a_t}.$$

Chứng minh. Qui nạp theo t.

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

5.4 Định lý.

a) Nếu p là số nguyên tố thì $\phi(p) = p - 1$.

b) Nếu p là số nguyên dương thỏa $\phi(p) = p - 1$ thì p là số nguyên tố.

Chứng minh.

a) Nếu $0 < a < p$ thì $(a, p) = 1$, do đó $\phi(p) = p - 1$.

b) Giả sử p không nguyên tố, khi đó có a thỏa $p = a.b$, $p > a > 1$. Từ định nghĩa của $\phi(p)$ ta có $A = \{1, 2, ..., p - 1\}$ là tập cả các phần tử nguyên dương không vượt quá p nguyên tố cùng nhau với p.

Suy ra $a \in A$, nghĩa là a nguyên tố cùng nhau với p. Điều này mâu thuẫn với a là ước của p (đpcm).

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

5.5 Định lý. cho p là số nguyên tố và n là số nguyên dương. Khi đó

$$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1) = p^n\left(1-\frac{1}{p}\right).$$

Chứng minh. Chia $\{1, 2, ..., p^n\}$ làm p^n - 1 tập hợp như sau:

$$\{1,2,...,p\},\{p+1,p+2,...,2p\},...,\{p^{n-1}+1,p^{n-1}+2,...,p^n\}$$

Trong mỗi tập con này chỉ có duy nhất một phần tử không nguyên tố cùng nhau với p. Suy ra số phần tử không nguyên tố cùng nhau với p bằng p^n-1, do đó

$$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1).$$

5.6 Thí dụ. $\phi(5^3) = 5^3 - 5^2 = 100; \phi(2^{10}) = 2^{10} - 2^9 = 512.$

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

5.7 Định lý. Cho m, n là các số nguyên dương và (m, n) =1. Khi đó

$$\phi(mn) = \phi(m)\phi(n).$$

Chứng minh. Biểu diễn 1, 2, ..., mn bằng ma trận sau

$$\begin{pmatrix} 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ m & 2m & 3m & \cdots & nm \end{pmatrix}$$

Nếu $0 < i < m + 1$, $(m, i) = d > 1$thì trên dòng thứ i không có phần tử nào nguyên tố cùng nhau với mn. Thật vậy, mỗi phần tử trên dòng i có dạng $tm + i$, từ $d|m$ và $d|i$ ta có $d|(tm + i)$. Suy ra

$$(tm + i, mn) \vdots\, d > 1.$$

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

xét dòng i có (m, i) =1. Trong $\mathbb{Z}_n$, từ (m, n) =1 ta có $\overline{m}$ khả nghịch

$$\Rightarrow \{\overline{1},\overline{2},\overline{3},...,\overline{n-1}\} = \{\overline{m},\overline{2m},...,\overline{(n-1)m}\} =$$
$$\{\overline{i},\overline{2m+i},\overline{3m+i},...,\overline{(n-1)m+i}\}$$

Suy ra trên dòng i có đúng $\phi(n)$ phần tử nguyên tố cùng nhau với n. Mặt khác, với mọi $0 \le t \le$, $(tm + i, m) = (i, m)$ =1. Suy ra mỗi phần tử nguyên tố cùng nhau với n trên dòng i, cũng nguyên tố cùng nhau với mn.

Ta có $\phi(m)$ dòng i thỏa $(m, i) = 1$ và do đó có tất cả $\phi(m)\phi(n)$ phần tử trong ma trận nguyên tố cùng nhau với mn.

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

5.8 Định lý. Cho $n = p_1^{a_1} p_2^{a_2} ... p_t^{a_t}$ là sự phân tích thành tích các thừa số nguyên tố. Khi đó

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_t}\right) = n\prod_{i=1}^{t}\left(1-\frac{1}{p_i}\right)$$

Chứng minh. Theo Định lý 5.5 và Định lý 5.7 Ta có

$$\phi(n) = \phi(p_1^{a_1}p_2^{a_2}...p_t^{a_t}) = \phi(p_1^{a_1})\phi(p_2^{a_2})...\phi(p_t^{a_t}) =$$
$$p_1^{a_1}\left(1-\frac{1}{p_1}\right)p_2^{a_2}\left(1-\frac{1}{p_2}\right)...p_t^{a_t}\left(1-\frac{1}{p_t}\right) =$$
$$p_1^{a_1}p_2^{a_2}...p_t^{a_t}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_t}\right) =$$
$$n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_t}\right) = n\prod_{i=1}^{t}\left(1-\frac{1}{p_i}\right).$$

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

5.10 Thí dụ

$$\phi(720) = \phi(2^4 3^2 5) = 720\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 192.$$

Thực hành. Tính $\phi(136125)$

Đáp án. 66000.

5.9 Định nghĩa. Cho f là hàm số học. Tổng tất cả các giá trị của f tại mọi ước số dương của n được kí hiệu là:

$$\sum_{d|n} f(d)$$

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

5.10 Thí dụ. $\sum_{d|12} f(d) = f(1) + f(2) + f(3) + f(6) + f(12).$

5.11 Định lý. Cho n là số nguyên dương. Khi đó

$$\sum_{d|n} \phi(n) = n.$$

Chứng minh. Với d là ước số dương của n, ta đặt

$$C_d = \{m \in \mathbb{N} | 1 \le m \le n, (m,n) = d\} =$$
$$\left\{m \in \mathbb{N} \middle| \frac{1}{d} \le \frac{m}{d} \le \frac{n}{d}, \left(\frac{m}{d},\frac{n}{d}\right) = 1\right\}.$$

Suy ra $|C_d| = \phi(n/d)$. Nếu $m \in C_{d_1} \cap C_{d_2}$ thì $(m,n) = d_1 = d_2$.Suy ra nếu $d_1 \ne d_2$ thì $C_{d_1} \cap C_{d_2} = \varnothing$.

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

Mặt khác $\forall m \in \{1,2,\ldots,n\}$, đặt $(m,n) = d$, do đó $m \in Cd$. Suy ra tập hợp $\{1,2,\ldots,n\}$ chia thành các lớp C_d, trong đó d chạy hết trong tập các ước số dương của n. Vậy

$$n = \sum_{d|n} C_d = \sum_{d|n} \phi\left(\frac{n}{d}\right)$$

Để ý nếu $d_1|n$ thì tồn tại duy nhất $d_2|n$ sao cho $d_1 d_2 = n$. Suy ra

$$\{d > 0 \mid d \mid n\} = \left\{\frac{n}{d} \middle| d > 0, d \mid n\right\}.$$

Kéo theo

$$n = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d).$$

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

Để minh họa cho định lý trên, xét $n = 18 = 2.3^2$ các ước dương của n là 1, 2, 3, 6, 9,18. Ta có

$$\{d > 0 | d \mid 18\} = \{1,2,3,6,9,18\} = \left\{\frac{n}{d} \middle| d > 0, d \mid n\right\} = \{18,9,6,3,2,1\}.$$

$$C_1 = \{1,5,7,11,13,17\}; C_2 = \{2,4,8,10,14,16\}; C_3\{3,5\};$$
$$C_6 = \{6,12\}; C_9 = \{9\}; C_{18} = \{18\}.$$
$$|C_1| = \phi\left(\frac{18}{1}\right) = \phi(18) = 18\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 6;$$
$$|C_2| = \phi\left(\frac{18}{2}\right) = \phi(9) = 9\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 3;$$
$$|C_3| = \phi\left(\frac{18}{3}\right) = \phi(6) = 6\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 2$$

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

$$|C_6| = \phi\left(\frac{18}{6}\right) = \phi(3) = 3\left(1-\frac{1}{3}\right) = 2;$$
$$|C_9| = \phi\left(\frac{18}{9}\right) = \phi(2) = 2\left(1-\frac{1}{2}\right) = 1;$$
$$|C_{18}| = \phi\left(\frac{18}{18}\right) = \phi(1) = 1.$$
$$n = \sum_{d|n} \phi(d) = \phi(1) + \phi(2) + \phi(3) + \phi(6) + \phi(9) + \phi(16)$$
$$= 6 + 6 + 2 + 2 + 1 + 1 = 18.$$