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

5.12 Hàm tổng các ước số σ: Cho n là số nguyên dương, giá trị của $\sigma(n)$ bằng tổng các ước số của n.

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

5.13 Thí dụ.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18	12	28

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

5.14 Hàm số các ước số τ: Cho n là số nguyên dương, giá trị của $\tau(n)$ bằng số các ước số của n.

$$\tau(n)=\sum_{d|n} 1.$$

5.15 Thí dụ.

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

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

5.16 Mệnh đề. Cho m,n là hai số nguyên dương và $(m, n) = 1$. Khi đó nếu d là ước dương của mn thì tồn tại duy nhất hai số nguyên dương a, b sao cho

$$a \mid m;\ b \mid n;\ d = a.b.$$

Chứng minh. phân tích m, n thành tích các thừa số nguyên tố.
$n = p_1^{r_1} p_2^{r_2} ... p_t^{r_t}; m = q_1^{s_1} q_2^{s_2} ... q_k^{s_k}$. Từ $(m, n) = 1$, ta có $p_1,...,p_t,q_1,...,q_k$ là các số nguyên tố phân biệt. Theo Bổ đề 5.12 chương 1, d có dạng

$$d = p_1^{u_1} p_2^{u_2} ... p_t^{u_t}.q_1^{v_1} q_2^{v_2} ... q_k^{v_k}$$

Đặt

$$a = p_1^{u_1} p_2^{u_2} ... p_t^{u_t}; b = q_1^{v_1} q_2^{v_2} ... q_k^{v_k} \Rightarrow d = ab; a \mid m, b \mid n.$$

chứng minh duy nhất. Giả sử $d = a_1b_1 = a_2b_2 (a_1 \mid m; a_2 \mid m; b_1 \mid n; b_2 \mid n)$

$$\Rightarrow \begin{cases} a_1 \mid a_2b_2 \\ a_2 \mid a_1b_1 \end{cases} \xrightarrow{(a_1,b_2)=1;(a_2,b_1)=1} \begin{cases} a_1 \mid a_2 \\ a_2 \mid a_1 \end{cases} \Rightarrow a_1 = a_2 \Rightarrow b_1 = b_2.$$

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

5.17 Định lý.Nếu f là hàm nhân tính thì hàm $F(n)=\sum_{d|n} f(d)$ Cũng là hàm nhân tính nghĩa là nếu $(m, n) = 1$ thì

$$F(mn) = F(m)F(n).$$

Chứng minh. Giả sử m, n là hai số nguyên dương nguyên tố cùng nhau. Theo Mệnh đề 5.6

$$F(mn)=\sum_{d|mn} f(d)=\sum_{d_1|m;d_2|n} f(d_1d_2)$$

Từ $(m,n)=1\Rightarrow(d_1,d_2)=1$ và f là hàm nhân tính, ta có

$$\sum_{d_1|m;d_2|n} f(d_1d_2)=\sum_{d_1|m;d_2|n} f(d_1)f(d_2)=$$
$$\sum_{d_1|m}\sum_{d_2|n} f(d_1)f(d_2)=\sum_{d_1|m} f(d_1)\sum_{d_2|n} f(d_2)=F(m)F(n).$$

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

với $m = 2^2.5$, $n = 3.7$, $mn = 420$. Tập hợp các ước dương của mn là:
{1 = 1.1, 2 = 2.1, 3 = 1.3, 4 = 4.1, 5 = 5.1, 6 = 2.3, 7 = 7.1,10 = 10.1, 12 = 4.3, 14 = 2.7,15 = 5.3, 20 = 20.1, 21 = 3.7, 28 = 4.7, 30 10.3, 35 = 5.7, 42 = 2.21, 60 = 20.3, 70 = 10.7, 84 = 4.21, 105 = 5.21, 140 = 20.7, 210 = 10.21, 420 = 20.21}.

$$F(m=2^2.5)=f(1)+f(2)+f(4)+f(5)+f(10)+f(20).$$
$$F(n=3.7)=f(1)+f(3)+f(7)+f(21).$$
$$F(mn)=f(1)f(1)+f(2)f(1)+f(1)f(3)+f(4)f(1)+$$
$$+f(5)f(1)+f(2)f(3)+f(1)f(7)+f(10)f(1)+f(4)f(3)+$$
$$+f(5)f(3)+f(20)f(1)+f(1)f(21)+f(4)f(7)+f(10)f(3)+$$
$$+f(5)f(35)+f(2)f(21)+f(20)f(3)+f(10)f(7)+f(4)f(21)+$$
$$+f(5)f(21)+f(20)f(7)+f(10)f(21)+f(20)f(21).$$

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

$$=\big(f(1)+f(2)+f(4)+f(5)+f(10)+f(20)\big)f(1)+$$
$$+\big(f(1)+f(2)+f(4)+f(5)+f(10)+f(20)\big)f(3)+$$
$$+\big(f(1)+f(2)+f(4)+f(5)+f(10)+f(20)\big)f(7)+$$
$$+\big(f(1)+f(2)+f(4)+f(5)+f(10)+f(20)\big)f(21)=$$
$$\big(f(1)+f(2)+f(4)+f(5)+f(10)+f(20)\big)\times$$
$$\big(f(1)+f(3)+f(7)+f(21)\big)=F(m)F(n).$$

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

5.18 Định lý. Hàm số học σ và hàm số học τ là các hàm nhân tính.

Chứng minh. Ta có ánh xạ đồng nhất từ $\mathbb{N}$ vào $\mathbb{N}$ và hàm số học biến mọi số nguyên dương thành phần tử là các hàm nhân tính. Áp dụng Định lý 5.17 với $(m, n) = 1$, ta có

$$\sigma(mn) = \sum_{d|mn} d = \sum_{d_1|m} d_1 \sum_{d_2|n} d_2 = \sigma(m)\sigma(n).$$

$$\tau(mn) = \sum_{d|mn} 1 = \sum_{d_1|m} 1 \sum_{d_2|n} 1 = \tau(m)\tau(n).$$

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

5.19 Bổ đề. Cho p là số nguyên tố và k là số nguyên dương. Khi đó

$$\sigma(p^k) = (1 + p + p^2 + ... + p^k) = \frac{p^{k+1} - 1}{p - 1}.$$

Chứng minh. Các ước dương của p^k là $1, p, p^2, ..., p^k$ do đó

$$\sigma(p^k) = (1 + p + p^2 + ... + p^k) = \frac{p^{k+1} - 1}{p - 1}.$$

5.20 Thí dụ.

$$\sigma(5^3) = 1 + 5 + 5^2 + 5^3 = 156.$$

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

5.21 Định lý. Cho $n = p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$ là sự phân tích ra thừa số nguyên tố của n. Khi đó

$$\sigma(n) = \frac{(p_1^{n_1+1} - 1)}{p_1 - 1} \frac{(p_2^{n_2+1} - 1)}{p_2 - 1} ... \frac{(p_k^{n_k+1} - 1)}{p_k - 1} = \prod_{i=1}^{k} \left(\frac{p_i^{n_i+1} - 1}{p_i - 1} \right).$$

$$\tau(n) = (n_1 + 1)(n_2 + 1) \cdots (n_k + 1) = \sum_{i=1}^{k} (n_i + 1).$$

Chứng minh. Áp dụng Định lý 5.18 và Bổ đề 5.19, ta có

$$\sigma(n) = \sigma(p_1^{n_1}) \cdots \sigma(p_k^{n_k}) = \frac{(p_1^{n_1+1} - 1)}{p_1 - 1} \cdots \frac{(p_k^{n_k+1} - 1)}{p_k - 1} = \prod_{i=1}^{k} \left(\frac{p_i^{n_i+1} - 1}{p_i - 1} \right).$$

kết quả sau chính là Mệnh đề 5.15 chương 1.

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

5.22 Thí dụ.

$$\sigma(2^3 7^2 11) = \frac{2^4 - 1}{2 - 1} \times \frac{7^3 - 1}{7 - 1} \times \frac{11^2 - 1}{11 - 1} = 10260.$$

$$\tau(2^3 7^2 11) = 4 \times 3 \times 2 = 24.$$

Thực hành. Cho $n = 114075$, tính $\sigma(n); \tau(n)$.

Đáp án. $\sigma(n) = 226920, \tau(n) = 36$.

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

§6 Cấp của số nguyên và nghiệm nguyên thủy.

6.1 Định nghĩa. Cho a và n là hai số nguyên dương và $(a, n) = 1$. Số nguyên dương k nhỏ nhất sao cho $a^k \equiv 1 (mod\ n)$ được gọi là ***cấp*** của a mod n. Cấp của a được kí hiệu là $ord_n a$.

6.2 Thí dụ.

a) $2^1 \equiv 2 (mod\ 7), 2^2 \equiv 4 (mod\ 7), 2^3 \equiv 1 (mod\ 7) \rightarrow ord_7 2 = 3.$

b) $3^1 \equiv 3 (mod\ 7), 3^2 \equiv 2 (mod\ 7), 3^3 \equiv 6 (mod\ 7),$
$3^4 \equiv 4 (mod\ 7), 3^5 \equiv 5 (mod\ 7), 3^6 \equiv 1 (mod\ 7) \rightarrow ord 73 = 6.$

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

6.3 Mệnh đề. Cho n và a là hai số nguyên thỏa $n > 0$, $(a, n) = 1$. khi đó $a^x \equiv 1 (\text{mod } n)$ khi và chỉ khi $(ord_n a) | x$.

Chứng minh. Giả sử $a^x \equiv 1 (\text{mod } n)$, dùng phép chia Euclid

$$x = q(ord_n a) + r, 0 \le r < (ord_n a) \Rightarrow a^x = \left(a^{ord_n a}\right)^q . a^r.$$

$$\Rightarrow a^x = \left(a^{ord_n a}\right)^q a^r \equiv 1^q a^r (\text{mod } n) \equiv a^r (\text{mod } n) \equiv 1 (\text{mod } n).$$

Từ định nghĩa của $ord_n a$ và $r < n$, ta có $r = 0$. Vậy $ord_n a$ là ước của n.

Nếu $(ord_n a) | x$ thì $(ord_n a) k = x$. Suy ra

$$a^x = \left(a^{ord_n a}\right)^k \equiv 1^k (\text{mod } n) \equiv 1 (\text{mod } n).$$

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

6.4 Hệ quả. Nếu $(a, n)=1$ và $n>0$ thì $ord_n a \mid \phi(n)$.

Chứng minh. Theo Định lý Euler $a^{\phi(n)} \equiv 1 \pmod n$, áp dụng 6.3 ta có $ord_n a \mid \phi(n)$.

6.5 Thí dụ. Tính $ord_{17}5$.

Ta có $\phi(17)=16$, suy ra $ord_{17}5 = 1;2;4;8;16$.

$$5^2 \equiv 8 \pmod{17}; 5^4 \equiv 3 \pmod{17}; 5^8 = 13 \pmod{17};$$
$$5^{16} \equiv 1 \pmod{17} \Rightarrow ord_{17}5 = 16.$$

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

6.6 Mệnh đề. Cho $(a, n)=1$, $n>0$ và i, j là hai số tự nhiên. Khi đó $a^i \equiv a^j \pmod n$ khi và chỉ khi $i \equiv j \pmod{ord_n a}$.

Chứng minh. giả sử $j < i$.

$$a^i \equiv a^j \pmod n \Leftrightarrow a^{i-j} \equiv 1 \pmod n$$
$$\xleftrightarrow{6.3} ord_n a \mid (i-j) \Leftrightarrow i \equiv j \pmod{(ord_n a)}.$$

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

6.7 Định nghĩa. Cho $(r, n)=1$, $n>0$. Nếu $ord_n r = \phi(n)$ thì r được gọi là nghiệm nguyên thủy của mod n.

6.8 Thí dụ. Ta có $ord_{17}5 = 16 = \phi(17)$. Suy ra 5 là nghiệm nguyên thủy mod 17.

6.9 Mệnh đề. Cho $(r, n)=1$, $n>0$ và r là nghiệm nguyên thủy mod n. Khi đó $r^1, r^2, \dots, r^{\phi(n)}$ là hệ reduced residue mod n.

Chứng minh. xét $\{r^1, r^2, \dots, r^{\phi(n)}\}$. Nếu $r^i \equiv r^j \pmod n$ thì $r^{(i-j)} \equiv 1 \pmod n$. Theo 6.6 $(i-j) \equiv 1 \pmod{ord_n r}$ hay $ord_n r \mid (i-j)$.

Từ $-ord_n r < i-j < ord_n r$, ta có $i=j$. Suy ra $\{r^1, r^2, \dots, r^{\phi(n)}\}$ có đúng $\phi(n)$ phần tử nguyên tố cùng nhau với n. Do đó $\{r^1, r^2, \dots, r^{\phi(n)}\}$ là hệ reduced residue mod n.

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

6.10 Thí dụ. $\phi(9)=6$, $ord_9 2 = 1;2;3;6$.

$$2^2 \equiv 4 \pmod 9; 2^3 \equiv 8 \pmod 9; 2^6 \equiv 1 \pmod 9;$$
$$\Rightarrow ord_9 2 = \phi(9).$$

Suy ra 2 là nghiệm nguyên thủy mod 9. Ta có

$$2^1 \equiv 2 \pmod 9, 2^2 \equiv 4 \pmod 9, 2^3 \equiv 8 \pmod 9,$$
$$2^4 \equiv 7 \pmod 9, 2^5 \equiv 5 \pmod 9, 2^6 \equiv 1 \pmod 9.$$

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

6.11 Định lý. Nếu $ord_n a = t$ và u là số nguyên dương thì

$$ord_n(a^u) = \frac{t}{(t,u)}.$$

Chứng minh.

$$(a^u)^{\frac{t}{(t,u)}} = (a^t)^{\frac{u}{(t,u)}} \equiv 1 \pmod n \Rightarrow ord_n(a^u) \Big| \frac{t}{(t,u)}.$$

$$(a^u)^k = a^{uk} \equiv 1 \pmod n \Rightarrow t \mid (uk) \Rightarrow \frac{t}{(t,u)} \Big| \left(k \frac{u}{(t,u)}\right)$$

$$\left(\frac{t}{(t,u)}, \frac{u}{(t,u)}\right) = 1 \Rightarrow \frac{t}{(t,u)} \Big| k$$

do đó $ord_n(a^u) = \frac{t}{(t,u)}$.

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

6.12 Hệ quả. Cho m là số nguyên lớn hơn 1 và r là nghiệm nguyên thủy mod n. Khi đó

$$ord_n r^u = \phi(n) \Leftrightarrow (u, \phi(n)) = 1.$$

Chứng minh. ($\rightarrow$) Giả sử $ord_n r^u = \phi(n)$ Theo 6.11

$$ord_n(a^u) = \frac{ord_n a}{(u, ord_n a)} = \frac{\phi(n)}{(u, ord_n a)}.$$
$$\Rightarrow (u, ord_n a) = 1.$$

($\leftarrow$) $(r^u)^{\phi(n)} = (r^{\phi(n)})^u \equiv 1 \pmod n$.

$(r^u)^k = r^{uk} \equiv 1 \pmod n \Rightarrow (ord_n r = \phi(n)) \mid uk$.

$(u, \phi(n)) = 1 \Rightarrow \phi(n) \mid k \Rightarrow ord_n(r^u) = \phi(n)$.

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

6.13 Định lý. Nếu số nguyên dương n có 1 nghiệm nguyên thủy thì m có tổng cộng $\phi(\phi(n))$ nghiệm nguyên thủy không đồng dư với nhau.

Chứng minh. Giả sử r là 1 nghiệm nguyên thủy của m, theo Mệnh đề 6.9 $\{r^1, r^2, \dots, r^{\phi(n)}\}$ là hệ reduced rescidue mod n. Theo Hệ quả 6.12, r^u là nghiệm nguyên thủy mod n khi và chỉ khi $(u, \phi(n))=1$. Do đó có chính xác $\phi(\phi(n))$ nghiệm nguyên thủy mod n không đồng dư với nhau.

6.14 Thí dụ. Với $m = 11$. Đơn thuần tính toán 2 là nghiệm nguyên thủy mod 11. Do đó có $\phi(\phi(11)) = \phi(10) = 4$ đó là các số 1, 3, 7, 9. Các nghiệm nguyên thủy mod 11 là 2, 2^3, 2^7, 2^9 hay 2, 8, 7, 6.

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

§7. Thặng dư bình phương.

7.1 Định nghĩa. Cho n là số nguyên dương, số nguyên a được gọi là một *thặng dư bình phương* mod n nếu $(a, n) = 1$ và phương trình đồng dư $x^2 \equiv a(mod\ n)$ có nghiệm, nói cách khác phương trình $x^2 = \bar{a}$ trong $\mathbb{Z}_n$ có nghiệm.

7.2 Bổ đề. Cho p là số nguyên tố lẻ và a là số nguyên không chia hết cho p. Khi đó, phương trình $x^2 = \bar{a}$ trong $\mathbb{Z}_n$ hoặc là vô nghiệm hoặc có đúng 2 nghiệm phân biệt.

Chứng minh. Theo Định lý Lagrange phương trình $x^2 = \bar{a}$ trong $\mathbb{Z}_p$ có không quá 2 nghiệm. Nếu $\bar{u}$ là 1 nghiệm của phương trình thì $-\bar{u}$ cũng là nghiệm. Nếu $\bar{u} = -\bar{u}$ thì $\overline{2u} = \bar{0}$, từ $(2, p) = 1$ ta có $\bar{u} = \bar{0}$ dẫn đến $\bar{a} = \bar{0}$ kéo theo $p|a$ (vô lý). Vậy $\bar{u}$ và $-\bar{u}$ là phân biệt.

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

7.3 Định lý. Nếu p là số nguyên tố lẻ thì tập $\{1, 2, \dots, p-1\}$ có đúng $(p-1)/2$ phần tử thặng dư bình phương mod p.

Chứng minh. Xét trong $\mathbb{Z}_p$. Từ Bổ đề 7.2 $\forall i = 1, \dots, (p-1)/2$, phương trình $x^2 = \overline{(i)^2}$ có 2 nghiệm là $\bar{i}$ và $\overline{p-i}$. Suy ra

$$\left\{(\bar{1})^2, (\bar{2})^2, \dots, \left(\frac{p-1}{2}\right)^2\right\} = \left\{\left(\frac{p-1}{2}+1\right)^2, \left(\frac{p-1}{2}+1\right)^2, \dots, (p-1)^2\right\}$$

Nếu $i \neq j, 1 \le i, j \le (p-1)/2, (\bar{i})^2 = (\bar{j})^2$ thì

$$(\bar{i}+\bar{j})(\bar{i}-\bar{j}) = \bar{0} \Rightarrow \bar{i} = \bar{j} \vee \bar{i} = \overline{p-j}.$$

cả 2 kết quả này đều vô lý. Suy ra

$$\left\{(\bar{1})^2, (\bar{2})^2, \dots, \left(\frac{p-1}{2}\right)^2\right\}$$

có $(p-1)/2$ phần tử phân biệt.

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

7.4 Thí dụ. Tìm tất cả các thặng dư bình phương mod 11, trong tập hợp $\{1,2, \dots, 11\}$.

Giải. $(p-1)/2 = 5$. $12 \equiv 1(mod\ 11)$, $1^2 \equiv 1(mod\ 11)$,
$2^2 \equiv 4(mod\ 11)$, $3^2 \equiv 9(mod\ 11)$, $4^2 \equiv 5(mod\ 11)$,
$5^2 \equiv 3(mod\ 11)$.
Các phần tử thặng dư mod 11 cần tìm là $\{1, 4, 9, 5, 3\}$

Thực hành. Tìm tất cả các thặng dư bình phương mod 19, trong tập hợp $\{1,2, \dots, 19\}$.

Đáp án. $\{1, 4, 9, 16, 6, 17, 11, 7, 5\}$.

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

7.5. Kí hiệu Legendre. Cho p là số nguyên tố lẻ và a là số nguyên không chia hết cho p. Kí hiệu $\left[\frac{a}{p}\right]$ được định nghĩa như sau.

$$\left[\frac{a}{p}\right] = \begin{cases} 1, & \text{nếu } a \text{ là thặng dư bình phương của } p \\ -1, & \text{nếu } a \text{ không là thặng dư bình phương của } p \end{cases}$$

7.6 Thí dụ. Theo Thí dụ 7.5, $\{1, 3, 4, 5, 9\}$ là các thặng dư bình phương. Do đó

$$\left[\frac{1}{11}\right] = \left[\frac{3}{11}\right] = \left[\frac{4}{11}\right] = \left[\frac{5}{11}\right] = \left[\frac{9}{11}\right] = 1$$

$$\left[\frac{2}{11}\right] = \left[\frac{6}{11}\right] = \left[\frac{7}{11}\right] = \left[\frac{8}{11}\right] = \left[\frac{10}{11}\right] = -1$$

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

7.7 Định lý(tiêu chuẩn Euler). Cho p là số nguyên tố lẻ và a là số nguyên không chia hết cho p. Khi đó

$$\left[\frac{a}{p}\right] \equiv a^{\frac{p-1}{2}} (\text{mod } p).$$

Chứng minh. Xét $\left[\frac{a}{p}\right] = 1$, khi đó tồn tại u sao cho $a \equiv u^2 (\text{mod } p)$.
Áp dụng Định lý Fermat nhỏ, $(a)^{((p-1/2))} = u^{p-1} \equiv 1 (\text{mod } p)$.

Xét $\left[\frac{a}{p}\right] = -1$, phương trình $x^2 = \bar{a}(\mathbb{Z}_p)$ vô nghiệm. Suy ra với mọi $1 \le i \le p-1$ đặt $\bar{j} = (\bar{i})^{-1}\bar{a}(1 \le j \le p-1)$ khi đó $\bar{j}$ là duy nhất và $\bar{i}\,\bar{j} = \bar{a}$. Phân các số $1, 2, \dots, p-1$ thành $((p-1)/2)$ cặp số u_t, v_t $(t = 1, 2, \dots, ((p-1)/2))$ sao cho $\bar{u}_t \bar{v}_t = \bar{a}$. Nhân tất cả các cặp số này lại, ta nhận được $(p-1)! \equiv a^{(p-1/2)} (\text{mod } p)$. Theo định lý Wilson

$$-1 \equiv (p-1)! (\text{mod } p) \equiv a^{(p-1/2)} (\text{mod } p).$$

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

7.8 Định lý. Cho p là số nguyên tố lẻ, a và b là các số nguyên không chia hết cho p. Khi đó.

a) Nếu $a \equiv b(mod\ p)$ thì $\left[\frac{a}{p}\right] = \left[\frac{b}{p}\right]$.

b) $\left[\frac{a}{p}\right]\left[\frac{b}{p}\right] = \left[\frac{ab}{p}\right]$

c) $\left[\frac{a^2}{p}\right] = 1$.

Chứng minh.

a) Nếu $a \equiv b(mod\ p)$ thì phương trình $x^2 \equiv a(mod\ p)$ có nghiệm khi và chỉ khi phương trình $x^2 \equiv b(mod\ p)$ có nghiệm Do đó

$$\left[\frac{a}{p}\right] = \left[\frac{b}{p}\right].$$

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

b) Dùng tiêu chuẩn Euler

$$\left[\frac{a}{p}\right]\left[\frac{b}{p}\right] \equiv a^{(p-1)/2}b^{(p-1)/2} (\text{mod } p) \equiv (ab)^{(p-1)/2} (\text{mod } p) \equiv \left[\frac{ab}{p}\right] (\text{mod } p) \Rightarrow \left[\frac{a}{p}\right]\left[\frac{b}{p}\right] = \left[\frac{ab}{p}\right].$$

c) $\left[\frac{a^2}{p}\right] = \left[\frac{a}{p}\right]^2 = (\pm 1)^2 = 1.$

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

7.9 Định lý. Nếu p là số nguyên tố lẻ thì

$$\left[\frac{-1}{p}\right] = \begin{cases} 1, khi\ p \equiv 1 (\text{mod } 4)\ (p = 4k+1) \\ -1, khi\ p \equiv -1 (\text{mod } 4)\ (p = 4k+3) \end{cases}.$$

Chứng minh. Theo tiêu chuẩn Euler.

$$\left[\frac{-1}{p}\right] = (-1)^{(p-1)/2} = (-1)^{(2k+u)}$$

$$p \equiv 1 (\text{mod } p) \Rightarrow u = 0 \Rightarrow \left[\frac{-1}{p}\right] = 1.$$

$$p \equiv -1 (\text{mod } p) \Rightarrow u = 1 \Rightarrow \left[\frac{-1}{p}\right] = -1.$$

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

7.10 Bổ đề Gauss. Cho p là số nguyên tố lẻ và $(a, p) = 1$. Nếu t là số các thặng dư dương bé nhất của các số $a, 2a, \ldots, ((p-1)/2)a$ lớn hơn $p/2$ thì $\left[\frac{a}{p}\right] = (-1)^t$.

Chứng minh. Gọi $A = \{s_1, s_2, \ldots, s_{(p-1)/2}\}$ là các thặng dư dương nhỏ nhất của tập $\{a, 2a, \ldots, ((p-1)/2)a\}$, do $(a, p) = 1$ nên $\bar{a}$ khả nghịch trong $\mathbb{Z}_p$ vì vậy tập A có đúng $(p-1)/2$ phần tử. Đặt

$$A_1 = \{p - s \in A | s \in A, s > p/2\}, A_2 = \{s \in A | s < p/2\}; |A_1| = t.$$

Nếu $A_1 \cap A_2 \neq \emptyset$ thì $\exists si, sj; p > s_i > p/2; sj < p/2$ và $p - s_i = s_j$ suy ra $p = s_i + s_j$.

Mặt khác, trong $\mathbb{Z}_p$ tồn tại $1 \le n, m \le (p-1)/2$ sao cho

$$\overline{s_i} = \overline{ma}, \overline{s_j} = \overline{na} \Rightarrow \overline{0} = \overline{p} = \overline{ma} + \overline{na} = (\overline{m} + \overline{n})\overline{a} \Rightarrow \overline{0} = \overline{m+n}.$$

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

Điều này mâu thuẫn với $1 \le n, m \le (p-1)/2$ suy ra $A_1 \cap A_2 = \emptyset$. Do đó

$$A_1 \cup A_2 = \{1, 2, \ldots, (p-1)/2\}.$$

Vậy ta có

$$\overline{\left(\frac{p-1}{2}\right)!} = \overline{\left(\prod_{u \in A_1} u\right)\left(\prod_{v \in A_2} v\right)} = \overline{(-1)^t s_1 s_2 \ldots s_{(p-1)/2}} = \overline{(-1)^t a^{(p-1)/2}\left(\frac{p-1}{2}\right)!}$$

$$\Rightarrow \overline{(-1)^t} = \overline{a^{(p-1)/2}} \xrightarrow{Euler} \overline{\left[\frac{a}{p}\right]} = \overline{a^{(p-1)/2}} = \overline{(-1)^t} \Rightarrow \left[\frac{a}{p}\right] = (-1)^t.$$