Mục lục

CHƯƠNG 1

Thuật toán Euclid và đẳng thức Bezout

Định nghĩa 1.1 (Tính chia hết)**.** Cho a, b là hai số nguyên. Ta nói rằng *a chia hết cho b* nếu tồn tại một số nguyên $c \in \mathbb{Z}$ sao cho $a = bc$.

Mệnh đề 1.2 (Phép chia Euclid)**.** *Cho a là một số nguyên, b là một số nguyên dương. Khi đó tồn tại duy nhất hai số nguyên $q, r \in \mathbb{Z}$ sao cho*

$$a = qb + r$$

và

$$0 \leqslant r < b.$$

Định lý 1.3 (Định lý Bezout)**.** *Cho a và b là hai số nguyên. Khi đó tồn tại hai số nguyên $m, n \in \mathbb{Z}$ sao cho:*

$$\text{UCLN}(a, b) = am + bn.$$

Chứng minh. Đặt $d = \text{UCLN}(a, b)$. Khi đó với mọi $m, n \in \mathbb{Z}$ ta luôn có, d là ước của $am + bn$.

Xét $D := \{e = am + bn \in \mathbb{Z} \,|m, n \in \mathbb{Z}\}$. Theo khẳng định trên ta luôn có d là ước của e với mọi $e \in D$.

Đặt $D_+ = \{e \in D \,|e > 0\}$. Với a, b cho trước ta luôn có thể chọn được $m, n \in \mathbb{Z}$ sao cho $am + bn > 0$, nên D_+ là một tập con khác rỗng của tập các số nguyên dương. Vì thế nó tồn tại phần tử nhỏ nhất. Gọi $d_+ = am_+ + bn_+$ là phần tử nhỏ nhất đó. Khi đó $d|d_+$ (do d_+ cũng là một phần tử của D). Ta sẽ chứng minh rằng $d_+ \,|d$. Điều này tương đương với việc chứng minh rằng

$$d_+ \,|a \,,\; d_+ \,|b$$

Giả sử phản chứng a không chia hết cho d, khi đó áp dụng phép chia Euclid cho a và d ta được $a = qd_+ + r$ với $0 < r < d_+$. Từ đó ta có

$$r = a - qd_+ = (1 - qm_+)a + (-qn_+)b \in D.$$

Ta vừa chỉ ra rằng r là một phần tử nhỏ hơn d và cũng thuộc D_+ (mâu thuẫn với giả thiết d_+ là số nhỏ nhất). Vậy d_+ phải là ước của a. Chứng minh tương tự ta cũng có d_+ cũng phải là ước của b.

Vậy $d = d_+ = am_+ + bn_+$. □

Hệ quả 1.4. *Cho a và b là hai số nguyên. Khi đó a và b nguyên tố cùng nhau khi và chỉ khi tồn tại hai số nguyên m và n thỏa mãn*

$$am + bn = 1.$$

Định nghĩa 1.5 (Đồng dư)**.** Cho $n \in N_+$ là một số nguyên dương. Ta nói

$$a \equiv b \mod n$$

khi và chỉ khi $a - b$ chia hết cho n.

Áp dụng phép chia Euclid cho cặp các số nguyên (a_1, n) và (a_2, n) ta được:

$$a_1 = q_1 n + r_1 \quad 0 \leqslant r_1 < n$$
$$a_2 = q_2 n + r_2 \quad 0 \leqslant r_2 < n.$$

Điều này dẫn đến $a_1 \equiv a_2 \mod n \Leftrightarrow r_1 \equiv r_2 \mod n$. Ta quan tâm đến tập hợp các lớp đồng dư của n $\mathbb{Z}/n\mathbb{Z}$.

- Tập $\mathbb{Z}/n\mathbb{Z}$ có đúng n phần tử.

  Ví dụ 1.6. *Với $n = 5$, ta có $\mathbb{Z}/5\mathbb{Z} = \{[0], [1], [2], [3], [4]\}$.*

- Trên tập $\mathbb{Z}/n\mathbb{Z}$ ta có thể cộng các lớp đồng dư, nhân các lớp đồng dư. Cụ thể:

$$\begin{cases} a_1 \equiv a_2 \mod n \\ b_1 \equiv b_2 \mod n \end{cases} \Rightarrow \begin{cases} a_1 + b_1 \equiv a_2 + b_2 \mod n \\ a_1 b_1 \equiv a_2 b_2 \mod n. \end{cases}$$

Định lý 1.7 (Gauss)**.** *Tập hợp $\mathbb{Z}/n\mathbb{Z}$ cùng với phép toán công và nhân ở trên lập thành một vành giao hoán (có tính chất giống như $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, ...$)*

Định nghĩa 1.8. Cho R là một vành giao hoán (có đơn vị). Một phần tử $a \in R$ được gọi là *nghịch đảo được* nếu tồn tại một phần tử $b \in R$ sao cho $ab = 1$ (tróng đó 1 là phần tử đơn vị của phép toán nhân). Ta kí hiệu R^* là tập hợp các phần tử nghịch đảo được (với phép nhân) của của R.

Ví dụ 1.9.

- *Với $R = \mathbb{R}$, ta có mọi phần tử $a \neq 0$ của $\mathbb{R}$ đều có phần tử nghịch đảo. Do đó $\mathbb{R}^* = \mathbb{R} - \{0\}$.*
- *Với $R = \mathbb{Q}$, ta có mọi phần tử $a \neq 0$ của $\mathbb{Q}$ đều có phần tử nghịch đảo. Do đó $\mathbb{Q}^* = \mathbb{Q} - \{0\}$.*
- *Với $R = \mathbb{Z}$. Giả sử $a \in \mathbb{Z}$ là một phần tử nghịch đảo được, khi đó ta có tồn tại $b \in \mathbb{Z}$ sao cho $ab = 1$. Điều này dẫn đến $a \in \{\pm 1\}$. Vậy $\mathbb{Z}^* = \{\pm 1\}$.*

Một câu hỏi hoàn toàn tự nhiên là vậy thì $(\mathbb{Z}/n\mathbb{Z})^* =$?

Mệnh đề 1.10. *Cho m là một số nguyên, $[m] \in \mathbb{Z}/n\mathbb{Z}$ là lớp đồng dư mod n của m . Khi đó $[m] \in (\mathbb{Z}/n\mathbb{Z})^*$ khi và chỉ khi* $\text{UCLN}(m, n) = 1$.

Chứng minh. Áp dụng định lý Bezout (xem hệ quả 1.4) ta có

$$\begin{aligned} \text{UCLN}(m,n) = 1 &\iff \exists\, a, b \in \mathbb{Z} \,:\, am + bn = 1 \\ &\iff am \equiv 1 \bmod n \\ &\iff [a]\,[m] = [1] \text{ (trong } \mathbb{Z}/n\mathbb{Z}). \end{aligned}$$

Hơn nữa, định lý Bezout còn cho phép ta tìm phần tử nghịch đảo của $m \mod n$ nếu $\text{UCLN}(m, n) = 1$. □

Hệ quả 1.11. *Cho n là một số nguyên dương. Khi đó ta có*

$$(\mathbb{Z}/n\mathbb{Z})^* = \{[m] \text{ lớp các đồng dư mod } n \text{ của } m \in \mathbb{Z}, \text{UCLN}(m, n) = 1\}.$$

Hơn nữa số lượng phần tử của tập hợp này là $\varphi(n)$ (với $\varphi(n)$ là hàm Euler đếm số các số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n).

Trường hợp đặc biệt khi $n = p$ với p là một số nguyên tố ta có m không chia hết cho n kéo theo $\text{UCLN}(m, n) = 1$, nên $[m]$ sẽ thuộc vào $(\mathbb{Z}/n\mathbb{Z})^*$. Do đó $(\mathbb{Z}/p\mathbb{Z})^* = (\mathbb{Z}/p\mathbb{Z}) - \{[0]\}$.Lúc này $\mathbb{Z}/p\mathbb{Z}$ không chỉ là một vành giao hoán mà nó còn là một trường.

Ví dụ 1.12. • $\mathbb{Z}/p\mathbb{Z}$ *là một trường.*

- $\mathbb{R}, \mathbb{Q}$ *là một trường.*
- $\mathbb{Z}$ *không phải là một trường, vì* 2 *không nghịch đảo được trong* $\mathbb{Z}$*.*
- $\mathbb{Z}/6\mathbb{Z}$ *không phải là một trường vì* $[2]$ *không nghịch đảo được trong* $\mathbb{Z}/6\mathbb{Z}$ *(do* $\text{UCLN}(2,6) = 2 \neq 1$*).*

Mệnh đề 1.13. *Ta có* $\mathbb{Z}/n\mathbb{Z}$ *là một trường khi và chỉ khi* n *là một số nguyên tố.*

Định lý 1.14 (Định lý Wilson)**.** *Cho* p *là một số nguyên tố lẻ khi đó ta có:*

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

Chứng minh. Ta có

$$(p-1)! = \prod_{a \in (\mathbb{Z}/p\mathbb{Z})^*} a.$$

Với mọi $a \in (\mathbb{Z}/p\mathbb{Z})^*$ luôn tồn tại duy nhất $b \in \left(\mathbb{Z}_{/p\mathbb{Z}}\right)^*$ sao cho $ab = 1$. Ta chia các lớp đồng dư khả nghịch mod p $\{[1], [2], ... [p-1]\}$ thành từng cặp (a, b) thỏa mãn tính chất $ab = 1$, khi đó chỉ còn lại 2 phần tử lẻ cặp là 1 và -1. Hai phân tử này là nghiệm của phương trình $x^2 = 1$ trong $\mathbb{Z}/p\mathbb{Z}$. Do đó

$$(p-1)! = 1 \left(\prod_{(a,b)} ab \right) .(-1) = -1$$

□

Bổ đề 1.15. *Cho* a, b *là 2 phần tử của* $(\mathbb{Z}/p\mathbb{Z})^*$*. Khi đó* ab *cũng là một phần tử của* $(\mathbb{Z}/p\mathbb{Z})^*$*.*

Chứng minh. Đây là hệ quả trực tiếp của việc $\text{UCLN}(a, p) = \text{UCLN}(b, p) = 1$ thì $\text{UCLN}(ab, p) = 1$. □

Mệnh đề 1.16. *Tập hợp* $(\mathbb{Z}/p\mathbb{Z})^*$ *cùng với phép toán nhân lập thành một nhóm giao hoán.*

Định lý 1.17 (Định lý Fermat nhỏ)**.** *Cho* p *là một số nguyên tố. Khi đó với mọi số nguyên* a *không chia hết cho* p *ta luôn có*

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

Định lý Fermat nhỏ là hệ quả trực tiếp của mệnh đề sau (với $G = (\mathbb{Z}/p\mathbb{Z})^*$ có $p-1$ phần tử)

Mệnh đề 1.18. *Cho G là một nhóm hữu hạn có n phần tử. Khi đó với mọi $g \in G$ ta luôn có $g^n = 1$ (ở đây 1 là phần tử trung hòa của G).*

Chứng minh. Lấy g là một phần tử bất kì trong G. Xét dãy các phần tử $1, g, g^2, g^3, \ldots,$ đều chứa các phần tử của G. Do G chỉ có hữu hạn phần tử nên trong dãy trên sẽ tồn tại ít nhất hai phần tử bằng nhau. Không mất tính tổng quát ta giả sử $g^i = g^j$ với $i > j$. Sử dụng luật giản ước ta có $g^{i-j} = 1$. Ta vừa chứng minh rằng tồn tại một số nguyên dương n sao cho $g^n = 1$. Gọi m là số nhỏ nhất trong các số nguyên dương đó. Khi đó G sẽ chia ra được thành các chu trình có m phần tử

Do đó $|G| = m \times$ số chu trình. Vì thế $g^{|G|} = 1$. □

Một vài ứng dụng của định lý Fermat nhỏ

Bài tập 1.1. Cho p là một số nguyên tố lẻ. Chứng minh rằng tồn tại vố số số nguyên dương n sao cho $2^n - n$ chia hết cho p.

Chỉ dẫn 1. Thực hiện phép chia Euclid n cho $p-1$ ta được

$$n = (p-1)q + r$$

với $0 \leqslant r < p-1$. Áp dụng định lý Fermat nhỏ ta thu được

$$2^n = 2^{(p-1)q+r} \equiv 2^r \mod p.$$

Lấy $r = 0$ đẳng thức trên cho ta $2^n \equiv 1 \mod p$. Giả sử rằng n là số nguyên dương thỏa mãn đề bài, khi đó $2^n - n$ chia hết cho p kéo theo $n \equiv 1 \mod p$.

Vậy ta chỉ cần chứng minh rằng có vô số số nguyên dương thỏa mãn hệ phương trình đồng dư tuyến tính

$$\begin{cases} n \equiv 1 \mod p \\ n \equiv 0 \mod p. \end{cases}$$

Bài toán này hoàn toàn có thể giải được nhờ vào định lý phần dư Trung Hoa.

Nếu chúng ta viết các số hữu tỷ dưới dạng thập phân chúng ta sẽ thấy rằng hoặc chúng có dạng hữu hạn hoặc có dạng vô hạn nhưng có những khối các chữ số được lặp đi lặp lại vô hạn lần. Độ dài của khối (nhỏ nhất) các chữ số được gọi là *chu kỳ* của số hữu tỷ đó.

Ví dụ 1.19. *Số* $\frac{1}{7} = 0,[142857] = 0,142857142857....$ *có chu kỳ là 6.*

Vậy tại sao một số hữu tỉ khi biểu diễn dưới dạng thập phân vô hạn lại có chu kỳ? Ta hoàn toàn có thể giải thích được điều này bằng việc sử dụng đính lý Fermat nhỏ (cho các số hữu tỉ dạng tối giản có mẫu số là một số nguyên tố) và định lý Euler tổng quát hơn cho một số hữu tỉ bất kì.

Định lý 1.20 (Định lý Euler)**.** *Cho n là một số nguyên dương. Khi đó với mọi m thỏa mãn tính chất* $\text{UCLN}(m,n) = 1$*, ta luôn có*

$$m^{\varphi(n)} \equiv 1 \mod n.$$

Chứng minh. Đây là hệ quả trực tiếp của mệnh đề 1.18 với $G = (\mathbb{Z}/n\mathbb{Z})^*$ có $\varphi(n)$ phần tử. □

Với ví dụ phía trên, $\frac{1}{7}$ có chu kỳ là 6 bởi vì 6 là số nguyên dương nhỏ nhất thỏa mãn tính chất $10^k \equiv 1 \mod 7$ (theo định lý Fermat nhỏ ta có $10^6 \equiv 1 \mod 7$). Tổng quát hơn, chu kỳ của số $1/p$ (với p là số nguyên tố khác 2 và 5) là $p-1$. Chu kỳ của số $1/n$ (với n là số nguyên dương lớn hơn 1 và nguyên tố cùng nhau với 10) là $\varphi(n)$.

Ngược lại giả sử x là một số thực có chu kỳ là n thì $(10^n - 1)x$ luôn là một số thập phân hữu hạn, do đó tồn tại m sao cho $10^m(10^n - 1)x$ là một số nguyên. Điều đó dẫn đến x phải là một số hữu tỷ.

Bài tập về Thuật toán Euclid và đẳng thức Bezout

Mệnh đề 1.21 (Thuật toán Euclid)**.** *Cho các số nguyên a và $b > 0$, thực hiện nhiều lần phép chia Euclid ta thu được dãy các phương trình sau :*

$$\begin{aligned}
a &= bq_1 + r_1, && 0 < r_1 < b \\
b &= r_1q_2 + r_2, && 0 < r_2 < r_1 \\
&\dots \\
r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1}, && 0 < r_{n-1} < r_{n-2} \\
r_{n-2} &= r_{n-1}q_n.
\end{aligned}$$

Ước chung lớn nhất $\text{UCLN}(a, b)$ *của a và b là r_{n-1}, phần dư khác không cuối cùng trong dãy các phép chia trên. Hơn thế nữa bằng việc khử $r_{n-2}, \dots, r_2, r_1$ từ các phương trình trên cho phép ta tìm được các số nguyên x, y thỏa mãn* ***đẳng thức Bezout*** $ax + by = \text{UCLN}(a, b)$.

Câu hỏi: Với a và b cho trước thì thuật toán Euclid cần phải thực hiện bao nhiêu bước (được hiểu là bao nhiêu phép chia) để có thể tính được $\text{UCLN}(a, b)$.

Bài tập 1.2. Với mỗi cặp số nguyên dương $a > b > 0$ ta ký hiệu $s(a, b)$ là số bước mà thuật toán Euclid cần dùng để tìm được $\text{UCLN}(a, b)$ (ví dụ trong phát biểu của mệnh đề trên ta có $s(a, b) = n$). Với mỗi số nguyên $a \geqslant 2$, ta định nghĩa độ cao $h(a)$ của a là số nguyên dương lớn nhất trong tập hợp các số $s(a, b)$ khi b chạy trên tập các số nguyên dương nhỏ hơn a. Chứng minh rằng $h(a) = 1$ khi và chỉ khi $a = 2$. Tính $h(a)$ với $2 \leqslant a \leqslant 8$.

Bài tập 1.3. Cho dãy Fibonacci được định nghĩa như sau: $F_1 = F_2 = 1$ và $F_{n+2} = F_n + F_{n+1}$ với mọi $n \geqslant 1$. Chứng minh rằng $h(F_{n+2}) \geqslant n$.

Bài tập 1.4 (Lamé, 1845)**.** Giả sử $a > b > 0$ là hai số nguyên dương thỏa mãn $s(a, b) = n$ và a la số nhỏ nhất thỏa mãn tính chất đó (nghĩa

là, nếu ta có $a' > b' > 0$ thỏa mãn $s(a', b') = n$ khi đó $a' \geqslant a$). Chứng minh rằng $a = F_{n+2}$ và $b = F_{n+1}$.

Bài tập 1.5. Chứng minh rằng $h(F_{n+2}) = n$ và F_{n+2} là số nguyên dương nhỏ nhất có độ cao đó.

Bài tập 1.6. Đặt $\phi = \frac{1+\sqrt{5}}{2}$. Chứng minh rằng $s(a, b) \sim \log_\phi(a\sqrt{5}) - 2$.

Định lý 1.22. *Cho a, b, c là các số nguyên, a và b khác không. Xét phương trình Diophante tuyến tính*

$$ax + by = c.$$

1. *Phương trình trên có nghiệm nguyên khi và chỉ khi $d = \text{UCLN}(a, b)$ là nghiệm của c.*
2. *Nếu (x_0, y_0) là một nghiệm đặc biệt của phương trình thì mọi nghiệm khác của phương trình có dạng*

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

với t là một số nguyên nào đó.

Bài tập 1.7. Giải phương trình nghiệm nguyên

$$3x + 4y + 5z = 6.$$

Với mỗi bộ n số nguyên dương $a_1, a_2 \ldots, a_n$ thỏa mãn $(a_1, \ldots, a_n) = 1$ ta định nghĩa $g(a_1, \ldots, a_n)$ là số nguyên dương N lớn nhất sao cho phương trình

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = N$$

không có nghiệm nguyên không âm. Bài toán xác định $g(a_1, \ldots, a_n)$ được biết đến với cái tên *Frobenius coin problem*.

Bài tập 1.8 (Sylvester, 1884)**.** Cho a, b là hai số nguyên dương, nguyên tố cùng nhau. Khi đó

$$g(a, b) = ab - a - b.$$

Bài tập 1.9. Cho a,b là các số nguyên dương. Chứng minh rằng số nghiệm không âm (x, y, z) của phương trình $ax + by + z = ab$ là

$$\frac{1}{2}[(a + 1)(b + 1) + \text{UCLN}(a, b) + 1].$$

Bài tập 1.10 (24th IMO)**.** Cho a, b, c là ba số nguyên dương đôi một nguyên tố cùng nhau. Chứng minh rằng

$$g(ab, bc, ca) = 2abc - ab - bc - ca.$$

Giả sử rằng phương trình

$$a_1x_1 + \dots a_mx_m = n,$$

với $a_i > 0$ với mọi i chạy từ 1 đến m, có nghiệm không âm và đặt A_n là số các nghiệm không âm $(x_1, \dots, x_m)$ của phương trình.

Bài tập 1.11. 1. Hàm sinh của dãy $(A_n)_{n\geqslant 1}$ là

$$f(x) = \frac{1}{\prod_{i=1}^{m}(1 - x^{a_i})}, \quad |x| < 1,$$

nghĩa là A_n bằng với hệ số của x^n trong khai triển ra chuỗi lũy thừa của f.

2. Đẳng thức sau đây là đúng:

$$A_n = \frac{1}{n!}f^{(n)}(0).$$

Bài tập 1.12. Tìm số n nguyên dương sao cho phương trình sau

$$x + 2y + z = n$$

có đúng 100 nghiệm không âm (x, y, z).

Bài tập 1.13. Cho a, b là hai số nguyên dương phân biệt sao cho $ab(a+b)$ chia hết cho $a^2 + ab + b^2$. Chứng minh rằng $|a - b| > \sqrt[3]{ab}$.

Bài tập 1.14. Chứng minh rằng dãy $1, 11, 111, \dots$ chứa một dãy con vô hạn mà các phần tử của nó đôi một nguyên tố cùng nhau.

Bài tập về Đồng dư, định lý Fermat nhỏ, đặc số Euler

Mệnh đề 1.23 (Định lý Euler)**.** *Cho n là một số nguyên dương. Gọi $\varphi(n)$ là đặc số Euler của n, nghĩa là số các số nhỏ hơn n và nguyên tố cùng nhau với n. Khi đó ta có nếu* $\text{UCLN}(a, n) = 1$ *thì*

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

Bài tập 1.15. 1. Cho p là một số nguyên tố. Chứng minh rằng

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

với mọi số nguyên dương n.

2. Chứng minh rằng $\varphi : \mathbb{Z}_+ \to \mathbb{Z}_+$ là một hàn nhân tính, nghĩa là với mọi số nguyên dương m và n nguyên tố cùng nhau ta luôn có:

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

Từ đó tìm ra công thức tổng quát cho $\varphi(n)$.

Bài tập 1.16. Chứng minh rằng $\varphi(n)$ có dạng lũy thừa của 2 khi và chỉ khi n có dạng $2^k p_1 p_2 \dots p_\ell$ với k và ℓ là một số tự nhiên nào đó và các p_i là có số nguyên tố Fermat (hay p_i là các số nguyên tố có dạng $2^{2^m} + 1$).

(Bài tập trên liên quan đến bài toán cổ điển là chỉ với thước thẳng và compass thì chúng ta có thể dựng được những n giác đều nào. Gauss đã chứng minh rằng nếu n-giác đều dựng được bằng thước thẳng và compass thì $\varphi(n)$ phải có dạng là lũy thừa của 2. Một hệ quả tức thì ta thấy được là ta không thể dựng được 7 giác đều vì $\varphi(7) = 6$ không phải là một lũy thừa của 2).

Bài tập 1.17 (Gauss)**.** Cho n là một số nguyên dương bất kì. Chứng minh rằng

$$\sum_{d \backslash n} \varphi(d) = n.$$

Bài tập 1.18 (Công thức ngược Möbius (Möbius inversion formula))**.** Với mọi số nguyên dương n, hàm Möbius của n: $\mu : \mathbb{Z}_+ \to \mathbb{N}$ được định nghĩa như sau:

$$\mu(n) = \begin{cases} 1 & \text{nếu } n = 1 \\ 0 & \text{nếu n có ước chính phương lớn hơn 1} \\ (-1)^k & \text{nếu n là tích của } k \text{ số nguyên tố phân biệt.} \end{cases}$$

Chứng minh rằng

$$\varphi(n) = \sum_{d \backslash n} \mu(d) \frac{n}{d}.$$

(Hai bài toán trên liên quan đến tính chất của các hàm số học nhân tính. Việc định nghĩa một tích xoắn (**Dirichlet convulution**) giữa hai hàm nhân tính $f * g(n) = \sum_{d\backslash n} f(d)g(\frac{n}{d})$ cũng cho ta một hàm số nhân tính. Điều này cho phép ta có một cấu trúc vành trên tập hợp các hàm số học nhân tính. Vành này được gọi là **vành Dirichlet**.)

Cho n và a là hai số nguyên dương cho trước thỏa mãn tính chất $\text{UCLN}(a, n) = 1$. Gọi S là tập hợp các số nguyên dương thỏa mãn tính chất $a^s \equiv 1 \mod n$. Theo định lý của Euler trên ta thầy tập này có một phần tử là $\varphi(n)$, tức là nó khác rỗng, do đó tập này có phần tử nhỏ nhất. Gọi phần tử nhỏ nhất đấy là cấp của phần tử a modulo n và được ký hiệu là $\text{ord}_n(a)$.

Bài tập 1.19. Chứng minh rằng số nguyên dương x thỏa mãn $a^x \equiv 1 \mod n$ khi và chỉ khi x chia hết cho $\text{ord}_n(a)$.

Bài tập 1.20.
1. Cho p là số nguyên tố lẻ, q và r là các số nguyên tố thỏa mãn tính chất $q^r + 1$ chia hết cho p. Chứng minh rằng hoặc $p - 1$ chia hết cho $2r$ hoặc $q^2 - 1$ chia hết cho p.

2. Tìm tất cả các bộ sắp thứ tự 3 số nguyên tố (p, q, r) thỏa mãn

$$p\backslash q^r + 1,\ q\backslash r^p + 1,\ r\backslash p^q + 1.$$

Bài tập 1.21. Tìm tất cả bộ 3 số nguyên lớn hơn 1 đôi một nguyên tố cùng nhau (a, b, c) thỏa mãn

$$b\backslash 2^a + 1,\ c\backslash 2^b + 1,\ a\backslash 2^c + 1.$$

Bài tập 1.22. Cho $a > 1$ và n là các số nguyên dương cho trước. Chứng minh rằng nếu p là ước nguyên tố của $a^{2^n}+1$ thì $p-1$ chia hết cho 2^{n+1}.

Bài tập 1.23. Cho p là số nguyên tố, và xét dãy $\{a_k\}_{k=0}^{\infty}$ được định nghĩa như sau $a_0 = 0$, $a_1 = 1$ và

$$a_{k+2} = 2a_{k+1} - pa_k$$

với $k \geqslant 0$. Giả sử rằng trong dãy xuất hiện số -1. Hãy tìm tất cả các giá trị của p.

Bài tập 1.24. Cho p là số nguyên tố có dạng $3k+2$ là ước của a^2+ab+b^2 với a, b là hai số nguyên nào đó. Chứng minh rằng a và b chia hết cho p.

Bài tập 1.25 (Bulgaria 1995)**.** Tìm tất cả các cặp số nguyên tố p, q sao cho pq là ước của $(5^p - 2^p)(5^q - 2^q)$.

Bài tập 1.26. Cho n là số nguyên dương lớn hơn 1. Chứng minh rằng n không là ước của $3^n + 1$.

Bài tập 1.27. Xét dãy $\{a_i\}$ được định nghĩa như sau

$$a_n = 2^n + 3^n + 6^n - 1$$

cho mọi số nguyên dương n. Tìm tất cả các số nguyên dương mà nguyên tố cùng nhau với tất cả các phần tử của dãy.

CHƯƠNG 2

Phương trình và hệ phương trình đồng dư

Định lý 2.1 (Định lí phần dư Trung Hoa)**.** *Cho $p, q \in \mathbb{Z}_+$ là hai số nguyên dương nguyên tố cùng nhau. Khi đó với mọi $a, b \in \mathbb{Z}$ luôn tồn tại duy nhất một lớp đồng dư x modulo pq thỏa mãn tính chất*

$$\begin{cases} x \equiv a \bmod p \\ x \equiv b \bmod q. \end{cases}$$

Cách chứng minh thứ nhất. Ta có $\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/q\mathbb{Z}, \mathbb{Z}/pq\mathbb{Z}$ là các vành giao hoán.

Xét ánh xạ

$$\begin{aligned} \psi : \mathbb{Z}/pq\mathbb{Z} &\to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ x &\mapsto (x \mod p, x \mod q). \end{aligned}$$

Giả sử ta có $\psi(x_1) = \psi(x_2)$. Từ định nghĩa của ψ ta có $x_1 - x_2$ phải chia hết cho p và q. Mặt khác ta lại có p và q nguyên tố cùng nhau, nên dẫn đến $x_1 - x_2$ phai chia hết cho pq. Nói một cách khác, ta có $x_1 \equiv x_2 \mod pq$. Vậy ψ là một đơn ánh. Hơn nữa do số lượng phần tử của $\mathbb{Z}/pq\mathbb{Z}$ và của $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ là bằng nhau và cùng bằng pq, nên ψ phải là một song ánh. □

Cách chứng minh thứ hai. **Cách này cho phép xây dựng nghiệm của hệ**

$$\begin{cases} x \equiv a \mod p \\ x \equiv b \mod q. \end{cases}$$

Áp dụng định lý Bezout (xem hệ quả 1.4) ta có do p và q nguyên tố cùng nhau nên tồn tại hai số nguyên m và n thỏa mãn đẳng thức

$$pm + qn = 1.$$

(Ta có thể dùng thuật toán Euclid để có thể tìm được các giá trị của m và n.)

Lấy $x = anq + bmp$, khi đó ta có x chính là nghiệm của hệ phương trình. □

Hệ quả 2.2. *Để giải phương trình đồng dư mod pq, chúng ta chỉ cần giải phương trình đồng dư mod p và mod q, sau đó dùng ánh xạ ngược của ψ để "ghép" nghiệm.*

Ví dụ 2.3.

- *Để giải phương trình đồng dư*

$$x^7 + 1 \equiv 0 \mod 143 = 13 \times 11.$$

Ta đi giải hệ phương trình đồng dư

$$\begin{cases} x^7 + 1 \equiv 0 \mod 13 \\ x^7 + 1 \equiv 0 \mod 11. \end{cases}$$

- *Giả sử $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ với p_i là các số nguyên tố đôi một khác nhau. Khi đó ta có*

$$f(x) \equiv 0 \mod n \Longleftrightarrow \begin{cases} f(x) \equiv 0 \mod p_1^{\alpha_1} \\ \vdots \\ f(x) \equiv 0 \mod p_m^{\alpha_m}. \end{cases}$$

Việc giải phương trình đồng dư mod n quy về việc giải hệ phương trình đồng dư mod $p_1^{\alpha_1}$,..., mod $p_m^{\alpha_m}$

Hệ quả của định lý phần dư Trung Hoa

1. **Tính chỉ số Euler**

Định nghĩa 2.4. Cho n là một số nguyên dương. Chỉ số Euler của n là số phần tử của tập hợp gồm các số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n. Ta ký hiệu chỉ số Euler của n là $\varphi(n)$.

Từ định nghĩa, ta dễ dàng thấy rằng

$$\begin{aligned}\varphi(n) &= |\{m \mod n \,|\, \text{UCLN}(m,n) = 1\}| \\ &= |(\mathbb{Z}/n\mathbb{Z})^*| \\ &= |\{m \in \mathbb{Z}/n\mathbb{Z} \,|\exists\, r : mr = 1\}|\,.\end{aligned}$$

Mệnh đề 2.5. *Hàm $\varphi : \mathbb{Z}_+ \to \mathbb{Z}_+ \quad n \mapsto \varphi(n)$ là một hàm nhân tính, nghĩa là với mọi số nguyên dương p và q nguyên tố cùng nhau ta luôn có:*

$$\varphi(pq) = \varphi(p)\varphi(q).$$

Chứng minh. Xét đẳng cấu vành (xem chứng minh thứ nhất của định lý phần dư Trung Hoa)

$$\psi : \mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

Ta có do p và q nguyên tố cùng nhau nên $mr \equiv 1 \mod pq$ khi và chỉ khi $mr \equiv 1 \mod p$ và $mr \equiv 1 \mod q$. Điều này đãn đến

$$m \in (\mathbb{Z}/pq\mathbb{Z})^* \iff \begin{cases} m \mod p \in (\mathbb{Z}/p\mathbb{Z})^* \\ m \mod q \in (\mathbb{Z}/p\mathbb{Z})^*. \end{cases}$$

Do đó ψ cảm sinh ra một song ánh (đẳng cấu nhóm)

$$(\mathbb{Z}/pq\mathbb{Z})^* \simeq (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^*.$$

Vì vậy số lương phần tử của hai tập hợp ở vế phải và vế trái phải bằng nhau. Nói một cách khác ta có

$$\varphi(pq) = \varphi(p)\varphi(q).$$

□

Mệnh đề trên cho phép chúng ta đưa việc tính chỉ số Euler $\varphi(n)$ về việc tính chỉ số Euler của một lũy thừa của một số nguyên tố

- Với p là một số nguyên tố, $\mathbb{Z}/p\mathbb{Z}$ là một trường, nên $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} - \{0\}$. Do đó $\varphi(p) = p - 1$.

- Vành $\mathbb{Z}/p^2\mathbb{Z}$ không phải là một trường vì phần tử p trong $\mathbb{Z}/p^2\mathbb{Z}$ không có phần tử nghịch đảo. Ta có

$$a \in (\mathbb{Z}/p^2\mathbb{Z})^* \iff a \not\equiv 0 \mod p.$$

  Trong $(\mathbb{Z}/p^2\mathbb{Z})$ có p phần tử chia hết cho p là: $0, p, \ldots, (p-1)p$. Do đó

$$\varphi(p^2) = |(\mathbb{Z}/p^2\mathbb{Z})^*| = p^2 - p = p(p-1).$$

- Bằng quy nạp theo r ta có thể chứng minh rằng

$$\varphi(p^r) = |(\mathbb{Z}/p^r\mathbb{Z})^*| = p^{r-1}(p-1).$$

2. **Tìm hiểu phương trình đồng dư.** Áp dụng định lý phần dư Trung Hoa, việc giải một phương trình đồng dư $f(x) \equiv 0 \mod n$ với $f(x)$ là một đa thức, được quy về việc giải các phương trình đồng dư có dạng $f(x) \equiv 0 \mod p^r$ với p là một ước nguyên tố của n.

   Ví dụ 2.6. • *Giải phương trình* $ax \equiv b \mod 28$ *với* a, b *là các tham số và* x *là ẩn số.*

   Áp dụng định lý phần dư Trung Hoa ta có phương trình đó tương đương với hệ phương trình

$$\begin{cases} ax \equiv b \mod 7 \\ ax \equiv b \mod 4. \end{cases}$$

   Đầu tiên ta giải phương trình mod 7.

   – *Nếu* $a \not\equiv 0 \mod 7$*, khi đó* $a \in (\mathbb{Z}/7\mathbb{Z})^*$*. Do đó tồn tại* m *sao cho* $am \equiv 1 \mod 7$*. Phương trình* $ax \equiv b \mod 7$ *lúc này tương đương với* $x \equiv bm \mod 7$*.*

   – *Nếu* $a \equiv 0 \mod 7$*, lúc này có hai khả năng xảy ra. Hoặc* $b \not\equiv 0 \mod 7$*, lúc này phương trình vô nghiệm; hoặc* $b \equiv 0 \mod 7$*, lúc này* x *có thể lấy giá trị tùy ý.*

   Giải phương trình mod 4

   – *Nếu* $a \not\equiv 0 \mod 2$*, khi đó* a *khả nghịch trong* $\mathbb{Z}/4\mathbb{Z}$*. Hay nói cách khác, tồn tại* $m \mod 4$ *sao cho* $am = 1$*. Điều này dẫn đến phương trình có nghiệm* $x \equiv mb \mod 4$*.*

   – *Nếu* $a \equiv 2 \mod 4$*, đặt* $a = 2a_1$*. Ta có* $a_1 \not\equiv 0 \mod 2$*.*

  - *Nếu b lẻ khi đó phương trình không có nghiệm.*
  - *Nếu b là số chẵn, đặt $b = 2b_1$. Phương trình của chúng ta tương đương với phương trình $a_1 x \equiv b_1 \mod 2$. Lúc này ta thu được 2 nghiệm mod 4.*

- *Nếu $a \equiv 0 \mod 4$, ta có:*
  - *Nếu $b \not\equiv 0 \mod 4$ thì phương trình vô nghiệm.*
  - *Nếu $b \equiv 0 \mod 4$ thì phương trình có 4 nghiệm mod 4.*

Sau khi giải hai phương trình mod 7 và mod 4 ta dùng ánh xạ ngược của đẳng cấu vành ψ để thu được nghiệm mod 28.

- *Giải phương trình $x^2 \equiv 7 \mod 3^2$.*

  Để giải phương trình này đầu tiên ta giải phương trình mod 3 trước. Giả sử x là nghiệm của phương trình ban đầu khi đó nó sẽ phải là nghiệm của phương trình (sau khi lấy modulo 3)

$$x^2 \equiv 1 \mod 3.$$

  Phương trình này có 2 nghiệm $x \equiv \pm 1 \mod 3$.

  - *Giả sử $x \equiv 1 \mod 3$. Đặt $x = 1 + 3y$, khi đó ta có phương trình ban đầu tương đương với*

$$\begin{aligned} 1 + 6y &\equiv 7 \mod 9 \\ 6y &\equiv 6 \mod 9 \\ 2y &\equiv 2 \mod 3 \\ y &\equiv 1 \mod 3. \end{aligned}$$

    Vậy phương trình ban đầu có nghiệm là $x \equiv 1 + 3.1 \equiv 4 \mod 9$.

  - *Ta làm tương tự cho trường hợp $x \equiv -1 \mod 3$.*

- *Giải phương trình $x^2 \equiv 7 \mod 3^3$.*

  Ta làm giống như giải phương trình bên trên. Đầu tiên giải phương trình mod 3. Ta thu được $x \equiv \pm 1 \mod 3$.

  Giả sử $x \equiv 1 \mod 3$ ta tiếp tục giải tìm nghiệm của phương trình $x^2 \equiv 7 \mod 3^2$. Theo trên ta có $x \equiv 1 + 3 \mod 3^2$.

Đặt $x = 4 + 9y$ khi đó ta có

$$\begin{aligned}(4+9y)^2 &\equiv 7 \mod 3^3\\ 16 + 72y + 81y^2 &\equiv 7 \mod 3^3\\ 9.8y &\equiv -9 \mod 9.3\\ 8y &\equiv -1 \mod 3\\ y &\equiv 1 \mod 3.\end{aligned}$$

Điều này dẫn đến nghiệm của phương trình cần giải là

$$x \equiv 1 + 3 + 3^2 \equiv 13 \mod 3^3.$$

(Cách tìm nghiệm của phương trình đồng dư mod p^k như trong ví dụ trên là cách tìm nghiệm bằng tiệm cận tuyến tính, cách tìm nghiệm này khá giống việc tìm nghiệm thực của một hàm số bằng phương pháp Newton. Ta sẽ bàn kĩ hơn vấn đề này ở các phần sau.)

Về cơ bản, nếu ta có thể giải được phương trình mod p thì cũng có thể giải được phương trình mod p^r. Do đó ta cần phải hiểu cách làm thế nào tìm được nghiệm của một phương trình đồng dư mod p trên trường $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

(a) **Phương trình bậc nhất:** $ax \equiv b \mod p$.

- Nếu $a \equiv 0 \mod p$, khi đó phương trình vô nghiệm nếu $b \not\equiv 0 \mod p$ và có đúng p nghiệm phân biệt nếu $b \equiv 0 \mod p$.
- Nếu $a \not\equiv 0 \mod p$, thì $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Do đó tồn tại m sao cho $am = 1$. Lúc này phương trình có nghiệm dua nhất $x \equiv bm \mod p$. (Ta có thể dùng thuật toán Euclid để tìm m.)

(b) **Phương trình bậc hai**: $x^2 \equiv a \mod p$.

Định lý 2.7. *Cho p là một số nguyên tố lẻ.*

- *Giả sử phương trình $x^2 \equiv a \mod p$ có nghiệm thì khi đó nó có 2 nghiệm phân biệt.*
- *Phương trình $x^2 \equiv a \mod p$ có đúng $\frac{p-1}{2}$ nghiệm phân biệt.*

Chứng minh. Tập hợp các phần tử nghịch đảo được $\mathbb{F}_p^* := (\mathbb{Z}/p\mathbb{Z})^*$ của $\mathbb{F}_p$ cùng với phép toán nhân (modulo p) lập thành một nhóm giao hoán.

Ta xét ánh xạ chính phương sau:

$$\begin{aligned} \iota : \mathbb{F}_p^* &\to \mathbb{F}_p^* \\ x &\mapsto x^2. \end{aligned}$$

Đây là một đồng cấu nhóm (nói cách khác ánh xạ này tương thich với phép nhân). Ảnh của ι làm một nhóm con của nhóm $\mathbb{F}_p^*$.

Xét $\ker \iota := \{x \in \mathbb{F}_p^*, x^2 = 1\}$. Tập này có 2 phần tử phân biệt là $\{\pm 1\}$.

Nhận xét, nếu $\iota(x) = \iota(y)$, khi đó do tính tương thích với phép nhân ta có $\iota(x.y^{-1}) = \iota(x).\iota(y)^{-1} = 1$, hay $x.y^{-1} \in \ker \iota$. Điều này chứng minh rằng nếu phương trình $x^2 = a \mod p$ có nghiệm x thì nó có đúng 2 nghiệm là x và $-x$.

Hơn nữa ta đó ta cũng suy ra rằng số phần tử của tập ảnh của ι là

$$|\mathrm{Im}(\iota)| = \frac{p-1}{2}.$$

Điều này dẫn đến khẳng định thứ hai của định lý. □

Việc tìm hiểu phương trình $x^2 \equiv a \mod p$ có nghiệm hay không có nghiệm với a cho trước nào là một bài toán quan trọng. Nó được quy về việc tính giá trị của ký hiệu Legendre $\left(\frac{a}{p}\right)$ sẽ được đề cập trong bài giảng sau.

Bài tập về Phương trình, hệ phương trình đồng dư

Cho $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ là một đa thức hệ số nguyên (các a_i là các số nguyên). Ta nói một số nguyên u là **nghiệm** của phương trình đồng dư $f(x) \equiv 0 \mod m$ nếu $f(u) \equiv 0 \mod m$. Ta có nếu $v \equiv u \mod m$ thì v cũng là nghiệm đồng dư của phương trình trên, do đó khi ta nói $x \equiv u \mod m$ là nghiệm của phương trình $f(x) \equiv u \mod m$, nghĩa là tất cả các số nguyên đồng dư u modulo m thỏa mãn phương trình $f(x) \equiv 0 \mod m$.

Giả sử $m = \prod_i p_i^{\alpha_i}$. Áp dụng định lý thặng dư trung hoa cho phép ta đưa việc giải phương trình $f(x) \equiv 0 \mod m$ và việc giải hệ các phương trình $f_x \equiv 0 \mod p_i^{\alpha_i}$ và ngược lại. Một trong những điều kiện quan trọng để có thể sử dụng được định lý thặng dư trung hoa là $\text{UCLN}(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ với mọi $i \neq j$. Một câu hỏi hoàn toàn tự nhiên đặt ra là nếu tính chất nguyên tố cùng nhau không còn đúng nữa thì liệu ta vẫn có thể giải được nữa hay không. Cụ thể là liệu có tìm được một số nguyên x sao cho $x \equiv a_i \mod n_i$ với các a_i và n_i cho trước hay không (chú ý ở đây ta không yêu cầu các n_i đôi một nguyên tố cùng nhau).

Bài tập 2.1 (Mở rộng của định lý thặng dư trung hoa)**.** Cho $n_1, \ldots, n_k$ là các số nguyên dương, và $a_1, \ldots, a_k$ là các số nguyên. Khi đó hệ phương trình

$$\begin{cases} x \equiv a_1 \mod n_1 \\ \cdots \\ x \equiv a_k \mod n_k \end{cases}$$

có nghiệm khi và chỉ khi $\text{UCLN}(n_i, n_j)$ là ước của $a_i - a_j$ với mọi $i \neq j$. Hơn nữa, nếu điều kiện này được thỏa mãn thì hệ phương trinh có nghiệm duy nhất $\mod \text{lcm}(n_1, \ldots, n_k)$ (ở đây lcm là ký hiệu của **bội chung nhỏ nhất**).

Ta thấy rằng nhờ vào việc sử dụng định lý thặng dư trung hoa, việc giải phương trình đồng dư modulo một số nguyên dương khác 0 bất kì được đưa về việc giải phương trình đồng dư modulo một lũy thừa của số nguyên tố p nào đó. Trong trường hợp tổng quát chúng ta không có cách giải phương trình $f(x) \equiv 0 \mod p$, tuy nhiên giả sử rằng ta tìm được nghiệm của phương trình $f(x) \equiv 0 \mod p$ thì ta có thể viết được công thức nghiệm cho phương trình $f(x) \equiv 0 \mod p^e$ với $e \geqslant 1$.

Bài tập 2.2 (Bổ đề Hensel)**.** Cho $f(x)$ là một đa thức với hệ số nguyên, và m,k là 2 số nguyên dương thỏa mãn $m \leqslant k$. Nếu r là một số nguyên thỏa mãn

$$f(r) \equiv 0 \mod p^k \text{ và } f'(r) \not\equiv 0 \mod p$$

khi đó luôn tồn tại một số nguyên s sao cho

$$f(s) \equiv 0 \mod p^{k+m} \text{ và } r \equiv s \mod p^k.$$

Hơn nữa s là duy nhất modulo p^{k+m} và có thể được tính dựa vào công thức sau

$$s = r - f(r).a$$

trong đó a là số nguyên thỏa mãn tính chất

$$a.f'(r) \equiv 1 \mod p^m.$$

Việc xây dựng nghiệm như trên khá gần với **phương pháp Newton** được dùng trong giải tích để tìm nghiệm thực của phương trình $f(x) = 0$ (với f là một hàm khả vi).

Bài tập 2.3 (Phương pháp Newton)**.** Giả sử rằng dãy sau được định nghĩa và hội tụ $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_{n+1})}$. Khi đó $x = \lim_{n\to\infty} x_n$ là nghiệm của $f(x) = 0$.

Trong phương pháp Newton, sự hội tụ của dãy x_n cho thấy rằng các x_i, x_j ngày càng gần nhau khi i và j lớn, nghĩa là khoảng cách giữa chúng càng ngày càng thu gọn lại. Đối với trường hợp modulo p của chúng ta, cần phải định nghĩa lại khái niệm gần nhau, việc này đưa đến một hệ thống số mới được gọi là các số p-adics.

Bài tập 2.4 (Phương trình đồng dư bậc nhất)**.** Nếu $d = \text{UCLN}(a, n)$, khi đó phương trình $ax \equiv b \mod n$ co nghiệm khi và chỉ khi d là ước của

b. Hơn nữa nếu d là ước của b và x_0 là nghiệm nào đó của phương trình thì nghiệm tổng quát của phương trình có dạng

$$x = x_0 + \frac{nt}{d}$$

với $t \in \mathbb{Z}$.

Bài tập 2.5 (Phương trình đồng dư bậc 2)**.** Cho p là một số nguyên tố lẻ và $f(x) = ax^2+bx+c$ với UCLN$(a, p) = 1$. Chứng minh rằng u là nghiệm của phương trình $f(x) \equiv 0 \mod p$ khi và chỉ khi $2au + b \equiv v \mod p$ với v là nghiệm của phương trình $v^2 \equiv b^2 - 4ac \mod p$. Hơn nữa với mỗi nghiệm v chỉ có duy nhất một nghiệm $u \mod p$ thỏa mãn $2au + b \equiv v \mod p$.

Theo bài tập trên ta thấy việc giải phương trình đồng dư bậc 2 được đưa về việc giải phương trình $x^2 \equiv m \mod p$ với p là số nguyên tố lẻ. Phương trình này hoặc có 2 nghiệm phân biệt hoặc vô nghiệm. Trong trường hợp a và p tổng quát chúng ta không có công thức nghiệm phụ thuộc vào a và p cho phương trình. Điều ta có thể làm đó là kiểm tra xem với m, p cho trước thì phương trình có nghiệm hay không mà thôi. Để làm điều này chúng ta sử dụng kí hiệu Legendre.

Định lý 2.8. *Cho p là số nguyên tố lẻ và a và b là cá số nguyên nguyên tố cùng nhau với p. Khi đó*

- $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$,
- $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$,
- $a \equiv b \mod p$ *kéo theo* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,
- $\left(\frac{a^2}{p}\right) = 1$, $\left(\frac{a^2b}{p}\right) = \left(\frac{b}{p}\right)$, $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

Bài tập 2.6 (Bổ đề Gauss)**.** Cho p là số nguyên tố lẻ và UCLN$(a, p) = 1$. Xét phần dư của các số $a, 2a, \ldots, \frac{(p-1)}{2}a$ khi chia cho p. Gọi n là số các phần dư lớn hơn $p/2$, khi đó $\left(\frac{a}{p}\right) = (-1)^n$.

Bài tập 2.7. Cho p là số nguyên tố lẻ và UCLN$(a, 2p) = 1$, khi đó $\left(\frac{a}{p}\right) = (-1)^t$ với $t = \sum_{j=1}^{(p-1)/2} \left[\frac{ja}{p}\right]$ và $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$. Ở đây $[x]$ là phần nguyên của số x.

Định lý 2.9 (Luật thuận nghịch chính phương)**.** *Cho p và q là 2 số nguyên tố lẻ phân biệt. Khi đó ta có*

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

Bài tập 2.8. Cho p là số nguyên tố, chứng minh rằng phương trình $x^2 - 3y^2 = p$ không có nghiệm nếu $p \not\equiv 1 \mod 12$.

Bài tập 2.9. Cho p,q là 2 số nguyên tố có dạng $4k + 3$. Chứng minh rằng phương trình $x^2 - py^2 = q$ không có nghiệm nguyên.

Bài tập 2.10. Chứng minh rằng phương trình $x^2 - 17y^2 = 12$ không có nghiệm nguyên.

CHƯƠNG 3

Các luật thuận nghịch

3.1 Thặng dư chính phương

Cho p là một số nguyên tố lẻ và a là một lớp đồng dư khả nghịch (hay nói cách khác UCLN$(a,p)=1$). Một câu hỏi hoàn toàn tự nhiên là liệu có tồn tại $x \mod p$ là nghiệm của phương trình $x^2 \equiv a \mod p$ hay không?

Trong bài giảng trước, bằng việc xét đồng cấu nhóm

$$\begin{aligned} \iota : \mathbb{F}_p^* &\to \mathbb{F}_p^* \\ x &\mapsto x^2. \end{aligned}$$

ta thu được $|\mathrm{Im}(\iota)| = \frac{p-1}{2}$. Hay nói một cách khác, có đúng $\frac{p-1}{2}$ lớp thặng dư chính phương (các lớp thặng dư mà phương trình trên có nghiệm) và $\frac{p-1}{2}$ lớp thặng dư không chính phương.

Định nghĩa 3.1 (Kí hiệu Legendre)**.** Cho p là một số nguyên tố lẻ, a là một số nguyên thỏa mãn tính chất UCLN$(a,p)=1$. Khi đó kí hiệu Legendre $\left(\frac{a}{p}\right)$ được định nghĩa như sau:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{nếu } a \text{ là một thặng dư chính phương} \\ -1 & \text{nếu } a \text{ không là một thặng dư chính phương} \end{cases}$$

Mệnh đề 3.2. *Cho p là một số nguyên tố lẻ và a là một số nguyên thỏa mãn tính chất* UCLN$(a,p)=1$*. Khi đó ta có:*

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

Chứng minh.

- Nếu a là một thặng dư chính phương, thì khi đó tồn tại $x \in \mathbb{F}_p^*$ sao cho $a \equiv x^2 \mod p$. Lấy lũy thừa $\frac{p-1}{2}$ cả hai vế của đẳng thức ta có

$$a^{\frac{p-1}{2}} \equiv x^{\frac{p-1}{2}} \equiv 1 \mod p.$$

  Đẳng thức cuối là hệ quả trực tiếp của định lý Fermat nhỏ.

- Nếu a không là một thặng dư chính phương, ta sẽ đi chứng minh rằng $a^{\frac{p-1}{2}} \not\equiv 1 \mod p$. (Theo định lý Fermat nhỏ ta có $a^{p-1} \equiv 1 \mod p$, nên điều này tương đương với $a^{\frac{p-1}{2}} \equiv -1 \mod p$.)

  Ta có nhận xét rằng $x^{\frac{p-1}{2}} - 1$ là một đa thức bậc $\frac{p-1}{2}$ với hệ số trên trường $\mathbb{F}_p$. Đa thức này đã có $\frac{p-1}{2}$ nghiệm phân biệt là các lớp thặng dư chính phương trong $\mathbb{F}_p^*$. Do đó điều phải chứng minh là hệ quả trực tiếp của Hệ quả 3.4 dưới đây.

□

Định lý 3.3 (Định lý Bezout)**.** *Cho $P(X) \in \mathbb{F}_p[X]$. Khi đó $a \in \mathbb{F}_p$ là nghiệm của đa thức P khi và chỉ khi tồn tại một đa thức $Q(X) \in \mathbb{F}_p[X]$ sao cho*

$$P(X) = (X - a).Q(X).$$

Chứng minh. Áp dụng thuật toán chia Euclid cho đa thức $P(X)$ và $X - a$, khi đó ta có tồn tại duy nhất một đa thức $Q(X) \in \mathbb{F}_p[X]$ và một hằng số $c \in \mathbb{F}_p$ (do bậc của đa thức $X - a$ là 1) sao cho

$$P(X) = (X - a).Q(X) + c.$$

- Nếu a là nghiệm của P thay $X = a$ vào phương trình trên ta thu được $c = 0$.

- Nếu $c = 0$, khi đó thay $X = a$ vào phương trình trên ta thu được $P(a) = 0$. Hay nói cách khác a là nghiệm của đa thức $P(X)$.

□

Hệ quả 3.4. *Cho $P(X) \in \mathbb{F}_p[X]$ là một đa thức có bậc là n. Khi đó $P(X)$ có không quá n nghiệm (tính cả bội) trong $\mathbb{F}_p$.*

Chứng minh. Gọi $\lambda_1, \ldots, \lambda_m$ là tất cả các nghiệm của $P(X)$ trong $\mathbb{F}_p$ khi đó áp dụng định lý Bezout ta có

$$P(X) = \prod_{i=1}^{m}(X - \lambda_i)Q(X).$$

Bậc của đa thức bên vế trái là n và của đa thức bên vế phải lớn hơn hoặc bằng m. Do đó $n \geqslant m$. □

Bổ đề 3.5 (Bổ đề Gauss)**.** *Cho p là một số nguyên tố lẻ và a là một số nguyên thỏa mãn tính chất* $\mathrm{UCLN}(a, p) = 1$*. Ta đem chia các lớp đồng dư nghịch đảo được modulo p thành 2 phần $\{1, 2, \ldots, \frac{p-1}{2}\} \sqcup \{\frac{p-1}{2}, \ldots, p-1\}$, rồi sau đó lấy các phần tử của phần đầu tiên nhân thêm với a. Với mỗi $j \in \{1, \ldots, \frac{p-1}{2}\}$, sử dụng phép chia Euclid cho ja và p ta thu được*

$$ja = \begin{cases} \left\lfloor \frac{ja}{p} \right\rfloor p + r_j & \text{nếu } r_j > \frac{p}{2} \\ \left\lfloor \frac{ja}{p} \right\rfloor p + s_j & \text{nếu } s_j < \frac{p}{2}. \end{cases}$$

Đặt $n = \left|\{j | r_j > \frac{p}{2}\}\right|$. Khi đó ta có

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

Chứng minh.

- Với mọi $i \neq j \in \{1, \ldots, \frac{p-1}{2}\}$ ta luôn có $r_i \neq r_j$. Thật vậy giả sử phản chứng $r_i = r_j$ khi đó từ định nghĩa của r_j ta có

  $$r_i - r_j \equiv (i - j)a \mod p.$$

  Điều này dẫn đến $i - j \equiv 0 \mod p$ (không thể xảy ra do $1 \leqslant i, j \leqslant \frac{p-1}{2}$ và $i \neq j$).

- Với mọi $i \neq j \in \{1, \ldots, \frac{p-1}{2}\}$ ta luôn có $s_i \neq s_j$. Điều này chứng minh tương tự như trên.

- Với mọi $i \neq j \in \{1, \ldots, \frac{p-1}{2}\}$ ta luôn có $p - r_i \neq s_j$. Thật vậy giả sử phản chứng $p - r_i = s_j$ khi đó từ định nghĩa của r_i và s_j ta có

  $$r_i + s_j \equiv (i + j)a \mod p.$$

  Điều này dẫn đến $i + j \equiv 0 \mod p$ (không thể xảy ra do $1 \leqslant i, j \leqslant \frac{p-1}{2}$).

Chúng ta vừa chứng minh rằng khi j chạy từ 1 đến $\frac{p-1}{2}$ thì tập hợp các số có dạng $p - r_j$ và s_j sẽ phủ hết tập hợp $\{1, 2, ..., \frac{p-1}{2}\}$.

Ta có các đẳng thức sau:

$$\begin{aligned} a^{\frac{p-1}{2}}.\left(\frac{p-1}{2}\right)! &\equiv \prod_{j=1}^{\frac{p-1}{2}} ja \mod p \\ &\equiv \left(\prod_j r_j\right)\left(\prod_j s_j\right) \mod p \\ &\equiv (-1)^n \left(\prod_j (p - r_j)\right)\left(\prod_j s_j\right) \mod p \\ &\equiv (-1)^n.\left(\frac{p-1}{2}\right)! \mod p. \end{aligned}$$

Mặt khác ta lại có UCLN$(\left(\frac{p-1}{2}\right)!, p) = 1$ nên đẳng thức cuối dẫn đến

$$a^{\frac{p-1}{2}} \equiv (-1)^n \mod p.$$

Kết hợp điều này và Mệnh đề 3.2 ta thu được điều phải chứng minh.

□

Bổ đề 3.6. *Cho p là một số nguyên tố lẻ, khi đó*

- *Ta có* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.
- *Với số nguyên a lẻ và nguyên tố cùng nhau với p thì* $\left(\frac{a}{p}\right) = (-1)^t$. *Ở đây* $t = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor$

Chứng minh. Nhắc lại rằng với mọi $j \in \{1, \ldots, \frac{p-1}{2}\}$ và a nguyên tố cùng nhau với p, sử dụng phép chia Euclid cho ja và p ta thu được

$$ja = \begin{cases} \left\lfloor \frac{ja}{p} \right\rfloor p + r_j & \text{nếu } r_j > \frac{p}{2} \\ \left\lfloor \frac{ja}{p} \right\rfloor p + s_j & \text{nếu } s_j < \frac{p}{2}. \end{cases}$$

Do đó ta có đẳng thức sau:

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p \left\lfloor \frac{ja}{p} \right\rfloor + \sum_{j=1}^{n} r_j + \sum_{j=1}^{k} s_j. \tag{3.1}$$

Hơn nữa theo chứng minh của bổ đề Gauss, khi j chạy từ 1 đến $\frac{p-1}{2}$ thì tập hợp các số có dạng $p - r_j$ và s_j sẽ phủ hết tập hợp $\{1, 2, ..., \frac{p-1}{2}\}$. Vì thế ta có:

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{n}(p - r_j) + \sum_{j=1}^{k} s_j = np - \sum_{j=1}^{n} r_j + \sum_{j=1}^{k} s_j. \tag{3.2}$$

Trừ cả hai vế của phương trình (3.1) cho phương trình (3.2), rồi lấy modulo 2 cả hai vế ta được:

$$(a-1)\left(\sum_{j=1}^{\frac{p-1}{2}} j\right) \equiv \left(\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor - n\right) p \mod 2. \tag{3.3}$$

- Với $a = 2$, ta có $\left\lfloor \frac{2a}{p} \right\rfloor = 0$ với mọi $j \in \{1, \ldots, \frac{p-1}{2}\}$. Do đó trong trường hợp này đẳng thức (3.3) tương đương với

$$n \equiv \sum_{j=1}^{\frac{p-1}{2}} j \equiv \frac{p^2-1}{8} \mod 2.$$

- Với a lẻ, ta có vế trái của đẳng thức (3.3) chia hết cho 2, nên ta thu được:

$$n \equiv \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor \mod 2.$$

Phần còn lại của chứng minh là hệ quả trực tiếp của Bổ đề Gauss. □

Định lý 3.7 (Luật thuận nghịch chính phương)**.** *Cho p và q là hai số nguyên tố lẻ phân biệt. Khi đó ta có:*

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

Chứng minh. Gọi S là tập hợp các số nguyên có dạng $kq - \ell p$ với k là các số nguyên chạy từ 1 đến $\frac{p-1}{2}$ và ℓ là số nguyên chạy từ 1 đến $\frac{q-1}{2}$.

- Với mọi $k \in \{1, \frac{p-1}{2}\}$ và $\ell \in \{1, \ldots, \frac{q-1}{2}\}$ ta luôn có $kq - \ell p \neq 0$. Thật vậy, giả sử $kq - \ell p = 0$, khi đó do p, q là hai số nguyên tố cùng nhau nên p phải là ước của k (điều này không thể xảy ra do $0 < k < p$).

- Với hai cặp $(k,\ell) \neq (k',\ell')$ thì $kq - \ell p \neq k'q - \ell' p$. Thật vậy, giả sử phản chứng ta có $kq - \ell p = k'q - \ell' p$. Khi đó do p, q là hai số nguyên tố cùng nhau nên p phải là ước của $k - k'$ và q phải là ước của $\ell - \ell'$. Mặt khác ta lại có $(k,\ell) \neq (k',\ell')$ nên hoặc $k - k' \neq 0$ hoặc $\ell - \ell' \neq 0$. Không mất tính tổng quát giả sử $k - k' \neq 0$, do p là ước của $k - k'$ nên $p \leqslant |k - k'|$ (điều này không thể xảy ra vì $1 \leqslant k, k' \leqslant \frac{p-1}{2}$).

Vậy S là tập hợp có $\frac{(p-1)}{2}\frac{(q-1)}{2}$ phần tử phân biệt và các phần tử này đều khác 0.

Gọi S_1, S_2 tương ứng là các tập con chứa các phần tử lớn hơn 0, nhỏ hơn 0 của S. Khi đó ta có

$$|S_1| + |S_2| = |S| = \frac{(p-1)}{2}\frac{(q-1)}{2}. \tag{3.4}$$

Giả sử $kq - \ell p$ là một phần tử thuộc S_1 khi đó ta có $\ell \leqslant \left\lfloor \frac{kq}{p} \right\rfloor$. Với $1 \leqslant k \leqslant \frac{p-1}{2}$ ta luôn có

$$\frac{kq}{p} \leqslant \frac{(p-1)q}{2p} < \frac{q}{2},$$

nên $\left\lfloor \frac{kq}{p} \right\rfloor \leqslant \frac{q-1}{2}$. Do đó với mỗi $k \in \{1, \ldots, \frac{p-1}{2}\}$ ta có $\left\lfloor \frac{kq}{p} \right\rfloor$ cách chọn ℓ sao cho $kq - \ell p \in S_1$. Vậy S_1 có số phần tử là

$$|S_1| = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor. \tag{3.5}$$

Làm tương tự ta có số phần tử của tập S_2 là

$$|S_2| = \sum_{\ell=1}^{\frac{q-1}{2}} \left\lfloor \frac{\ell p}{q} \right\rfloor. \tag{3.6}$$

Kết hợp (3.4), (3.5) và (3.6), ta được

$$\sum_{\ell=1}^{\frac{q-1}{2}} \left\lfloor \frac{\ell p}{q} \right\rfloor + \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor = \frac{(p-1)}{2}\frac{(q-1)}{2}. \tag{3.7}$$

Áp dụng Bổ đề 3.6, ta có $\left(\frac{p}{q}\right) = (-1)^{\sum_{\ell=1}^{\frac{q-1}{2}} \left\lfloor \frac{\ell p}{q} \right\rfloor}$ và $\left(\frac{q}{p}\right) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor}$.

Vậy

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{\ell=1}^{\frac{q-1}{2}} \left\lfloor \frac{\ell p}{q} \right\rfloor + \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor} = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}.$$

□

3.2 Luật thuận nghịch tổng quát

Một câu hỏi tương tự với trường hợp bậc 2, đó là cho p là một số nguyên tố, a là một lớp đồng dư modulo p thì phương trình

$$x^3 \equiv a \mod p$$

khi nào thì có nghiệm?

Tương tự như trên, ta xét đồng cấu nhóm

$$\begin{aligned} \varepsilon : \mathbb{F}_p^* &\to \mathbb{F}_p^* \\ x &\mapsto x^3. \end{aligned}$$

Lúc này câu hỏi trên tương đương với câu hỏi a khi nào thì nằm trong ảnh của đồng cấu ε.

Theo định lý về đồng cấu nhóm ta có $\mathbb{F}_p^*/\ker(\varepsilon) \simeq \mathrm{Im}(\varepsilon)$. Do đó trước tiên ta đi tìm hiểu hạt nhân của đồng cấu ε

$$\ker(\varepsilon) = \{x \in \mathbb{F}_p^* | \, x^3 = 1\}.$$

(Điều này tương đương với việc nghiên cứu phương trình đồng dư $x^3 \equiv 1 \mod p$).

Bổ đề 3.8. *Số phần tử của hạt nhân của đồng cấu ε là*

$$|\ker(\varepsilon)| = \begin{cases} 1 & \textit{nếu 3 không phải là ước của } p-1 \\ 3 & \textit{nếu 3 là ước của } p-1. \end{cases}$$

Mệnh đề này có thể phát biểu dưới dạng sơ cấp như sau: phương trình $x^3 \equiv 1 \mod p$ có nghiệm duy nhất nếu $p = 3$ hoặc p là số nguyên tố có dạng $3k+2$ và có 3 nghiệm phân biệt nếu p có dạng $3k+1$.

Chứng minh. • Giả sử $p-1$ không chia hết cho 3, khi đó UCLN$(3, p-1) = 1$. Áp dụng thuật toán Euclid, ta luôn tìm được số nguyên $m \in \mathbb{Z}$ sao cho $3m \equiv 1 \mod (p-1)$. Giả sử x là nghiệm của phương trình $x^3 \equiv 1 \mod p$. Lấy lũy thừa bậc m cả hai vế ta thu được

$$x^{3m} \equiv 1 \mod p. \tag{3.8}$$

Mặt khác do x là nghiệm của phương trình $x^3 \equiv 1 \mod p$ nên UCLN$(x, p) = 1$. Áp dụng định lý Fermat nhỏ và $3m \equiv 1 \mod (p-1)$ ta có

$$x^{3m-1} \equiv 1 \mod p. \tag{3.9}$$

Từ (3.8) và (3.9), ta thu được $x \equiv 1 \mod p$.

- Giả sử 3 là ước của $p-1$. Ta sẽ chứng minh rằng $|\ker(\varepsilon)| = 3$.

  Theo Hệ quả 3.4, ta có phương trình $x^3 = 1$ không thể có quá 3 nghiệm trong $\mathbb{F}_p$. Ta sẽ chứng minh rằng tồn tại $x \not\equiv 1 \mod p$ là nghiệm của phương trình $x^3 = 1$. Khi đó $\{1, x, x^2\}$ chính là 3 nghiệm của phương trình $x^3 - 1 = 0$.

  Do $p-1$ chia hết cho 3, nên ta có thể đặt $p-1 = 3m$. Theo định lý Fermat nhỏ, với mọi $y \in \mathbb{F}_p^*$ ta luôn có

  $$1 = y^{p-1} = y^{3m} = (y^m)^3.$$

  Lấy $x = y^m$ ta sẽ được nghiệm của phương trình $x^3 = 1$. Do đó bài toán sẽ được chứng minh khi ta có thể tìm được $y \in \mathbb{F}_p^*$ sao cho $y^m \not\equiv 1 \mod p$. Điều này đúng do theo Hệ quả 3.4 thì phương trình $y^m - 1 = 0$ có không quá $m-1$ ($m - 1 = \frac{p-1}{3} - 1 < p-2$) nghiệm khác 1.

□

Hệ quả 3.9. • *Nếu 3 là ước của $p-1$, thì phương trình $x^3 \equiv a \mod p$ luôn có đúng 1 nghiệm với mọi $a \in \mathbb{F}_p^*$.*

- *Nếu 3 không là ước của $p-1$ thì phương trình $x^3 \equiv a \mod p$ hoặc vô nghiệm hoặc có đúng 3 nghiệm phân biệt.*

Chứng minh. • Khi $p-1$ không chia hết cho 3, theo Bổ đề 3.8 ở trên, ta có $|\ker(\varepsilon)| = 1$. Do đó ε là một đơn ánh giữa hai tập hợp hữu hạn có cùng số lượng phần tử. Vậy nó phải là một song ánh. Hay

nói một cách khác, với mọi $a \in \mathbb{F}_p^*$ ta luôn tìm được một và chỉ một phần tử $x \in \mathbb{F}_p^*$ sao cho $x^3 = a$.

- Khi $p-1$ chia hết cho 3, theo Bổ đề 3.8 ở trên, ta có $|\ker(\varepsilon)| = 3$. Gọi x_1, x_2, x_3 là 3 phần tử của $\ker(\varepsilon)$. Giả sử x là một nghiệm của phương trình $x^3 = a$. Khi đó xx_i là 3 nghiệm phân biệt của phương trình $x^3 = a$. Áp dụng Hệ quả 3.4, chúng chính là tất cả các nghiệm của phương trình đó.

□

Trong trường hợp $p - 1 = 3m$, nếu phương trình $x^3 \equiv a \mod p$ có nghiệm thì $a^m \equiv 1 \mod p$ (hệ quả của định lý Fermat nhỏ). Ta thu được điều kiện cần để phương trình $x^3 \equiv a \mod p$ có nghiệm.

Giống với trường hợp bậc 2, việc nghiên cứu xem phương trình bậc 3 $x^3 \equiv a \mod p$ có nghiệm khi nào dẫn đến **Luật thuận nghịch bậc 3**. Luật này được xây dựng cho trường các số Eisenstein $\mathbb{Q}[j]$ với $j = \exp^{\frac{2i\pi}{3}}$; căn nguyên thủy bậc 3 của đơn vị.

Trong các chứng minh ở phía trên, Hệ quả 3.4 mặc dù khá đơn giản nhưng đóng một vài trò khá quan trọng. Chúng ta sẽ dành phần cuối của bài giảng này cho các ứng dụng khác của Hệ quả này.

3.3 Một vài ứng dụng của Hệ quả 3.4

Định nghĩa 3.10. Cho p là một số nguyên tố. Theo định lý Fermat nhỏ, với mọi $x \in \mathbb{F}_p^*$ ta có $x^{p-1} \equiv 1 \mod p$. Một lớp đồng dư $x \in \mathbb{F}_p^*$ được gọi là **căn nguyên thủy** của p nếu $x^d \not\equiv 1 \mod p$ với mọi $0 < d < p-1$.

Định lý 3.11. *Mọi số nguyên tố đều có căn nguyên thủy.*

Chứng minh. Với mỗi $x \in \mathbb{F}_p^*$, theo đinh lý Fermat nhỏ ta có $x^{p-1} \equiv 1 \mod p$. Do đó $S_x := \{n \in \mathbb{Z}_+ | x^n \equiv 1 \mod p\}$ là tập con khác rỗng của tập các số nguyên dương. Vì thế nó tồn tại phần tử nhỏ nhất. Gọi $\text{ord}(x)$ là phần tử nhỏ nhất đó của S_x. (Phần tử này còn được gọi là **cấp** của phần tử x trong $\mathbb{F}_p^*$). Đặt

$$d = \max\{\text{ord}(x) | x \in \mathbb{F}_p^*\}.$$

Từ định nghĩa của d, ta thấy rằng

$$d \leqslant p - 1. \tag{3.10}$$

Khẳng định: " Số nguyên dương d chia hết cho $\text{ord}(x)$ với mọi $x \in \mathbb{F}_p^*$".

Giả sử khẳng định trên là đúng, khi đó phương trình $x^d \equiv 1 \mod p$ có ít nhất $p-1$ nghiệm trong $\mathbb{F}_p$. Áp dụng Hệ quả 3.4, ta có:

$$d \geqslant p-1. \tag{3.11}$$

Kết hợp (3.10) và (3.11) ta được $d = p-1$. Từ đó thu được điều phải chứng minh.

Vậy việc còn lại của chúng ta là đi chứng minh khẳng định ở phía trên. Giả sử phản chứng rằng tồn tại một phần tử x sao cho $\text{ord}(x)$ không là ước của d. Khi đó sẽ tồn tại số nguyên tố q mà số mũ lớn nhất của q trong biểu diễn thành tích các thừa số nguyên tố của $\text{ord}(x)$ sẽ phải lớn hơn số mũ đó trong biểu diễn thành tích các số nguyên tố của d. Gọi q^e, q^f tương ứng là số mũ lớn nhất của q trong biểu diễn thành tích các thừa số nguyên tố của $\text{ord}(x)$ và của d. Khi đó $e > f \geqslant 0$.

Gọi g là phần tử có cấp là d. Khi đó $g_1 = g^{q^f}$ là phần tử có cấp là $n_1 = d/q^f$ và $g_2 = x^{\text{ord}(x)/q^e}$ là phần tử có cấp là $n_2 = q^e$. Từ định nghĩa của e và f ta có n_1 không chia hết cho q. Do đó $\text{UCLN}(n_1, n_2) = 1$.

Trong một nhóm giao hoán, nếu g_1 có cấp là n_1 và g_2 có cấp là n_2 với $\text{UCLN}(n_1, n_2) = 1$ thì $g_1 g_2$ sẽ có cấp là $n_1 n_2$. Do đó phần từ $g^{q^f} x^{\text{ord}(x)/q^e}$ có cấp là

$$\frac{d}{q^f} q^e = dq^{e-f} > d.$$

Điều này mâu thuẫn với tình chất lớn nhất của d.

□

Định nghĩa 3.12. Cho $P \in \mathbb{F}_p[X]$ là một đă thức với hệ số trên $\mathbb{F}_p$. Ta gọi P_0 là **dạng rút gọn** của P nếu

- đa thức P_0 là một đa thức có bậc nhỏ hơn hoặc bằng $p-1$;
- với mọi $x \in \mathbb{F}_p$ ta luôn có $P_0(x) = P(x)$.

Theo định lý Fermat nhỏ ta luôn có $x^p \equiv x \mod p$ với mọi $x \in \mathbb{F}_p$. Do đó bằng cách thay X^p bằng X trong biểu thức của P ta sẽ thu được dạng rút gọn P_0.

Bổ đề 3.13. *Cho P_0 và Q_0 là hai đa thức có bậc nhỏ hơn hoặc bằng $p-1$ với hệ số trên một trường $\mathbb{F}_p$. Giả sử rằng $P_0(x) = Q_0(x)$ với mọi $x \in \mathbb{F}_p$*

khi đó

$$P_0(X) \equiv Q_O(X).$$

Chứng minh. Ta áp dụng Hệ quả 3.4 cho đa thức $H(X) = P_0(X) - Q_0(X)$ có bậc nhỏ hơn hoặc bằng $p-1$ và có p nghiệm phân biệt. □

Định nghĩa về dạng rút gọn hoàn toàn có thể mở rộng cho đa thức nhiều biến như sau

Định nghĩa 3.14. Cho $P \in \mathbb{F}_p[X_1, \ldots, X_n]$ là một đa thức n biến với hệ số trên $\mathbb{F}_p$. Đa thức $P_0 \in \mathbb{F}_p[X_1, \ldots, X_n]$ được gọi là dạng rút gọn của P nếu:

- $\deg_{X_i} P_0 \leqslant p-1$, (bất đẳng thức này được đọc là bậc của đa thức P_0 theo biến X_i bất kì đều nhỏ hơn hoặc bằng $p-1$)
- $P_0(x_1, \ldots, x_n) = P(x_1, \ldots, x_n) \quad \forall (x_1, \ldots, x_n) \in \mathbb{F}_p^n$.

Định lý 3.15 (Định lý Chevalley)**.** *Cho $F(X_1, \ldots, X_n) \in \mathbb{F}_p[X_1, X_2, ..., X_n]$ là một đa thức có bậc nhỏ hơn n. Khi đó nếu $F(x_1, \ldots, x_n) = 0$ có nghiệm thì nó có ít nhất hai nghiệm phân biệt.*

Chứng minh. Giả sử $F(x_1, \ldots, x_n) = 0$ có đúng một nghiệm là $(a_1, \ldots, a_n)$. Khi đó ta xét các đa thức sau

$$H(X_1, \ldots, X_n) = 1 - F(X_1, \ldots, X_n)^{p-1},$$

và

$$P(X_1, \ldots, X_n) = \prod_{i=1}^{n} \left(1 - (X_i - a_i)^{p-1}\right)$$

Với mọi $(x_1, \ldots, x_n) \neq (a_1, \ldots, a_n)$ ta có $F(x_1, \ldots, x_n) \neq 0$. Áp dụng định lý Fermat nhỏ ta có $F(x_1, \ldots, x_n)^{p-1} = 1$. Điều này dẫn đến $H(x_1, \ldots, x_n) = 0$. Vậy

$$H(x_1, \ldots, x_n) = \begin{cases} 1 & \text{nếu} (x_1, \ldots, x_n) = (a_1, \ldots, a_n) \\ 0 & \text{trong các trường hợp còn lại.} \end{cases}$$

Với mọi $(x_1, \ldots, x_n) \neq (a_1, \ldots, a_n)$, luôn tồn tại i sao cho $x_i - a_i \neq 0$. Áp dụng định lý Fermat nhỏ ta có $(x_i - a_i)^{p-1} = 1$. Điều này dẫn đến $P(x_1, \ldots, x_n) = 0$.

Vậy

$$P(x_1,\ldots,x_n)=\begin{cases}1 & \text{nếu}(x_1,\ldots,x_n)=(a_1,\ldots,a_n)\\ 0 & \text{trong các trường hợp còn lại.}\end{cases}$$

Gọi H_0 là dạng rút gọn của H. Khi đó ta có

$$P_(x_1,\ldots,x_n)=H_0(x_1,\ldots,x_n)\quad\forall(x_1,\ldots,x_n)\in\mathbb{F}_p^n.$$

Điều này không thể xảy ra vì đa thức P có bậc là $n(p-1)$, trong khi đó đa thức H_0 lại có bậc nhỏ hơn $n(p-1)$ (do $\deg(H_0)\leqslant\deg(H)=(p-1)\deg(F)<n(p-1)$). □

Bài tập 3.1 (Định lý Warning)**.** Cho $F(X_1,\ldots,X_n)\in\mathbb{F}_p[X_1,X_2,...,X_n]$ là một đa thức có bậc nhỏ hơn n. Chứng minh rằng số các nghiệm của F là một bội số của p.

Bài tập về Luật thuận nghịch

Luật thuận nghịch có thể coi là một dạng tổng quát hóa của luật thuận nghịch chính phương đã được đề cập trong các bài học trước. Lịch sử phát triển của luật thuận nghịch cũng là lịch phát triển của lý thuyết số đại số. Trong bài báo "**Vorlesung über die Theorie der algebraischen Zahlen**", Hecke có viết một đoạn như sau:

"*Lý thuyết số hiện đại ra đời từ khi phát hiện ra luật thuận nghịch. Nếu chỉ nhìn cách diễn đạt thì nó thuộc về lý thuyết nghiên cứu các số hữu tỉ, vì phát biểu của nó giống như một quan hệ đơn giản giữa các số hữu tỉ, tuy nhiên nội dung của nó đã vượt xa lĩnh vực các số hữu tỉ.[...]. Sự phát triển của lý thuyết số đại số đã thực sự chỉ ra rằng nội dung của luật thuận nghịch chính phương chỉ trở nên dễ hiểu nếu chúng ta xem xét nó trong bối cảnh các số đại số tổng quát và đó chính là minh chứng cho việc bản chất của một vấn đề chỉ được hiện rõ ra khi ta nhìn nó ở một tầm cao hơn.*"

Định lý 3.16 (Luật thuận nghịch chính phương)**.** *Cho p và q là 2 số nguyên tố lẻ phân biệt. Khi đó ta có*

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

Hơn nữa ta có

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad \text{và} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}};$$

chúng lần lượt được gọi là luật bổ sung thứ nhất và thứ hai.

Bài tập 3.2 (Legendre)**.** Giả sử rằng $a, b, c \in \mathbb{Z}$ là các số nguyên thỏa mãn các tính chất sau:

- chúng đôi một nguyên tố cùng nhau;

- ít nhất một trong 3 tích ab, bc, ca là không âm;
- các phương trình đồng dư sau có nghiệm

$$u^2 \equiv -bc \mod a,\ v^2 \equiv -ca \mod b,\ w^2 \equiv -ab \mod c.$$

Chứng minh rằng phương trình diophantine sau

$$ax^2 + by^2 + cz^2 = 0$$

có nghiệm nguyên không tầm thường.

(Gợi ý :bài tập tương đương với việc chứng minh rằng phương trình $ax^2 + by^2 = cz^2$ với $ab < 0$ hoặc $ac > 0$ có nghiệm không tầm thường nếu các phương trình đồng dư $x^2 \equiv bc \mod a$, $x^2 \equiv ca \mod b$, $x^2 \equiv -ab \mod c$. có nghiệm. Để giải bài toán phát biểu lại ta thực hiện các bước sau

- Chứng minh rằng ta chỉ cần giải bài toán cho bộ ba số tự nhiên a, b, c không có ước chính phương.
- Lấy p là một ước nguyên tố lẻ của c, chọn $x = \alpha, y = \beta$ là một nghiệm không tầm thường của phương trình $ax^2 + by^2 = 0$ trong $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ và chứng minh rằng $ax^2 + by^2 \equiv a(x + \alpha\beta^{-1}y)(x - \alpha\beta^{-1}y) \mod p$. Đặc biệt chứng minh rằng, với mọi ước nguyên tố lẻ p của abc, tồn tại các dạng tuyến tính $\ell_p = rx + sy + tz$ và $m_p = ux + vy + wz$ sao cho $ax^2 + by^2 - cz^2 \equiv \ell_p m_p \mod p$.
- Dùng quan hệ đồng dư $ax^2 + by^2 - cz^2 \equiv (ax + by + cz)^2 \mod 2$ để chứng minh sự tồn tại của các dạng tuyến tính ℓ_2 và m_2.
- Sử dụng định lý thặng dư Trung Hoa để xây dựng các dạng tuyến tính $\ell(x, y, z), m(x, y, z)$ sao cho $\ell(x, y, z) \equiv \ell_p(x, y, z) \mod p$ cho tất các ước nguyên tố p của abc (tương tự cho m). Từ đó kết luận rằng $ax^2 + by^2 - cz^2 \equiv \ell(x, y, z)m(x, y, z) \mod abc$.
- Lấy x,y z là các số nguyên chạy trong tập sau

$$0 \leqslant x < \sqrt{bc},\ 0 \leqslant y < \sqrt{ca},\ 0 \leqslant z < \sqrt{ab}.$$

  Nếu $a = b = c = 1$ ta có khẳng định là tầm thường (bộ các số Pythagore), ngược lại thì cả 3 số $\sqrt{ab}, \sqrt{bc}, \sqrt{ca}$ không thể đồng thời là số nguyên, do đó có nhiều hơn $\sqrt{ab}\sqrt{bc}\sqrt{ac} = abc$ bộ 3 số

(x, y, z). Từ đó suy ra tồn tại hai bộ (x_1, y_1, z_1) và (x_2, y_2, z_2) thỏa mãn tính chất $\ell(x_1, y_1, z_1) \equiv \ell(x_2, y_2, z_2) \mod abc$. Điều đó kéo theo $\ell(x_0, y_0, z_0) \equiv 0 \mod abc$ với $x_0 = x_2 - x_1$, $y_0 = y_2 - y_1$ và $z_0 = z_2 - z_1$.

- Chứng minh rằng $ax_0^2 + by_0^2 - cz_0^2$ là số nguyên chia hết cho abc và nằm trong đoạn từ $-abc$ đến $2abc$. Sử dụng đẳng thức sau để kết thúc chứng minh:

$$(z^2+ab)(ax^2+by^2-cz^2-abc) = a(xz+by)^2+b(yz-ax)^2-c(z^2+ab)^2.)$$

Bài tập 3.3. Dùng khẳng định của bài tập 2 thêm với giả thiết là cho trước hai số nguyên tố cùng nhau a và b thì có vô số số nguyên tố p thỏa mãn tính chất $p \equiv a \mod b$ hãy chứng minh lại luật thuật nghịch chính phương.

Bài tập 3.4. Cho p là số nguyên tố lẻ, và đặt α_{ij} là số lượng phần tử của tập hợp

$$A_{ij} := \left\{ k \in \{1, 2, \ldots, p-1\} : \left(\frac{k}{p}\right) = (-1)^i, \left(\frac{k+1}{p}\right) = (-1)^j \right\}.$$

Chứng minh rằng

- $p - 2 = \alpha_{00} + \alpha_{01} + \alpha_{10} + \alpha_{11}$;
- $-1 - \left(\frac{-1}{p}\right) = \sum_{k=1}^{p-2} \left\{ \left(\frac{k}{p}\right) + \left(\frac{k+1}{p}\right) \right\} = 2\alpha_{00} - 2\alpha_{11}$;
- $1 - \left(\frac{-1}{p}\right) = \sum_{k=1}^{p-2} \left\{ \left(\frac{k}{p}\right) - \left(\frac{k+1}{p}\right) \right\} = 2\alpha_{01} - 2\alpha_{10}$;
- $-1 = \sum_{k=1}^{p-2} \left\{ \left(\frac{k}{p}\right) \left(\frac{k+1}{p}\right) \right\} = \alpha_{00} - \alpha_{01} - \alpha_{10} + \alpha_{11}$.

Từ đó thu được $\alpha_{00} = \frac{p-5}{4}$, $\alpha_{01} = \alpha_{10} = \alpha_{11} = \frac{p-1}{4}$ nếu $p \equiv 1 \mod 4$ và $\alpha_{01} = \frac{p+1}{4}$, $\alpha_{00} = \alpha_{10} = \alpha_{11} = \frac{p-3}{4}$ nếu $p \equiv 3 \mod 4$.

Bài tập 3.5. Đặt $N(x^2+y^2=1)$ là số nghiệm $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ của phương trình $x^2 + y^2 = 1$, tương tự, đặt $N(x^2 = a)$ là số nghiệm của phương trình $x^2 = a$ trong $\mathbb{F}_p$. Chứng minh rằng $N(x^2 + y^2 = 1) = p - \left(\frac{-1}{p}\right)$ bằng cách tính tổng sau

$$\sum_{a+b=1} N(x^2 = a)N(x^2 = b) = \sum_{a+b=1} \left(1 + \left(\frac{a}{p}\right)\right)\left(1 + \left(\frac{b}{p}\right)\right).$$

Bài tập 3.6. Cho p là số nguyên tố lẻ, chứng minh rằng mỗi nghiệm (x, y) của $x^2 + y^2 = 1$ trong $\mathbb{F}_p$ sẽ cho ta 8 nghiệm phân biệt $(\pm x, \pm y)$ và $(\pm y, \pm x)$ trừ trường hợp hoặc $x = 0$ hoặc $y = 0$ hoặc $x = y$. Đếm số nghiệm của phương trình trong 3 trường hợp vừa liệt kê đó, từ đó chứng minh luật bổ sung thứ hai của luật thuận nghịch chính phương (gợi ý dùng công thức bài trên).

Bài tập 3.7.

- Cho $p = 2m + 1$ và $q = 2n + 1$ là các số nguyên tố, đặt $S_{p,q}$ là tập hợp tất cả các nghiệm trong $\mathbb{F}_p$ của phương trình $x_1^2 + \cdots + x_q^2 = 1$. Chứng minh rằng số lượng phân tử của $S_{p,q}$ bằng $p^{q-1} + (-1)^{mn} p^n$.

- Xét ánh xạ $\phi : S_{p,q} \to S_{p,q}$ định nghĩa bởi $(x_1, \ldots, x_q) \mapsto (x_2, \ldots, x_q, x_1)$. Chứng minh rằng ϕ có điểm cố định khi và chỉ khi $\left(\frac{p}{q}\right) = 1$. Kiểm tra rằng $\left(\frac{p}{q}\right) = -1$ khi và chỉ khi $|S_{p,q}| \equiv 0 \mod q$ bằng cách tính các quỹ đạo của ϕ, và sau đó sử dụng công thức vừa tính được ở phần trên đưa ra một chứng minh mới cho luật thuận nghịch chính phương.

Bài tập 3.8.

- Cho p là một số nguyên tố lẻ và $f \in \mathbb{Z}[x]$ là một đa thức có bậc $\geqslant 1$. Chứng minh rằng so $N_p(f)$ các nghiệm $(x, y) \in \mathbb{F}_p^2$ của phương trình đồng dư $y^2 \equiv f(x) \mod p$ có thể biểu diễn dưới dạng $N_p(f) = p + S_p(f)$ với $S_p(f) = \sum_{x=0}^{p-1} \left(\frac{f(x)}{p}\right)$.

- Chứng minh rằng $N_p(f) = p + (-1)^{(p-1)/2}$ với $f(x) = 1 - x^2$, và $N_p(f) = p - \left(\frac{a}{p}\right)$ với $f(x) = x^3 + ax^2$.

- Cho $k \in \mathbb{Z} - \{0\}$ và đặt $f(x) = (x + k)(x + k^2)$. Chứng minh rằng $S_p(f) = \left(\frac{k}{p}\right) T_p(f)$, trong đó $T_p(f) = 1 + \sum_{x=1}^{(p-1)/2} \left\{ \left(\frac{1+x}{p}\right) + \left(\frac{1-x}{p}\right) \right\} \left(\frac{1+x^2}{p}\right)$ không phụ thuộc vào k. Chứng minh rằng $T \mod 4$ chỉ phụ thuộc vào $p \mod 8$.

Bài tập 3.9 (Euler)**.** Cho $a \in \mathbb{Z}$ là một số nguyên không có ước chính phương. Cho c và d là hai số nguyên dương thỏa mãn tính chất $c \equiv d \mod 4a$. Chứng minh rằng phương trình $x^2 - ay^2 = sz^2$ có nghiệm nguyên với $s = c$ khi và chỉ khi nó có nghiệm nguyên với $s = d$.

Bài tập 3.10. Cho p là số nguyên tố dạng 3k+1. Chứng minh rằng p có thể viết dưới dạng $p = a^2 + 3b^2$ với a và b là các số nguyên (cách viết

này là duy nhất sai khác dấu của a, b). Từ đó suy ra $4p$ có thể viết được dưới dạng $L^2 + 27M^2$ (cách viết này là duy nhất sai khác dấu của L, M)

Bài tập 3.11. Chứng minh rằng nếu p là số nguyên tố dạng 3k+2 thì phương trình đồng dư $x^3 \equiv c \mod p$ luôn có nghiệm với mọi $c \in \mathbb{Z}$.

CHƯƠNG 4

Các số p-adics

4.1 Bổ đề Hensel

Cho $\mathbb{P} \in \mathbb{Z}[X]$ là một đa thức với hệ số nguyên. Cho $x_0 \in \mathbb{Z}$ thỏa mãn tính chất $\mathbb{P}(x_0) \equiv 0 \mod p$. Giả sử rằng $P'(x_0) \not\equiv 0 \mod p$. Khi đó với mọi $n \in \mathbb{N}$ luôn tồn tại duy nhất một lớp đồng dư $x_n \mod p^n$ sao cho:

a) $x_n \equiv x_0 \mod p$,

b) $P(x_n) \equiv 0 \mod p^{n+1}$.

Chứng minh. Ta sẽ chứng minh bằng quy nạp theo n.

- Với $n = 0$, đây là giả thiết của bổ đề.
- Với $n = 1$, từ giả thiết ta có $x_0 \in \mathbb{Z}$ thỏa mãn tính chất

$$P(x_0) \equiv 0 \mod p$$

và

$$P'(x_0) \not\equiv 0 \mod p.$$

Xét $x_1 = x_0 + py_1$, khi đó sử dụng khai triển Taylor cho đa thức P tại lân cận của điểm $x = x_0$ ta thu được:

$$P(x_1) = P(x_0) + py_1P'(x_0) + \underbrace{\frac{P''(x_0)}{2}p^2y_1^2 + \frac{P'''(x_0)}{3!}p^3y_1^3 + \dots}_{\text{các hạng tử đều chia hết cho } p^2}.$$

Điều này dẫn đến $P(x_1) \equiv 0 \mod p^2$ khi và chỉ khi

$$P(x_0) + py_1P'(x_0) \equiv 0 \mod p^2.$$

Ngoài ra do $P(x_0) \equiv 0 \mod p$ nên $P(x_0) = a_0 p$ với a_0 là một số nguyên nào đó. Vì thế ta có:

$$a_0 p + p y_1 P'(x_0) \equiv 0 \mod p^2.$$

Đẳng thức này tương đương với

$$a_0 + y_1 P'(x_0) \equiv 0 \mod p. \tag{4.1}$$

Hơn nữa, từ giả thiết $P'(x_0) \not\equiv 0 \mod p$, ta biết được $P'(x_0)$ là phần tử nghịch đảo được của $\mathbb{Z}/p\mathbb{Z}$. Do đó tồn tại duy nhất một phần tử $b \in \mathbb{Z}/p\mathbb{Z}$ sao cho $bP(x_0) \equiv 1 \mod p$. Nhân cả hai vế đẳng thức (4.1) với b, ta thu được

$$a_0 b + y_1 \equiv 0 \mod p.$$

Hay

$$y_1 \equiv -b a_0 \mod p.$$

Vậy tồn tại duy nhất một lớp đồng dư y_1 modulo p sao cho

$$P(x_0 + p y_1) \equiv 0 \mod p.$$

Ta vừa chứng minh rằng bổ đề cũng đúng cho trường hợp $n = 1$.

- Giả sử khẳng định đúng với $n \geqslant 1$, tức là tồn tại duy nhất một lớp đồng dư $x_n \mod p^n$ sao cho:

$$P(x_n) \equiv 0 \mod p^{n+1}$$

và

$$x_n \equiv x_0 \mod p.$$

Đẳng thức $x_n \equiv x_0 \mod p$ kéo theo $P'(x_n) \equiv P'(x_0) \not\equiv 0 \mod p$. Hay nói cách khác ta có $P'(x_n)$ là một phần tử nghịch đảo được của $\mathbb{Z}/p\mathbb{Z}$.

Tương tự như trên ta xét $x_{n+1} = x_n + p^{n+1} y_{n+1}$, rồi khai triển Taylor đa thức P tại lân cận của điểm x_n ta được:

$$P(x_{n+1}) = P(x_n) + p^{n+1} y_{n+1} P'(x_n) + \underbrace{\frac{P''(x_n)}{2} p^{2(n+1)} y_{n+1}^2 + \dots}_{\equiv 0 \mod p^{n+2}}.$$

Điều này dẫn đến $P(x_{n+1}) \equiv 0 \mod p^{n+2}$ khi và chỉ khi

$$P(x_n) + p^{n+1} y_{n+1} P'(x_n) \equiv 0 \mod p^{n+2}.$$

Ngoài ra do $P(x_n) \equiv 0 \mod p^{n+1}$ nên $P(x_n) = a_n p^{n+1}$ với a_n là một số nguyên nào đó. Vì thế ta có:

$$a_n p^{n+1} + p^{n+1} y_{n+1} P'(x_n) \equiv 0 \mod p^{n+2}.$$

Đẳng thức này tương đương với

$$a_n + y_{n+1} P'(x_n) \equiv 0 \mod p. \tag{4.2}$$

Hơn nữa, ta lại có $P'(x_n)$ là một phần tử nghịch đảo được của $\mathbb{Z}/p\mathbb{Z}$. Do đó đẳng thức (4.2) tương đương với

$$y_{n+1} \equiv -\frac{a_n}{P'(x_n)} \mod p.$$

□

Việc xây dựng x_{n+1} từ x_n như trong chứng minh trên gợi ta nhớ đến **phương pháp Newton**. Phương pháp này được dùng để tìm nghiệm thực gần đúng của phương trình $P(x) = 0$ với P là một hàm số thực. Phương pháp Newton được phát biểu như sau (để đơn giản ta bỏ qua các điều kiện kỹ thuật của hàm P để các bước sau có thể làm được):

1. Giả sử x_0 là một số thực đủ gần với nghiệm của phương trình thỏa mãn tính chất $P'(x_0) \neq 0$. Xét $x_1 = x_0 + y_0$. Khai triển Taylor hàm $P(x)$ tại tiệm cận của điểm x_0 ta thu được

$$P(x_1) = P(x_0) + P'(x_0) y_0 + \underbrace{\frac{P''(x_0)}{2!} y_0^2 + \frac{P'''(x_0)}{3!} y_0^3 + \dots}_{\text{bỏ qua khi } y \text{ tiến tới } 0}.$$

2. Ta giải phương trình: $P(x_0) + P'(x_0) y_0 = 0$ được

$$y_0 = -\frac{P(x_0))}{P'(x_0)}.$$

Từ đó thu được một giá trị xấp xỉ mới tốt hơn x_0; đó là

$$x_1 = x_0 - \frac{P(x_0)}{P'(x_0)}.$$

3. Thay vai trò của x_0 bằng x_1 trong các bước thực hiện trên, ta xây dựng được một giá trị xấp xỉ mới $x_2 = x_1 - \frac{P(x_1)}{P'(x_1)}$.

4. Cứ tiếp tục xây dựng như vậy, ta sẽ thu được một dãy các xấp xỉ $x_1, x_2, \ldots, x_n, \ldots$. Với hàm các điều kiện khởi đầu đủ tốt, ta giả sử rằng dãy x_n sẽ hội tụ về một giá trị thực x. Khi đó ta có

$$x = x - \frac{P(x)}{P'(x)}.$$

Đơn giản hai vế ta thu được $P(x) = 0$. Hay nói một cách khác x là nghiệm của phương trình ta cần tìm.

Ta nhận thấy rằng để có thể sử dụng được phương pháp Newton thì $|P(x_0)|$ nhỏ và $|P'(x_0)|$ lớn. Vậy thì nếu đặt bổ đề Hensel trong cùng bối cảnh của phương pháp Newton, lúc này sẽ cần có một cách nói về "độ lớn" mới (theo nghĩa p-adic) mà độ lớn nhỏ tương ứng với $P(x_0) \equiv 0 \mod p$ và độ lớn to tương ứng với $P'(x_0) \not\equiv 0 \mod p$.

4.2 Chuẩn p-adic

Định nghĩa 4.1. Cho p là một số nguyên tố và $x \in \mathbb{Q}^*$ là một số hữu tỉ khác 0 bất kì. Khi đó $x = \frac{m}{n}$ với m, n là hai số nguyên khác không và nguyên tố cùng nhau. Giả sử $m = p^{r_1}m'$ và $n = p^{r_2}n'$ với $r_1, r_2 \in \mathbb{N}$ và $\text{UCLN}(p, m') = \text{UCLN}(p, n') = 1$. (Chú ý rằng do m, n nguyên tố cùng nhau, nên trong r_1 và r_2 phải có ít nhất một số bằng 0). Ta định nghĩa:

$$|x|_p = \left|\frac{m}{n}\right|_p = p^{-(r_1 - r_2)}.$$

Trong trường hợp $x = 0$, ta định nghĩa $|0|_p = 0$.

Từ định nghĩa ta thấy rằng một số hữu tỉ có chuẩn p-adic càng nhỏ thì lũy thừa của p mà nó chia hết càng lớn.

Ví dụ 4.2. $|1|_p = 1$, $|p|_p = p^{-1}$, $|p^2|_p = p^{-2}$, ... $|p^k|_p = p^{-k}$.

Sử dụng định nghĩa chuẩn p-adic, các điều kiện của bổ đề Hensel có thể phát biểu lại như sau:

$$P(x_0) \equiv 0 \mod p \Leftrightarrow |P(x_0)|_p \leqslant p^{-1}$$

và

$$P(x_0) \not\equiv 0 \mod p \Leftrightarrow |P(x_0)|_p = 1.$$

Mệnh đề 4.3. *Trên tập hợp các số nguyên $\mathbb{Z}$ được trang bị một chuẩn p-adic $|\bullet|_p$, ta luôn có:*

- $|mn|_p = |m|_p.|n|_p$.
- $|m+n|_p \leqslant \max(|m|_p, |n|_p)$

Chứng minh.

- Ta viết $m = p^{r_1}m'$ và $n = p^{r_2}n'$ với $\text{UCLN}(p, m') = \text{UCLN}(p, n') = 1$. Khi đó $mn = p^{r_1+r_2}m'n'$, với $\text{UCLN}(p, m'n') = 1$. Điều đó dẫn đến

$$|mn|_p = p^{-(r_1+r_2)} = p^{-r_1}p^{-r_2} = |m|_p|n|_p.$$

- Do vai trò của m, n là như nhau nên không mất tính tổng quát ta có thể giả sử $r_1 \leqslant r_2$. Khi đó ta có p^{r_1} là ước chung của m và n. Do đó p^{r_1} cũng là ước của $m+n$. Điều này dẫn đến

$$|m+n|_p \leqslant p^{-r_1} = \max\{p^{-r_1}, p^{-r_2}\} = \max\{|m|_p, |n|_p\}.$$

□

Sử dụng chuẩn p-adic để nhìn lại bổ đề Hensel. Ta đã xây dựng được dãy các sô $x_0, x_1, \ldots$ thỏa mãn tính chất $P(x_i) \equiv 0 \mod p^{i+1}$ và $x_{i+1} \equiv x_i \mod p^{i+1}$ với mọi $i \in \mathbb{N}$.

Bằng quy nạp ta có thể chứng minh rằng với mọi $m, n \geqslant N$ ta luôn có

$$x_m \equiv x_n \mod p^{N+1}).$$

Điều này kéo theo

$$|x_m - x_n|_p \leqslant p^{-(N+1)}.$$

Vậy dãy $x_0, x_1, \ldots, x_n, \ldots$ là một dãy Cauchy đối với chuẩn p-adic. Rất tiếc rằng trong trường hợp tổng quát một dãy Cauchy các số nguyên sẽ không hội tụ đến một số nguyên. Do đó để dãy trên hội tụ ta cần *đầy đủ hóa* $\mathbb{Z}$ theo chuẩn p-adic (nói cách khác, là làm đầy $\mathbb{Z}$ để sao cho mọi dãy Cauchy trong làm đầy này đều hội tụ). Gọi $\mathbb{Z}_p$ là đầy đủ hóa của $\mathbb{Z}$ theo chuẩn p-adic. Khi đó các phần tử của nó là các lớp tương đương

của tập hợp các dãy Cauchy (tương ứng với chuẩn p-adic) trên $\mathbb{Z}$ và với quan hệ tương đương là:

"Hai dãy Cauchy $(a_1, a_2, \dots, a_n, \dots)$ và $(b_1, b_2, \dots, b_n, \dots)$ được gọi là tương đương với nhau khi và chỉ khi dãy $(a_1, b_1, a_2, b_2, \dots, a_n, b_n, \dots)$ vẫn còn là một dãy Cauchy."

Các phần tử của $\mathbb{Z}_p$ có thể được mô tả như sau:

"Một số nguyên p-adic $a \in \mathbb{Z}_p$ chính là một dãy Cauchy $a = (a_0, a_1, \dots)$ với $a_i \in \mathbb{Z}/p^{i+1}\mathbb{Z}$ thỏa mãn tính chất $a_{i+1} \equiv a_i \mod p^i$. Hơn nữa,

$$|a|_p = p^{-i}$$

với i là chỉ số tự nhiên nhỏ nhất thỏa mãn tính chất $a_i \neq 0$."

Lúc này bổ đề Hensel có thể phát biểu lại như sau:

Mệnh đề 4.4 (Bổ đề Hensel)**.** *Cho $P(X) \in \mathbb{Z}[X]$ là một đa thức với hệ số nguyên. Giả sử x_0 là một số nguyên thỏa mãn tính chất*

$$\begin{cases} P(x_0) \equiv 0 \mod p \\ P'(x_0) \not\equiv 0 \mod p \end{cases}$$

Khi đó tồn tại duy nhất một số nguyên p-adic $x \in \mathbb{Z}_p$ sao cho $x \equiv x_0 \mod p$ và là nghiệm của phương trình $P(x) = 0$.

Hệ quả 4.5. *Sử dụng ký hiệu của mệnh đề phía trên, khi đó phương trình $P(x) = 0$ có nhiều nhất một nghiệm nguyên $x \in \mathbb{Z}$ thỏa mãn tính chất $x \equiv x_0 \mod p$.*

Nhận xét: Các số p-adic cho chúng ta một cái nhìn giải tích trong việc giải các phương trình đồng dư.

Bài tập 4.1. Phát biểu và chứng minh bổ đề Hensel suy biến.

Ta để ý rằng $\mathbb{R}$ chính là trường đầy đủ của $\mathbb{Q}$ theo chuẩn giá trị tuyệt đối thông thường. Với tôpô thông thường (cảm sinh từ chuẩn giá trị tuyệt đối), trên $\mathbb{R}$ ta có kết quả quan trọng sau:

Định lý 4.6 (Định lý Bolzano - Weierstrass)**.** *Tập $[0, 1]$ là một tập compact trên $\mathbb{R}$ với tôpô thông thường. (Hay nói một cách khác mọi dãy $x_0, x_1, \dots, x_n, \dots$ có vô hạn phần tử trong $[0, 1]$ đều có thể trích ra được một dãy con hội tụ trong $[0, 1]$).*

Chứng minh. Chia tập $S_0 := [0,1]$ thành 2 tập con $\left[0, \frac{1}{2}\right]$ và $\left[\frac{1}{2}, 1\right]$. Do dãy $\{x_i\}$ có vô hạn phần tử nên một trong hai tập con này sẽ có ít nhất một tập chứa vô hạn phần tử của dãy $\{x_i\}$. Ta gọi S_1 là tập có tính chất này và lấy x_{i_1} là phần tử bất kì của dãy $\{x_i\}$ nằm trong S_1. Khoảng cách giữa hai đầu mút của tập S_1 là $\frac{1}{2}$

Ta lại chia tập S_1 thành hai phần bằng nhau, một trong hai phần này phải chứa vô hạn phần tử của dãy $\{x_i\}$. Gọi S_2 là phần chứa vô hạn phần tử của dãy $\{x_i\}$ và lấy x_{i_2} là một phần tử bất kì của dãy nằm trong S_2. Khoảng cách giữa hai điểm đầu mút của S_2 là $\frac{1}{4}$.

Tiếp tục làm như vậy ta thu được dãy các tập con lồng nhau $S_0 \supset S_1 \supset \cdots \supset S_j \supset \ldots$ sao cho mỗi S_j đều chứa vô hạn phần tử của dãy $\{x_i\}$ và khoảng cách giữa hai đầu mút của S_j là $\frac{1}{2^j}$. Trên mỗi S_j ta lấy một phần tử bất kì x_{i_j} của dãy đã cho. Khi đó với mọi $\varepsilon > 0$ ta luôn tìm được $N \in \mathbb{N}$ sao cho $\frac{1}{2^j} < \varepsilon$ với mọi $j \geqslant N$. Mặt khác ta lại có $x_{i_j} \in S_N$ với mọi $j \geqslant N$ nên

$$|x_{i_j} - x_{i_k}| \leqslant \frac{1}{2^N} < \varepsilon$$

với mọi $j, k \geqslant N$.

Ta vừa chứng minh rằng dãy $\{x_{i_j}\}$ là một dãy Cauchy trong $\mathbb{R}$, nên nó cũng là một dãy hội tụ. □

Với $\mathbb{Z}_p$ là một đầy đủ của $\mathbb{Z}$ theo chuẩn p-adic ta cũng có một kết quả tương tự.

Định lý 4.7. *Tập $\mathbb{Z}_p$ là một tập compact với tôpô cảm sinh từ chuẩn p-adic. (Hay nói một cách khác mọi dãy $x_0, x_1, \ldots, x_n, \ldots$ có vô hạn phần tử trong $\mathbb{Z}_p$ đều có thể trích ra được một dãy con hội tụ trong $\mathbb{Z}_p$.)*

Chứng minh. Từ giả thiết $x_i \in \mathbb{Z}_p$ ta có $x_i = (a_{i,0}, a_{i,1}, \ldots)$ với $a_{i,j} \in \mathbb{Z}/p^{j+1}\mathbb{Z}$ và thỏa mãn tính chất $a_{i,j+1} \equiv a_{i,j} \mod p^{j+1}$.

Do dãy $\{x_i\}$ có vô hạn phần tử nên trong p lớp đồng dư modulo p sẽ có ít nhất một lớp đồng dư $b_0 \in \mathbb{Z}/p\mathbb{Z}$ là giá trị của $a_{i,0}$ vô hạn lần. Hay nói cách khác tồn tại $b_0 \in \mathbb{Z}/p\mathbb{Z}$ sao cho có vô hạn số của dãy x_i có khởi đầu là b_0.

Do chỉ có p lớp đồng dư $b \mod \mathbb{Z}/p^2\mathbb{Z}$ thỏa mãn tính chất $b \equiv b_0 \mod p$, nên tồn tại ít nhất một lớp đồng dư $b_1 \mod \mathbb{Z}/p^2\mathbb{Z}$ thỏa mãn tính chất $b_1 \equiv b_0 \mod p$ là giá trị của $a_{i,1}$ của phần tử x_i có khởi đầu là

b_0 vô hạn lần. Hay nói một cách khác sẽ có vô hạn phần tử của x_i có khởi đầu là (b_0, b_1).

Cứ tiếp tục như vậy ta nhận được phần tử $x = (b_0, b_1, \dots, b_n, \dots) \in \mathbb{Z}_p$ là điểm hội tụ của một dãy con của dãy $\{x_i\}$. □

Mệnh đề 4.8. *Cho $P \in \mathbb{Z}[X]$ là một đa thức với hệ số nguyên. Giả sử rằng*

$$P(x) \equiv 0 \mod p^n$$

luôn có nghiệm với mọi số nguyên dương n. Khi đó tồn tại $x \in \mathbb{Z}_p$ sao cho $P(x) = 0$.

Chứng minh. Từ giả thiết ta có với mọi số nguyên dương n luôn tồn tại $a_n \mod p^n$ thỏa mãn tính chất

$$P(a_n) \equiv 0 \mod p^n.$$

Xét dãy các phần tử $x_i \in \mathbb{Z}_p$ được định nghĩa như sau:

$$x_i = (a_i \mod p, \dots, a_i \mod p^{i-1}, a_i, a_i, \dots).$$

Do $\mathbb{Z}_p$ là một tập compact nên từ dãy trên ta luôn có thể trích ra được một dãy con $\{x_{i_j}\}$ thỏa mãn tính chất $x_{i_j} \to x \in \mathbb{Z}_p$ khi j tiến tới $+\infty$. Điều này dẫn đến

$$\lim_{j \to \infty} |P(x_{i_j})|_p = |P(x)|_p.$$

Mặt khác ta lại có $0 \leqslant |P(x_{i_j})|_p \leqslant p^{-i_j} \leqslant p^{-j}$ với mọi $j \in \mathbb{N}$, nên theo nguyên lý kẹp ta có

$$\lim_{j \to \infty} |P(x_{i_j})|_p = 0.$$

Kết hợp hai đẳng thức trên ta nhận được $|P(x)|_p = 0$. Điều này chỉ xảy ra khi $P(x) = 0$.

□

Một trong những phương pháp giải phương trình nghiệm hữu tỷ (nguyên lý Hasse địa phương-toàn cục)

- Giả sử phương trình $P(x) = 0$ có nghiệm hữu tỷ thì nó phải có nghiệm thực (nghiệm hữu tỷ cũng chính là nghiệm thực) và nghiệm p-adic (việc tồn tại nghiệm p-adic chính là hệ quả trực tiếp của

Mệnh đề 4.8). Do đó nếu chứng minh được rằng hoặc phương trình không có nghiệm thực, hoặc không có nghiệm p-adic với một số p nguyên tố nào đó thì phương trình cũng không có nghiệm hữu tỷ.

- Rất tiếc rằng điều kiện có nghiệm thực và nghiệm p-adic chỉ là điều kiện cần chứ không phải là điều kiện đủ. Có những phương trình có cả nghiệm thực và nghiệm p-adic với mọi số nguyên tố p nhưng nó hoàn toàn không có nghiệm hữu tỷ.

Bài tập về Các Số p-adic

Cho k là một trường và $\mathbb{R}_+ := \{x \in \mathbb{R} : x \geqslant 0\}$ là tập hợp các số thực không âm.

Định nghĩa 4.9. Một **giá trị tuyệt đối** (đôi khi cũng được gọi là **chuẩn**) trên k là một hàm số

$$| \quad | : k \to \mathbb{R}_+$$

thỏa mãn các tính chất sau:

1. $|x| = 0$ khi và chỉ khi $x = 0$,
2. $|xy| = |x||y|$ với mọi $x, y \in k$,
3. $|x + y| \leqslant |x| + |y|$ với mọi $x, y \in k$.

   Chúng ta sẽ gọi một giá trị tuyệt đối trên k là **không Ácsimét** nếu nó thỏa mãn thêm điều kiện sau:

4. $|x + y| \leqslant \max\{|x|, |y|\}$ với mọi $x, y \in k$;

   và là **Ácsimét** nếu ngược lại.

Bài tập 4.2. Cho k là một trường có hữu hạn phần tử. Chứng minh rằng chỉ có duy nhất một giá trị tuyệt đối trên k và nó là giá trị tuyệt đối tầm thường (nghĩa là $|x| = 1$ với mọi $x \neq 0$).

Định nghĩa 4.10. Cố định p là một số nguyên tố nào đó. Với mọi $x \in \mathbb{Q} - \{0\}$ ta luôn có thể biểu diễn duy nhất dưới dạng $x = p_p^v(x)\frac{a}{b}$ trong đó $v_p(x)$ là một số nguyên nào đó phụ thuộc vào x; a và b là hai số nguyên nguyên tố cùng nhau và nguyên tố cùng nhau với p. Ta định nghĩa giá trị tuyệt đối p-adic của $x \in \mathbb{Q}$ như sau

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{nếu } x \neq 0, \\ 0 & \text{nếu } x = 0. \end{cases}$$

Bài tập 4.3. Chứng minh rằng hàm $|\quad|_p$ là một giá trị tuyệt đối không Ácsimét trên $\mathbb{Q}$.

Bài tập 4.4. Chứng minh rằng một giá trị tuyệt đối $|\quad|$ trên $\mathbb{Q}$ là không Ácsimét khi và chỉ khi $|n| \leqslant 1$ với mọi $n \in \mathbb{Z}$.

Bài tập 4.5. Cho $|\quad|$ một giá trị tuyệt đối trên $\mathbb{Q}$. Chứng minh rằng nếu tập giá trị tuyệt đối của các số nguyên bị chặn bởi $C < \infty$ thì $|\quad|$ là không Ácsimét hơn thế và $C = 1$.

Định nghĩa 4.11. Cho k là một trường và $|\quad|$ là một giá trị tuyệt đối trên k. Ta định nghĩa **khoảng cách** $d(x, y)$ giữa hai phần tử $x, y \in k$ bởi

$$d(x, y) = |x - y|.$$

Định nghĩa 4.12. Cho k là một trường và $|\quad|$ là một giá trị tuyệt đối trên k. Cho $a \in k$ và $r \in \mathbb{R}_+$. **Hình cầu mở** tâm a bán kính r là tập hợp

$$B(a, r) := \{x \in k : d(x, a) < r\}.$$

Hình cầu đóng tâm a bán kính r là tập hợp

$$\overline{B}(a, r) := \{x \in k : d(x, a) \leqslant r\}.$$

Một tập con $A \subset k$ được gọi là **mở** nếu với mọi $x \in A$ luôn tồn tại $r > 0$ sao cho $B(x, r) \subset A$. Tập con A được gọi là **đóng** nếu $k - A$ là một tập mở.

Bài tập 4.6. Cho k là một trường và $|\quad|$ là một giá trị tuyệt đối không Ácsimét trên k. Chứng minh rằng

- Nếu $b \in B(a, r)$ thì $B(a, r) = B(b, r)$; nói một cách khác mọi điểm trong hình cầu mở đều là tâm của hình cầu mở đó.
- Nếu $b \in \overline{B}(a, r)$ thì $\overline{B}(a, r) = \overline{B}(b, r)$; nói một cách khác mọi điểm trong hình cầu đóng đều là tâm của hình cầu đóng đó.
- Tập hợp $B(a, r)$ là một tập vừa đóng vừa mở.
- Nếu $r \neq 0$, thì tập hợp $\overline{B}(a, r)$ là một tập vừa đóng vừa mở.
- Hai hình cầu mở bất kì hoặc rời nhau hoặc chứa nhau (tức là một hình cầu sẽ được chứa hoàn toàn trong hình cầu khác).

- Hai hình cầu mở bất kì hoặc rời nhau hoặc chứa nhau.

Định nghĩa 4.13. Cho k là một trường và $|\quad|$ là một giá trị tuyệt đối trên k. Một tập hợp $S \subset k$ được gọi là **liên thông** nếu không tồn tại hai tập mở $U_1, U_2 \subset k$ thỏa mãn các tính chất sau:

- $U_1 \cap U_2 = \emptyset$,
- $S = (S \cap U_1) \cup (S \cap U_2)$,
- Cả hai tập $S \cap U_1$ và $S \cap U_2$ đều khác rỗng.

Bài tập 4.7. Cho A và B là hai tập con liên thông của k. Chứng minh rằng nếu $A \cap B \neq \emptyset$ thì $A \cup B$ cũng là một tập liên thông.

Bài tập 4.8. Với mọi $x \in k$, ta định nghĩa **thành phần liên thông của** x là hợp của tất cả các tập con liên thông chứa x của k. (Theo bài trên, ta có thể hiểu thành phần liên thông của x chính là tập liên thông lớn nhất chứa x của k). Chứng minh rằng nếu giá trị tuyệt đối trên k không Ácsimét thì thành phần liên thông của bất kì điểm $x \in k$ nào cũng chỉ chứa duy nhất một phần tử và phần tử đó là x.

Định nghĩa 4.14. Hai giá trị tuyệt đối $|\quad|_1$ và $|\quad|_2$ trên k được gọi là **tương đương** với nhau nếu mọi tập mở tương ứng với giá trị tuyệt đối này cũng là tập mở tương ứng với giá trị tuyệt đối kia.

Bài tập 4.9. Cho hai giá trị tuyệt đối $|\quad|_1$ và $|\quad|_2$ trên k. Chứng minh rằng các khẳng định sau là tương đương:

- $|\quad|_1$ và $|\quad|_2$ tương đương với nhau;
- Với mọi $x \in k$, ta có $|x|_1 < 1$ khi và chỉ khi $|x|_2 < 1$;
- tồn tại một số thực dương α thỏa mãn tính chất với mọi $x \in k$ ta có
$$|x|_1 = |x|_2^{\alpha}.$$

Bài tập 4.10 (Định lý của Ostrowski)**.** Chứng minh rằng mọi giá trị tuyệt đối không tầm thường trên $\mathbb{Q}$ thì tương đương với hoặc là giá trị tuyệt đối thông thường trên $\mathbb{Q}$ hoặc là giá trị tuyệt đối p-adic với p là một số nguyên tố nào đó.

Bài tập 4.11 (Công thức tích)**.** Cho $x \in \mathbb{Q} - \{0\}$. Chứng minh rằng

$$\prod_{p \leqslant \infty} |x|_p = 1$$

trong đó $p \leqslant \infty$ nghĩa là tích được lấy trên toàn bộ các số nguyên tố của $\mathbb{Q}$, bao gồm cả ∞ (ở đây $|\quad|_\infty$ là giá trị tuyệt đối thông thường).

Định nghĩa 4.15. Cho k là một trường và $|\quad|$ là một giá trị tuyệt đối trên k.

- Một dãy các phần tử $x_n \in k$ được gọi là **một dãy Cauchy** nếu với mọi $\varepsilon > 0$, tồn tại $M > 0$ sao cho $|x_n - x_m| < \varepsilon$ với mọi $n, m \geqslant M$.
- Trường k được gọi là **đầy đủ** tương ứng với giá trị tuyệt đối $|\quad|$ nếu mọi dãy Cauchy của k đều hội tụ trong k.
- Một tập con $S \subset k$ được gọi là **trù mật** trong k nếu với mọi $x \in k$ và $\varepsilon > 0$ ta có
$$B(x, \varepsilon) \cap S \neq \emptyset.$$

Bài tập 4.12. Chứng minh rằng $\mathbb{R}$ là một trường đầy đủ, $\mathbb{Q}$ là tập con trù mật của $\mathbb{R}$ (tương ứng với giá trị tuyệt đối thông thường).

Bài tập 4.13. Chứng minh rằng $\mathbb{Q}$ không phải là một trường đầy đủ với bất kì giá trị tuyệt đối không tầm thường nào.

Bài tập 4.14. Cho p là một số nguyên tố. Ta kí hiệu $\mathcal{C}_p(\mathbb{Q})$ là tập hợp tất cả các dãy Cauchy (tương ứng với giá trị tuyệt đối p-adic) của $\mathbb{Q}$. Trên $\mathcal{C}_p(\mathbb{Q})$ ta trang bị hai phép toán như sau:

$$(x_n) + (y_n) = (x_n + y_n),$$

$$(x_n).(y_n) = (x_n.y_n).$$

Chứng minh rằng với 2 phép toán trên $\mathcal{C}_p(\mathbb{Q})$ là một vành giao hoán có đơn vị.

Bài tập 4.15. Hãy tìm 2 dãy Cauchy (tương ứng với giá trị tuyệt đối p-adic nào đó) khác dãy 0 mà tích của chúng là dãy gồm duy nhất phần tử 0.

Bài tập 4.16. Ta ký kiệu $\mathcal{N}$ là tập hợp con của $\mathcal{C}_p(\mathbb{Q})$ gồm các dãy Cauchy tiến đến 0.

$$\mathcal{N} := \{(x_n) : \lim_{n\to\infty} |x_n|_p = 0\}.$$

Ta xét tập hợp $\mathbb{Q}_p$ trong đó các phần tử của nó là các tập hợp có dạng

$$(x_n) + \mathcal{N}.$$

Trên $\mathbb{Q}_p$ ta xây dựng hai phép toán sau

$$((x_n) + \mathcal{N}) + ((y_n) + \mathcal{N}) = (x_n + y_n) + \mathcal{N},$$

$$((x_n) + \mathcal{N}).((y_n) + \mathcal{N}) = (x_n.y_n) + \mathcal{N}.$$

Chứng minh rằng $\mathbb{Q}_p$ là một trường.

Bài tập 4.17. Cho $(x_n) \in \mathcal{C}_p(\mathbb{Q}) - \mathcal{N}$. Chứng minh rằng tồn tại $N > 0$ sao cho $|x_n|_p = |x_m|_p$ với mọi $n, m \geqslant N$.

Theo bài tập trên ta có nếu $(x_n) \in \mathcal{C}_p(\mathbb{Q})$ thì dãy $|x_n|_p$ hội tụ trên $\mathbb{R}$. Ta có thể viết $\lim_{n\to\infty} |x_n|_p$.

Bài tập 4.18. Chứng minh rằng nếu $(y_n) \in (x_n) + \mathcal{N}$ thì $\lim_{n\to\infty} |y_n|_p = \lim_{n\to\infty} |x_n|_p$. Từ đó ta có thể định nghĩa được giá trị p-adic cho các phần tử $\lambda = (x_n) + \mathcal{N} \in \mathbb{Q}_p$ như sau

$$|\lambda|_p = \lim_{n\to\infty} |x_n|_p.$$

Bài tập 4.19. Chứng minh rằng giá trị p-adic được định nghĩa như ở bài trên là một giá trị tuyệt đối trên $\mathbb{Q}_p$.

Bài tập 4.20. Với mỗi $x \in \mathbb{Q}$, ta đồng nhất nó với phần tử $(x) + \mathcal{N}$ của $\mathbb{Q}_p$ (ở đây (x) là dãy gồm toàn các phần tử có giá trị là x). Chứng minh rằng $\mathbb{Q}$ trù mật trong $\mathbb{Q}_p$ (tương ứng với giá trị tuyệt đối bài trên).

Bài tập 4.21. Chứng minh rằng $\mathbb{Q}_p$ là trường đầy đủ tương ứng với giá trị tuyệt đối ở bài trên.

Định nghĩa 4.16. Vành các số nguyên p-adic là

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leqslant 1\}.$$

Bài tập 4.22. Chứng minh rằng với mọi $x \in \mathbb{Z}_p$, luôn tồn tại một dãy Cauchy (α_n) hội tụ tới x có tính chất sau:

- $\alpha_n \in \mathbb{Z}$ thỏa mãn $0 \leqslant \alpha_n \leqslant p^n - 1$,
- Với mọi n ta có $\alpha_n \simeq \alpha_{n-1} \mod p^{n-1}$.

Hơn nữa dãy thỏa mãn tính chất trên là duy nhất.

Bài tập 4.23. Chứng minh rằng mọi phần tử $x \in \mathbb{Z}_p$ đều có thể viết dưới dạng

$$x = b_0 + b_1 p + b_2 p^2 + \cdots + b_n p^n + \ldots$$

với $0 \leqslant b_i \leqslant p - 1$ và cách viết trên là duy nhất.

Bài tập 4.24. Chứng minh rằng mọi dãy x_n với $x_n \in \mathbb{Z}_p$ đều có thể trích ra được một dãy con hội tụ. Hay nói một cách khác $\mathbb{Z}_p$ là compact dãy.

Bài tập 4.25. Cho p là số nguyên tố lẻ. Chứng minh rằng $\sqrt{2} \in \mathbb{Z}_p$ khi và chỉ khi p có dạng $8k \pm 1$.

Bài tập 4.26. Cho k là một số nguyên dương. Chứng minh rằng $\sqrt{k} \in \mathbb{Z}_2$ khi và chỉ khi k có dạng $4^a(8b + 1)$.

CHƯƠNG 5

Xấp xỉ số thực bằng số hữu tỉ

5.1 Xấp xỉ số thực bằng số hữu tỉ

Cho $\alpha \in \mathbb{R}$ là một số thực, ta biết rằng có thể tìm các số hữu tỉ $\frac{p}{q}$ gần α một cách tuỳ ý, nói một cách khác có thể làm nhỏ tuỳ ý đại lượng

$$\left|\alpha - \frac{p}{q}\right|.$$

Một vấn đề xảy ra là khi ta cố gắng làm cho số hữu tỉ $\frac{p}{q}$ tiến gần đến α thì chúng ta cũng có thể phải làm cho tử và mẫu số p, q ngày càng lớn. Một câu hỏi được đặt ra là khi ta xấp xỉ α bởi các số hữu tỉ có mẫu số không quá lớn thì xấp xỉ đó sẽ tốt đến mức độ nào?

(Do khi biểu diễn một số hữu tỉ dưới dạng $\frac{p}{q}$ ta luôn có thể để cho mẫu số q là một số nguyên dương, nên trong các phần tiếp theo nếu ta không giải thích gì thêm thì mẫu số của một số hữu tỉ sẽ luôn là một số nguyên dương.)

Xét trường hợp $\alpha = \frac{m}{n} \in \mathbb{Q}$ là một số hữu tỉ. Một điều hiển nhiên là α có thể được xấp xỉ một cách chính xác bởi chính nó. Vậy nếu muốn xấp xỉ nó bằng các số hữu tỉ khác thì sao?

Với mọi số hữu tỉ $\frac{p}{q} \neq \frac{m}{n}$ (ta có thể yêu cấu rằng q là một số nguyên dương) ta luôn có

$$\left|\frac{m}{n} - \frac{p}{q}\right| = \left|\frac{mq - np}{nq}\right| \geqslant \frac{1}{nq}.$$

Bất đẳng thức cuối cùng nhận được do $|mq - np|$ là một số nguyên dương.

Ta nhận thấy rằng cách duy nhất để có thể cho $\frac{p}{q}$ tiến gần đến α là cho q tiến đến ∞.

Tổng kết lại, trong trường hợp α là số hữu tỉ thì nó sẽ được xấp xỉ hoàn hảo bởi chính nó, nhưng dùng số hữu tỉ khác để xấp xỉ thì lại không được tốt.

Xét trường hợp α là số vô tỉ. Ta có kết quả sau:

Mệnh đề 5.1 (Dirichlet)**.** *Giả sử α là một số vô tỉ. Khi đó tồn tại vô số số hữu tỉ $\frac{p}{q}$ sao cho*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{5.1}$$

Chứng minh. Cố định một số nguyên dương n. Ta xét $n+1$ số dạng $i\alpha - [i\alpha]$ với $i \in \{0, 1, \ldots, n\}$: các số này thuộc $[0;1)$. Mặt khác $[0;1)$ có thể phân hoạch thành n bán khoảng như sau

$$[0;1) = \left[0; \frac{1}{n}\right) \cup \left[\frac{1}{n}; \frac{2}{n}\right) \cup \ldots \cup \left[\frac{n-1}{n}; 1\right).$$

Do đó, theo nguyên lý Dirichlet, tồn tại hai số $0 \leqslant i < j \leqslant n$ sao cho $i\alpha - [i\alpha]$ và $j\alpha - [j\alpha]$ cùng thuộc một bán khoảng $\left[\frac{k}{n}; \frac{k+1}{n}\right)$, với $0 \leqslant k < n$ nào đó. Ta có

$$|(i-j)\alpha - [i\alpha] + [j\alpha]| < \frac{1}{n}.$$

Chọn $p = [i\alpha] - [j\alpha]$ và $q = j - i$ thì p, q là các số nguyên, trong đó $q > 0$ và thoả mãn

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{nq} \leqslant \frac{1}{q^2}.$$

Bây giờ ta chứng minh có vô hạn số $\frac{p}{q}$ như vậy. Theo trên, với mỗi số nguyên dương n, tồn tại các số nguyên p_n, q_n trong đó $q_n \leqslant n$ sao cho

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{nq_n} \leqslant \frac{1}{q_n^2}.$$

Với mọi $n \in \mathbb{N}$ ta luôn có thể chọn được $N > n$ đủ lớn sao cho $|q_N\alpha - p_N| > \frac{1}{N}$ (do α là số vô tỉ nên ta luôn có $q_N\alpha - p_N \neq 0$). Khi đó hai

phân số $\frac{p_N}{q_N}$ và $\frac{p_n}{q_n}$ là khác nhau. Thật vậy, giả sử phản chứng ta có

$$\left|\alpha - \frac{p_n}{q_n}\right| = \left|\alpha - \frac{p_N}{q_N}\right| \leqslant \frac{1}{N^2}.$$

Nhân cả hai vế bất đẳng thức với $q_n > 0$ ta được $|p_n\alpha - q_n| \leqslant \frac{q_n}{N^2} < \frac{1}{N}$ (mâu thuẫn với điều kiện chọn N). □

Trong các phần tiếp theo chúng ta sẽ trình bày cách tiếp cận bài toán xấp xỉ bằng các số hữu tỉ một cách có hệ thống hơn.

5.2 Dãy số Farey

Với mỗi số thực α ta cho tương ứng với một tia có gốc là $(0, 0)$ và hệ số góc là α (tia này được gọi là tia α). Số hữu tỉ $\frac{m}{n}$ tương ứng với tia $\frac{m}{n}$; tia này đi qua điểm có toạ độ (n, m). Một tia tương ứng với số hữu tỉ ta gọi là **tia hữu tỉ**.

Lúc này bài toán xấp xỉ số thực α bởi các số hữu tỉ được đưa về việc xác định các tia hữu tỉ gần với tia cα. Khi α là một số thực dương thì tia α luôn được chứa trong hình vuông $n \times n$ nằm trong góc phần tư thứ nhất và có đỉnh là gốc toạ độ; hai cạnh nằm trên hai trục toạ độ (với $\alpha < 0$ thì tia α luôn nằm trong hình vuông $n \times n$ đối xứng với hình vuông này qua trục tung). Để biết được tia hữu tỉ nào gần với tia α ta cần biết các tia hữu tỉ đi qua điểm nằm trong hoặc trên các hình vuông vừa được nhắc đến. Ta thu được dãy số Farey sau:

Bậc									
1	$\frac{0}{1}$				$\frac{1}{1}$				$\frac{1}{0}$
2	$\frac{0}{1}$		$\frac{1}{2}$		$\frac{1}{1}$		$\frac{2}{1}$		$\frac{1}{0}$
3	$\frac{0}{1}$	$\frac{1}{3}$	$\frac{1}{2}$	$\frac{2}{3}$	$\frac{1}{1}$	$\frac{3}{2}$	$\frac{2}{1}$	$\frac{3}{1}$	$\frac{1}{0}$

Ta nhận thấy dãy Farey có quy luật sau:

- Nếu ở dòng thứ $N+1$ xuất hiện $\dfrac{p}{q}$ không có trong dòng thứ N và nếu
$$\frac{p_i}{q_i} < \frac{p}{q} < \frac{p_{i+1}}{q_{i+1}}$$
trong đó $\dfrac{p_i}{q_i}$ và $\dfrac{p_{i+1}}{q_{i+1}}$ là hai số liên tiếp ở dòng thứ N, thì $p = p_i + p_{i+1}$ và $q = q_i + q_{i+1}$.

- Với mỗi số nguyên dương N, dãy Farey bậc N, kí hiệu $\mathcal{F}_N$, là tập tất cả các phân số tối giản có dạng $\dfrac{p}{q}$ trong đó $0 \leqslant p \leqslant q \leqslant N$ được sắp xếp tăng dần. Chẳng hạn
$$\mathcal{F}_3 = \left\{\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}\right\}.$$

- Nếu $\dfrac{p_i}{q_i}$ và $\dfrac{p_{i+1}}{q_{i+1}}$ là hai phân số liên tiếp của một dãy Farey bậc N thì diện tích tam giác tạo bởi 3 điểm $(0,0)$, (q_i, p_i) và (q_{i+1}, p_{i+1}) bằng $\dfrac{1}{2}$.

Trong hình vuông $N \times N$, giả sử rằng tia α nằm giữa tia $\dfrac{p_i}{q_i}$ và tia $\dfrac{p_{i+1}}{q_{i+1}}$ với $\dfrac{p_i}{q_i} < \dfrac{p_{i+1}}{q_{i+1}}$ là hai số liên tiếp trong $\mathcal{F}_N$; điều này tương đương với
$$\frac{p_i}{q_i} < \alpha < \frac{p_{i+1}}{q_{i+1}}.$$

Lúc này tia α đi qua miền trong của hình bình hành tạo bởi 4 điểm $(0,0)$, (q_i, p_i), (q_{i+1}, p_{i+1}) và $(q_i+q_{i+1}, p_i+p_{i+1})$ (để ý rằng tia $\dfrac{p_i + p_{i+1}}{q_i + q_{i+1}}$ cũng nằm giữa 2 tia $\dfrac{p_i}{q_i}$ và tia $\dfrac{p_{i+1}}{q_{i+1}}$). Do đó hoặc α nằm giữa $\dfrac{p_i}{q_i}$ và $\dfrac{p_i + p_{i+1}}{q_i + q_{i+1}}$ hoặc nằm giữa $\dfrac{p_i + p_{i+1}}{q_i + q_{i+1}}$ và $\dfrac{p_{i+1}}{q_{i+1}}$. Giả sử α nằm giữa $\dfrac{p_i}{q_i}$ và $\dfrac{p_i + p_{i+1}}{q_i + q_{i+1}}$. Khi đó
$$\left|\alpha - \frac{p_i}{q_i}\right| < \left|\frac{p_i + p_{i+1}}{q_i + q_{i+1}} - \frac{p_i}{q_i}\right| = \frac{1}{q_i(q_i + q_{i+1})} < \frac{1}{Nq_i}.$$
Bất đẳng thức cuối nhận được do $\dfrac{p_i + p_{i+1}}{q_i + q_{i+1}} \notin \mathcal{F}_N \implies q_i + q_{i+1} > N$.

Định lý 5.2 (Hurwitz)**.** *Với mọi số vô tỉ α, tồn tại vô hạn số hữu tỉ $\frac{p}{q}$, với $(p,q)=1$ sao cho*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}. \tag{5.2}$$

Chứng minh. Giả sử $\frac{a}{b}$ và $\frac{c}{d}$ là hai phân số liên tiếp trong dãy Farey bậc N và $\frac{a}{b} < \alpha < \frac{c}{d}$. Khi đó $\frac{a}{b}, \frac{a+c}{b+d}, \frac{c}{d}$ là các phân số liên tiếp trong $\mathcal{F}_{N+1}$. Không mất tính tổng quát, giả sử rằng

$$\frac{a}{b} < \alpha < \frac{a+c}{b+d}.$$

Ta giả sử phản chứng rằng định lý Hurwitz là sai, khi đó ta có với N đủ lớn

$$\begin{cases} \alpha - \frac{a}{b} \geqslant & \frac{1}{b^2\sqrt{5}} \\ \frac{c}{d} - \alpha \geqslant & \frac{1}{d^2\sqrt{5}} \\ \frac{a+c}{b+d} - \alpha \geqslant & \frac{1}{(b+d)^2\sqrt{5}}. \end{cases}$$

Cộng hai bất đẳng thức đầu tiên cho ta

$$\frac{c}{d} - \frac{a}{b} \geqslant \frac{1}{\sqrt{5}}\left(\frac{1}{b^2} + \frac{1}{d^2}\right).$$

Do $\frac{a}{b}, \frac{c}{d}$ là hai phân số liên tiếp nên $bc - ad = 1$. Vậy

$$b^2 - bd\sqrt{5} + d^2 \leqslant 0.$$

Điều này suy ra

$$\overline{\phi} < \frac{b}{d} < \phi$$

trong đó $\phi = \frac{1+\sqrt{5}}{2}$ và $\overline{\phi} = \frac{\sqrt{5}-1}{2}$ là hai nghiệm của phương trình $X^2 - \sqrt{5}X + 1 = 0$. Vì $1 + \overline{\phi} = \phi$ nên khi cộng các vế bất đẳng thức trên với 1 ta thu được

$$\phi < \frac{b+d}{d} \tag{5.3}$$

Mặt khác, cộng bất đẳng thức thứ hai và thứ ba rồi lập luận tương tự cho ta

$$\overline{\phi} < \frac{b+d}{d} < \phi.$$

Điều này mâu thuẫn với (5.3).

Nhận xét. Hằng số $\sqrt{5}$ trong (5.1) là tốt nhất theo nghĩa: Tồn tại số vô tỉ α sao cho với mọi số dương $A > \sqrt{5}$ thì chỉ có hữu hạn phân số hữu tỉ $\frac{p}{q}$ thoả mãn

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{Aq^2}.$$

Để xây dựng số vô tỉ α ta xét dãy các tia được định nghĩa như sau:

- Tia t_{-1} đi qua điểm $v_{-1} = (1, 0)$.
- Tia t_0 đi qua điểm $v_0 = (0, 1)$.
- Tia t_{i+2} đi qua điểm $v_{i+2} = v_i + v_{i+1}$ với mọi $i \geqslant -1$.

(Chú ý: việc xây dựng các điểm tiếp theo là tổng của hai điểm được định nghĩa trước đó, xuất phát từ việc xây dựng hình bình hành có 4 đỉnh là $(0, 0)$, v_i, v_{i+1} và $v_i + v_{i+1}$ như trong cách xấp xỉ một số thực bằng dãy Farey.)

Gọi (x_i, y_i) là tọa độ của các điểm v_i, khi đó bằng quy nạp ta có thể thấy rằng với mọi $i \geqslant 0$, x_i và y_i tương ứng là phần tử thứ i và thứ $i+1$ của dãy Fibonacci cho bởi $f_0 = 0, f_1 = 1$ và $f_{n+2} = f_{n+1} + f_n$.

Công thức tổng quát cho phần tử thứ n của dãy Fibonacci là (có thể chứng minh bằng phương pháp quy nạp theo n):

$$f_n = \frac{\phi^n - (-\overline{\phi})^n}{\sqrt{5}} \quad \text{với mọi } n \geqslant 0. \tag{5.4}$$

Do đó

$$f_n\phi - f_{n+1} = (-1)^{n+1}\overline{\phi}^n = \frac{(-1)^{n+1}}{\phi^n}.$$

Điều này dẫn đến

$$\left|\phi - \frac{f_{n+1}}{f_n}\right| = \frac{1}{\phi^n f_n}.$$

Vế phải của đẳng thức tiến đến 0 khi n tiến ra vô cùng, nên các tia t_n sẽ tiến gần đến tia ϕ khi n tiến ra vô cùng.

Ta sẽ lấy $\alpha = \phi$. Giả sử A là một số thực dương sao cho có vô hạn số hữu tỉ $\frac{p}{q}$ thỏa mãn

$$\left|\phi - \frac{p}{q}\right| < \frac{1}{Aq^2}. \tag{5.5}$$

Do ϕ và $-\overline{\phi}$ là 2 nghiệm phân biệt của phương trình $x^2 - x - 1 = 0$ nên với mọi $\frac{p}{q}$ ta có

$$\left|\frac{p}{q} - \phi\right| \left|\frac{p}{q} + \overline{\phi}\right| = \left|\frac{p^2}{q^2} - \frac{p}{q} - 1\right| = \frac{1}{q^2}|p^2 - pq - q^2| \tag{5.6}$$

Vế trái của (5.6) khác 0 do cả ϕ và $\overline{\phi}$ đều là các số vô tỉ, nên vế phải của nó cũng phải là một số khác 0. Vì thế $|p^2 - pq - q^2| \geqslant 1$ và ta có

$$\left|\frac{p}{q} - \phi\right| \left|\frac{p}{q} + \overline{\phi}\right| \geqslant \frac{1}{q^2}. \tag{5.7}$$

Giả sử ta có dãy vô hạn các số hữu tỉ $\frac{p_i}{q_i}$, với $q_i > 0$ thỏa mãn điều kiện (5.5), hay

$$\left|\phi - \frac{p_i}{q_i}\right| \leqslant \frac{1}{Aq_i^2}. \tag{5.8}$$

Khi đó $q_i\phi - \frac{1}{Aq_i} < p_i < q_i\phi + \frac{1}{Aq_i}$, và điều này kéo theo rằng với q_i cho trước ta chỉ có hữu hạn các số p_i để cho số hữu tỉ $\frac{p_i}{q_i}$ thỏa mãn điều kiện (5.5). Do đó q_i sẽ phải tiến tới ∞ khi i tiến tới ∞.

Kết hợp (5.6), (5.7) và bất đẳng thức tam giác ta thu được

$$\frac{1}{q_i^2} \leqslant \left|\frac{p_i}{q_i} - \phi\right| \left|\frac{p_i}{q_i} + \overline{\phi}\right| = \left|\frac{p_i}{q_i} - \phi\right| \left|\frac{p_i}{q_i} - \phi + \sqrt{5}\right| < \frac{1}{Aq_i^2}\left(\frac{1}{Aq_i^2} + \sqrt{5}\right)$$

hay

$$A < \frac{1}{Aq_i^2} + \sqrt{5}$$

và vì thế

$$A \leqslant \lim_{i\to\infty}\left(\frac{1}{Aq_i^2} + \sqrt{5}\right) = \sqrt{5}.$$

□

5.3 Liên phân số

Trong phần này chúng ta tiếp cận với một cách khác để có thể xấp xỉ một số thực bằng các số hữu tỉ. Ý tưởng của phương pháp này xuất phát từ thuật toán Euclid.

Cho hai số nguyên a, b với $b > 0$, ta thực hiện thuật toán Euclid như sau: ta lấy a đem chia cho b được thương là a_0, dư là r_0 với $0 \leqslant r_0 < b$. Nếu $r_0 > 0$ ta thực hiện phép chia có dư b cho r_0, được dư r_1. Cứ thế, nếu bước thứ i ta nhận được số dư r_{i+1} mà khác 0 thì ta thực hiện phép chia có dư r_i cho r_{i+1} để được dư r_{i+2}. Thuật toán sẽ dừng lại khi phần dư của phép chia bằng 0. Trong trường hợp a và b là hai số nguyên tố cùng nhau, thuật toán chi Euclid cho chúng ta dãy các đẳng thức sau:

$$\begin{aligned}
a &= a_0 b + r_0 \\
b &= a_1 r_0 + r_1 \\
r_0 &= a_2 r_1 + r_2 \\
r_1 &= a_3 r_2 + r_3 \\
&\vdots \\
r_{k-3} &= a_{k-1} r_{k-2} + 1 \\
r_{k-2} &= a_k.
\end{aligned}$$

Ta có

$$\frac{a}{b} = a_0 + \frac{r_0}{b} = a_0 + \frac{1}{a_1 + \dfrac{r_0}{r_1}} = \cdots = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots \cfrac{1}{a_k}}}}}} \tag{5.9}$$

Một biểu diễn có dạng như trên được gọi là một biểu diễn liên phân số của $\dfrac{a}{b}$. Ta để ý rằng $a_0 = \left\lfloor \dfrac{a}{b} \right\rfloor$, $a_1 = \left\lfloor \dfrac{b}{r_0} \right\rfloor$ và $a_j = \left\lfloor \dfrac{r_{j-2}}{r_{j-1}} \right\rfloor$ với mỗi $j = 2, 3, \ldots, k$.

Cho α là một số thực bất kì.

- Nếu α là một số hữu tỉ, ta luôn tìm được hai số nguyên a, b nguyên tố cùng nhau và $b > 0$ sao cho $\alpha = \frac{a}{b}$. Thuật toán Euclid ở trên cho phép ta tìm được dạng liên phân số của α.

- Nếu α là một số vô tỉ, ta không thể dùng phép chia Euclid ở đây, tuy nhiên việc xác định các giá trị $a_0, a_i, \ldots, a_i$ như là phần nguyên của một số thực vẫn có thể làm được. Cụ thể như sau: Ta lấy $a_0 = \lfloor \alpha \rfloor$, khi đó $\alpha = a_0 + \dfrac{1}{\alpha_1}$. với $\alpha_1 > 1$ là một số vô tỉ. Ta lại lấy $a_1 = \lfloor \alpha_1 \rfloor$ và viết $\alpha_1 = a_1 + \dfrac{1}{\alpha_2}$. Cứ tiếp tục như vậy ta xây dựng được một dãy các số nguyên a_k và các số vô tỉ α_k bằng công thức truy hồi như sau:

$$\begin{cases} a_k = \lfloor \alpha_k \rfloor \\ \alpha_{k+1} = \dfrac{1}{\alpha_k - a_k}. \end{cases}$$

(Do α_k là số vô tỉ và a_k là số nguyên nên $\alpha_k - a_k \neq 0$; điều này cho phép định nghĩa phía trên của chúng ta là có nghĩa.) Đặt

$$r_n = \langle a_0, \ldots, a_n \rangle := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots \cfrac{1}{a_n}}}}}}.$$

Do a_0 là các số nguyên và $a_i \geqslant 1$ với mọi $i \geqslant 1$ nên dãy r_n hội tụ đến α (xem Bài tập 5.4). Ta thu được biểu diễn liên phân số (vô hạn) của số vô tỉ α

$$\alpha = \langle a_0, a_1, \ldots \rangle = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}}. \tag{5.10}$$

Các số r_n được gọi là **xấp xỉ thứ** n của α.

Ví dụ 5.3. *Ta có*

$$\frac{1+\sqrt{5}}{2} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\ddots}}}}}.$$

Liên phân số cho phép người ta tìm được "xấp xỉ tốt nhất" của α. Giả sử $\dfrac{p_n}{q_n}$ là phân số tối giản của xấp xỉ thứ n của α khi đó ta có các tính chất sau:

1. **Với mọi $n \geqslant 0$ ta luôn có $|\alpha q_n - p_n| > |\alpha q_{n+1} - p_{n+1}|$.**
2. **Với mọi $n \geqslant 0$ ta có $\left|\alpha - \dfrac{p_n}{q_n}\right| < \dfrac{1}{2q_n^2}$.**
3. **Nếu $\dfrac{p}{q}$ thoả mãn $\left|\alpha - \dfrac{p}{q}\right| < \dfrac{1}{2q^2}$ thì $\dfrac{p}{q}$ phải là phần tử của dãy (r_n).**
4. **Trong 3 phân số liên tiếp $\dfrac{p_n}{q_n}$, $\dfrac{p_{n+1}}{q_{n+1}}$, $\dfrac{p_{n+2}}{q_{n+2}}$ luôn có ít nhất một phân số $\dfrac{p}{q}$ mà**

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

Hơn nữa số $\sqrt{5}$ không thể làm tốt hơn được. Điều này cho chúng ta một chứng minh khác của định lý Hurwitz.

Nhận xét 5.4. ***Xấp xỉ một số thực bằng dãy Farey và bằng sử dụng liên phân số khác giống nhau.*** *Khi sử dụng liên phân số, để tìm một tia hữu tỉ mới tiến gần đến tia α, thay vì chúng ta xây dựng các hình bình hành với đỉnh thuộc vào các tia đã biết, thi ta sử dụng các a_i. Cách xây dựng này cho phép ta tiến gần tia α nhanh hơn cách của dựng hình bình hành. Cụ thể như sau (với α là một số thực dương):*

- *Vẫn giống như khi làm việc với dãy Farey, ta khởi đầu với 2 tia gốc tại $(0,0)$ tương ứng đi qua điểm $v_0 = (0,1)$ và đi qua điểm $v_1 = (1,0)$.*

- *Sự khác biệt bắt đầu từ bước này. Đối với dãy Farey ta sẽ lấy tia đi qua điểm $u_2 = v_0 + v_1$ là đỉnh còn lại của hình bình hành có 4 đỉnh là $(0,0)$, v_0, v_1. Đối với liên phân số, ta sẽ lấy $a_0 = \lfloor \alpha \rfloor$, sau đó xét tia đi qua điểm $v_2 = v_0 + a_0 v_1$.*
- *Tiếp theo tùy thuộc vào việc tia α nằm giữa 2 tia nào để xây dựng tiếp.*

Ngoài việc sử dụng liên phân số để xấp xỉ một số thực bất kì bằng các số hữu tỉ, nó còn có nhiều ứng dụng khác chẳng hạn như tìm nghiệm của một phương trình Pell $x^2 - dy^2 = 1$ với d là một số nguyên dương lớn hơn 1 và không có ước chính phương khác 1. Giả sử (x, y) là một nghiệm cua phương trình Pell, khi đó $\frac{x}{y}$ có thể xem như là một xấp xỉ của số vô tỉ $\sqrt{d}$. Vậy để tìm $\frac{x}{y}$ ta sẽ đi tìm phân số liên tục của $\sqrt{d}$.

Để kết thúc bài giảng, chúng ta sẽ nhắc đến một định lý quan trọng cho thấy liên phân số là một công cụ tốt để nghiên cứu các số vô tỉ bậc hai. (Một số vô tỉ α được gọi là vô tỉ bậc 2 nếu nó là nghiệm của một phương trình bậc 2 với hệ số hữu tỉ).

Định nghĩa 5.5. Ta nói một liên phân số $\langle a_0, a_1, \ldots \rangle$ là **tuần hoàn** nếu tồn tại một số nguyên dương $r > 0$ sao cho $a_{n+r} = a_n$ với mọi n đủ lớn nào đó.

Định lý 5.6 (Euler-Lagrange)**.** *Khai triển liên phân số của một số vô tỉ α là tuần hoàn khi và chỉ khi α là số vô tỉ bậc hai.*

Bài tập về Liên phân số

Cho $x_0, x_1, \ldots, x_k, \ldots$ là các số thực với $x_i > 0$ với mọi $i \geqslant 1$. Ta xây dựng dãy các số thực $\{r_i\}$ và $\{h_i, k_i\}$ bằng quy nạp như sau:

$$r_0 = \langle x_0 \rangle := x_0,\ r_n = \langle x_0, x_1, \ldots, x_n \rangle := \left\langle x_0, x_1, \ldots, x_{n-1} + \frac{1}{x_n} \right\rangle \forall n \geqslant 1,$$

$$h_{-2} = 0,\ h_{-1} = 1,\ h_i = x_i h_{i-1} + h_{i-2} \quad \forall i \geqslant 0$$

và

$$k_{-2} = 1,\ k_{-1} = 0,\ k_i = x_i k_{i-1} + k_{i-2} \quad \forall i \geqslant 0.$$

- Các $\langle x_0, x_1, \ldots, x_n \rangle$ được định nghĩa như trên, được gọi là một **liên phân số** có độ dài n dùng để biểu thị số thực r_n. Chúng được gọi chung là các **liên phân số hữu hạn**.
- Một liên phân số được gọi là **đơn giản** nếu các số x_i xây dựng nên nó đều là các số nguyên.

Bài tập 5.1. Cho $\langle a_0, a_1, \ldots, a_n \rangle$ và $\langle b_0, b_1, \ldots, b_m \rangle$ là hai liên phân số hữu hạn và đơn giản với a_n và b_m là các số lớn hơn 1. Chứng minh rằng nếu

$$\langle a_0, a_1, \ldots, a_n \rangle = \langle b_0, b_1, \ldots, b_m \rangle$$

thì $n = m$ và $a_i = b_i$ với mọi i chạy từ 0 đến n.

Bài tập 5.2. Chứng minh rằng mọi liên phân số hữu hạn đều là biểu thị của một số hữu tỉ. Ngược lại mọi số hữu tỉ đều có thể được biểu thị bởi một liên phân số hữu hạn. Hơn nữa mỗi một số hữu tỉ có đúng 2 cách biểu thị bằng liên phân số.

Bài tập 5.3. Chứng minh rằng:

- $r_i = \frac{h_i}{k_i}, \forall i \geqslant 0.$

- $h_i k_{i-1} - h_{i-1} k_i = (-1)^{i-1}$ và $r_i - r_{i-1} = \frac{(-1)^{i-1}}{k_i k_{i-1}}$ với mọi $i \geqslant 1$.
- $h_i k_{i-2} - h_{i-2} k_i = (-1)^i x_i$ và $r_i - r_{i-2} = \frac{(-1)^i x_i}{k_i k_{i-2}}$ với mọi $i \geqslant 1$.

Bài tập 5.4. Giả sử rằng các số x_i là các số nguyên và $x_i > 0$ với mọi $i \geqslant 1$.

- Chứng minh rằng h_i/k_i là một phân số tối giản.
- Chứng minh rằng dãy r_n hội tụ. Hơn nữa ta có $r_{2k} < \lim_{i\to\infty} r_i < r_{2k+1}$ với mọi $k \in \mathbb{N}$.

Bài tập trên cho phép ta có định nghĩa sau: "Một dãy vô hạn các số nguyên $x_0, x_1, \ldots$, trong đó $x_i > 0$ với mọi $i \geqslant 1$, xác định một **liên phân số đơn giản có độ dài vô hạn** $\langle x_0, x_1, \ldots \rangle$. Giá trị của liên phân số đó được định nghĩa bởi $\lim_{n\to\infty} \langle x_0, \ldots, x_n \rangle$."

Bài tập 5.5. Chứng minh rằng giá trị của một liên phân số đơn giản có độ dài vô hạn là một số vô tỉ. Hơn nữa hai liên phân số đơn giản có độ dài vô hạn khác nhau thì có giá trị khác nhau. (Ta nói $\langle x_0, x_1, \ldots \rangle \neq \langle y_0, y_1, \ldots \rangle$ nếu tồn tại i sao cho $x_i \neq y_i$.)

Bài tập 5.6. Chứng minh rằng mọi số vô tỉ được biểu thị duy nhất bởi một liên phân số đơn giản có độ dài vô hạn.

Bài tập 5.7. Cho ξ là một số vô tỉ được biểu thị bởi liên phân số đơn giản có dộ dài vô hạn $\langle x_0, x_1, \ldots \rangle$. Cho a/b là một số hữu tỉ có mẫu số là một số nguyên dương. Chứng minh rằng nếu $|\xi b - a| < |\xi k_n - h_n|$ với mọi số nguyên dương n nào đó thì $b \geqslant k_{n+1}$.

Bài tập 5.8. Sử dụng kí hiệu của bài trước. Chứng minh rằng nếu số hữu tỉ a/b với $b \geqslant 1$ thỏa mãn tính chất

$$\left|\xi - \frac{a}{b}\right| < \frac{1}{2b^2}$$

thì tồn tại một số nguyên n sao cho $a/b = h_n/k_n$.

Bài tập 5.9. Sử dụng kí hiệu của bài trước. Chứng ming rằng với mọi $n \geqslant 0$ ta luôn có $\left|\xi - \frac{h_n}{k_n}\right| < \frac{1}{2k_n^2}$ hoặc $\left|\xi - \frac{h_{n+1}}{k_{n+1}}\right| < \frac{1}{2k_{n+1}^2}$.

Bài tập 5.10 (Định lý của Hurwitz)**.** Cho ξ là một số vô tỉ, chứng minh rằng tồn tại vô hạn số hữu tỉ h/k thỏa mãn tính chất

$$\left|\xi - \frac{h}{k}\right| < \frac{1}{\sqrt{5}k^2}.$$

Hơn nữa $\sqrt{5}$ là số tốt nhất (theo nghĩa nếu ta thay $\sqrt{5}$ bởi một số c lớn hơn, thì khẳng định trên không còn đúng nữa).

Một liên phân số đơn giản $\langle x_0, x_1, \dots \rangle$ có độ dài vô hạn được gọi là **có chu kỳ** nếu tồn tại một số nguyên dương n sao cho $x_r = x_{n+r}$ với mọi r đủ lớn. Một liên phân số đơn giản có độ dài vô hạn được gọi là **có chu kỳ thuần** nếu tồn tại số nguyên dương n sao cho $a_i = a_{i+n}$ với mọi $i \geqslant 0$.

Bài tập 5.11. Chứng minh rằng một số vô tỉ được biểu thị bởi một liên phân số đơn giản có độ dài vô hạn và có chu kỳ khi và chỉ khi nó có dạng $\frac{a+\sqrt{b}}{c}$ trong đó a, b, c là các số nguyên, $c \neq 0$ và $b > 0$ không phải là một số chính phương.

Bài tập 5.12. Chứng minh rằng số vô tỉ $\xi = \frac{a+\sqrt{b}}{c}$ được biểu thị bởi một liên phân số đơn giản có độ dài vô hạn và có chu kỳ thuần khi và chỉ khi $\xi > 1$ và $-1 < \xi' < 0$ trong đó $\xi' = \frac{a-\sqrt{b}}{c}$.

Bài tập 5.13. Cho d là một số nguyên dương không phải là số chính phương. Chứng minh rằng biểu thị liên phân số đơn giản của $\sqrt{d}$ có dạng

$$\sqrt{d} = \langle a_0, \overline{a_1, a_2, \dots, a_r, 2a_0} \rangle$$

với a_0 là phần nguyên của $\sqrt{d}$. Ở đây dấu gạch ngang trên đầu các số $a_1, a_2, \dots$ có nghĩa rằng khối các số đó được lặp lại vô hạn lần.

CHƯƠNG 6

Phương trình Pell

6.1 Phương trình Pell

Ta xét phương trình

$$x^2 - dy^2 = 1. \tag{6.1}$$

Chú ý rằng nếu (x_1, y_1) và (x_2, y_2) là nghiệm của (6.1) thì

$$1 = (x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = (x_1x_2 + dy_1y_2)^2 - d(x_1y_2 + x_2y_1)^2.$$

Do đó với $x_3 = x_1x_2 + dy_1y_2$ và $y_3 = x_1y_2 + x_2y_1$ thì (x_3, y_3) cũng là nghiệm của (6.1). Điều này cho phép ta định nghĩa một phép toán hai ngôi trên tập các nghiệm của phương trình (6.1) như sau:

$$(x_1, y_1) \times (x_2, y_2) := (x_1x_2 + dy_1y_2, x_1y_2 + x_2y_1).$$

Dễ kiểm tra thấy $\times$ có tính chất kết hợp, $(1, 0)$ là phần tử đơn vị và phần tử nghịch đảo của nghiệm (x, y) là nghiệm $(x, -y)$. Do đó tập nghiệm của phương trình Pell (6.1) có cấu trúc của một nhóm giao hoán.

Kể tử bây giờ ta giả sử $d > 0$ không phải là một số chính phương (điều này dẫn đến $\sqrt{d}$ là một số vô tỉ bậc 2). Giả sử (x, y) với $x, y > 0$ là một nghiệm của (6.1). Khi đó

$$\left|\frac{x}{y} - \sqrt{d}\right| = \frac{1}{y(x + y\sqrt{d})} < \frac{1}{2y^2}.$$

Theo tính chất của liên phân số, $\dfrac{x}{y}$ phải nằm trong dãy các xấp xỉ $r_n = \dfrac{p_n}{q_n}$ của $\sqrt{d}$. Do đó để tìm nghiệm của (6.1), ta chỉ cần xét các xấp xỉ $\dfrac{p_n}{q_n}$ được

xây dựng từ khai triển liên phân số của $\sqrt{d}$. Theo định lý của Lagrange, ta biết rằng khai triển liên phân số của $\sqrt{d}$ là tuần hoàn. Gọi ℓ là chu kỳ của khai triển, khi đó:

- nếu ℓ chẵn thì $(p_{\ell-1}, q_{\ell-1})$ là nghiệm của phương trình;
- nếu ℓ lẻ thì $(p_{2\ell-1}, q_{2\ell-1})$ là nghiệm của phương trình.

Từ nghiệm vừa tìm được, cùng với cấu trúc nhóm giao hoán của tập nghiệm, ta hoàn toàn có thể tìm được tất cả các nghiệm còn lại của phương trình.

6.2 Phương trình $x^2 + dy^2 = n$

Trong phần này chúng ta sẽ trình bày thuật toán Cornacchia dùng để tìm nghiệm nguyên của phương trình

$$x^2 + dy^2 = n \tag{6.2}$$

trong đó d, n là các số tự nhiên. Giả sử (x, y) là nghiệm của phương trình khi đó dựa vào đánh giá bất đẳng thức ta có $x^2 \leqslant n$ và $y^2 \leqslant n$. Do đó với n cho trước phương trình chỉ có hữu hạn nghiệm (x, y) và các nghiệm này thỏa mãn tính chất $x, y \leqslant \sqrt{n}$.

Thuật toán sau cho phép ta đi tìm nghiệm nguyên thủy (các nghiệm (x, y) thỏa mãn tính chất $\text{UCLN}(x, y) = 1$) của phương trình trên:

- Bước 1: Giải phương trình đồng dư

$$x^2 \equiv -d \mod n.$$

- Bước 2: Giả sử $r_1 \leqslant \frac{n}{2}$ là nghiệm của phương trình đồng dư trên. Sử dụng thuật toán Euclid để tìm

$$\begin{cases} r_2 & \equiv n \mod r_1 \\ r_3 & \equiv r_1 \mod r_2 \\ r_{i+2} & \equiv r_i \mod r_{i+1} \, \forall i \geqslant 1. \end{cases}$$

  Cụ thể hơn r_2 chính là phần dư của phép chia Euclid của n cho r_1, r_3 chính là phần dư của phép chia Euclid của r_1 cho r_2, với mọi $i \geqslant 1$ thì r_{i+2} chính là phần dư của phép chua Euclid của r_i cho r_{i+1}. Chúng ta sẽ dừng lại khi tìm được $r_k^2 < n \leqslant r_{k-1}^2$.

- Bước 3: Nếu $\dfrac{n - r_k^2}{d} = s^2$ với s là một số nguyên dương, khi đó $(x, y) = (r_k, s)$ là nghiệm của phương trình $x^2 + dy^2 = n$.

Nhược điểm của thuật toán này là ta không biết được phương trình có nghiệm hay không.

Đối với việc giải một phương trình Điôphăng bậc 2 hai biến (x, y) $f(x, y) = 0$ với f là một đa thức bậc 2 có hệ số nguyên (hay thậm chí nhiều biến hơn). Bằng việc sử dụng các biến đổi tuyến tính ta có thể quy về việc giải các phương trình Pell tổng quát $ax^2 + by^2 = n$ (khi $a.b < 0$ phương trình này cư xử rất giống với phương trình $x^2 - dy^2 = n$; khi $ab > 0$ thì nó lại cư xử khá giống với phương trình $x^2 + dy^2 = n$). Do đó việc sử dụng một cách linh hoạt liên phân số hoặc thuật toán Cornacchia sẽ giúp ta có thể giải được những bài giải phương trình Điôphăng bậc 2. Tóm lại để giải phương trình nghiệm nguyên bậc 2 ta sẽ thông qua hai bước sau:

- Giải phương trình đồng dư.
- Thuật toán Euclid / Phân số liên tục.

Dưới đây là một ví dụ cho cách tiếp cận này.

Định lý 6.1 (Fermat)**.** *Cho p là số nguyên tố lẻ. Khi đó p là tổng của hai số chính phương $p = x^2 + y^2$ khi và chỉ khi $p \equiv 1 \pmod 4$.*

Chứng minh. • Bước đồng dư:

Giả sử $p = x^2 + y^2$ với x, y là hai số tự nhiên nào đó. Do p là số nguyên tố nên $\text{UCLN}(x, y) = 1$ và $x, y \in \mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$. Vì thế la luôn có thể chọn được a sao cho $x \equiv ya \pmod p$. Bình phương cả hai vế của đồng nhất thức, rồi chia cả hai vế của nó cho y^2 (có thể làm được điều này vì $y \in \mathbb{F}_p^*$) ta thu được

$$a^2 \equiv -1 \pmod p.$$

Điều này dẫn đến -1 là một số chính phương modulo p.

Ta lại có $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, nên -1 là một số chính phương modulo p khi và chỉ khi $\frac{p-1}{2}$ là một số chẵn. Nói một cách khác thì

$$p \equiv 1 \pmod 4.$$

- Bước Euclid: Xây dựng nghiệm nguyên từ nghiệm đồng dư.

  Ta sẽ sử dụng thuật toán Euclid trong vành các số nguyên của Gauss:

  $$\mathbb{Z}[i] = \{m + in \mid m, n \in \mathbb{Z}\}.$$

  Vành $\mathbb{Z}[i]$ là một vành giao hoán với các phép toán như sau:

  $$(m + in) + (m' + in') := m + m' + i(n + n')$$

  và

  $$(m + in)(m' + in') := mm' - nn' + i(m'n + mn').$$

  Trên vành $\mathbb{Z}[i]$ ta có một chuẩn **chuẩn** N; là một ánh xạ từ $\mathbb{Z}[i]$ vào $\mathbb{Z}$ được định nghĩa bởi công thức sau:

  $$N(m + in) := m^2 + n^2.$$

  Ta có

  $$\begin{aligned} N\left((m + in)(m' + in')\right) &= (mm' - nn')^2 + (mn' + m'n)^2 \\ &= N(m + in)N(m' + in'). \end{aligned}$$

  Hay nói một cách khác, chuẩn của một tích thì bằng tích của các chuẩn. Do đó một phần tử $m + in$ khả nghịch trong vành $\mathbb{Z}[i]$ thì chuẩn của nó sẽ phải khả nghịch trong vành $\mathbb{Z}$. Mặt khác trên $\mathbb{Z}$ chỉ có 2 phần tử khả nghịch là $\{\pm 1\}$, nên nếu $m + in \in \mathbb{Z}[i]^\times$ thì $m^2 + n^2 = 1$. Bằng tính toán ta thu được

  $$\mathbb{Z}[i]^\times = \{1, -1, i, -i\}.$$

  Bài toán tìm $x, y \in \mathbb{Z}$ sao cho $x^2 + y^2 = p$ với $p \equiv 1 \pmod 4$, lúc này trở thành tìm số nguyên Gauss $x + iy$ sao cho $N(x + iy) = p$.

  Do $p \equiv 1 \pmod 4$ nên -1 là số chính phương modulo p. Gọi a là nghiệm của phương trình $x^2 + 1 = 0$ trong $\mathbb{F}_p^*$. Ta có

  $$p \mid a^2 + 1 = N(a + i) = N(a - i).$$

  Hơn nữa $(a + i) - (a - i) = 2i$ gần như nghịch đảo được trong vành $\mathbb{Z}[i]$ nên $p^2 \nmid N(a + i)$ và $p^2 \nmid N(a - i)$. Do đó nếu ta có thể sử dụng

khái niệm về ước chung lớn nhất trên vành $\mathbb{Z}[i]$, thì ta chỉ việc lấy $x+iy = \text{UCLN}(a+i, p)$ và lúc này chắc chắn ta sẽ có $N(x+iy) = p$.

Việc còn lại của chúng ta là chứng minh rằng trên vành các số nguyên Gauss ta vẫn có khái niệm ước chung lớn nhất. Điều này là hệ quả trực tiếp của mệnh đề 6.2 dưới đây nói rằng trên vành các số nguyên Gauss tồn tại một phép chia Euclid.

□

Mệnh đề 6.2. *Cho α và β là hai phần tử của $\mathbb{Z}[i]$ với $\beta \neq 0$, khi đó tồn tại hai số nguyên Gauss γ và ρ sao cho*

$$\alpha = \beta\gamma + \rho, \quad N(\rho) \leqslant \frac{1}{2}N(\beta) < N(\beta).$$

Chứng minh. Chuẩn trên $\mathbb{Z}[i]$ liên quan mật thiết với khái niệm giá trị tuyệt đối (hay còn gọi là module) của một số phức: $N(a+ib) = |a+ib|^2$.

Ta đồng nhất tập các số nguyên Gauss với lưới các điểm nguyên trên mặt phẳng phức. Mọi số phức đều sẽ nằm trong (tính cả trên cạnh) một hình vuông 1x1 với 4 đỉnh nằm trong $\mathbb{Z}[i]$. Do đó ta luôn có thể tìm được một phần tử thuộc $\mathbb{Z}[i]$ (là một trong 4 đỉnh của hình vuông vừa nhắc đến) sao cho khoảng cách giữa nó và số phức được chọn không vượt quá $1/\sqrt{2}$. Bây giờ ta xét số phức α/β. Gọi γ là đỉnh của hình vuông 1x1 chứa α/β và gần α/β nhất, Khi đó ta có

$$|\alpha/\beta - \gamma| \leqslant 1/\sqrt{2}.$$

Nhân cả hai vế với $|\beta|$ rồi bình phương cả hai vế bất đẳng thức nhận được, ta có

$$N(\alpha - \beta\gamma) \leqslant N(\beta).$$

Bây giờ ta lấy $\rho = \alpha - \beta\gamma$. □

Nhận xét 6.3. *1. Không giống như trên vành các số nguyên $\mathbb{Z}$, thương và phần dư trong phép chia Euclid trên vành các số nguyên Gauss không duy nhất. Ví dụ, với $\alpha = 37 + 2i$ và $\beta = 11 + 2i$, ta dễ dàng kiểm tra được:*

$$\alpha = 3.\beta + (4 - 4i), \quad \alpha = (3 - i)\beta + (2 + 7i).$$

Tuy nhiên nó không ảnh hưởng gì đến việc chứng minh sự tồn tại của khái niệm ước chung lớn nhất. Ta vẫn sử dụng chứng minh tương tự như trong vành các số nguyên.

2. *Với d là một số tự nhiên không chính phương, ta cũng có vành $\mathbb{Z}[\sqrt{d}] := \{x + y\sqrt{d}\}$ là một vành giao hoán được trang bị một chuẩn $N(x + y\sqrt{d}) = x^2 - dyr$. Khi đó $\mathbb{Z}[\sqrt{d}]^* = \{x + \sqrt{d}y \mid x^2 - dy^2 = \pm 1\}$. Phương trình Pell cho phép chúng ta tìm các phần tử nghịch đảo được của vành $\mathbb{Z}[\sqrt{d}]$.*

Hệ quả 6.4. *Phương trình $x^2 + y^2 = d$ có nghiệm nguyên khi và chỉ khi $\mathrm{ord}_p(d)$ là một số chẵn với mọi số nguyên tố lẻ $p \equiv -1 \pmod 4$. Trong đó $\mathrm{ord}_p(d)$ là số mũ n lớn nhất thỏa mãn tính chất $p^n \backslash d$.*

Bài tập về Phương trình Pell

Xét phương trình Điôphăng sau đây

$$x^2 - dy^2 = n. \tag{6.3}$$

- Nếu d là một số chính phương, việc giải phương trình để tìm nghiệm nguyên có thể thực hiện khá dễ dàng khi sử dụng hằng đẳng thức $a^2 - b^2 = (a-b)(a+b)$ và biết cách giải hệ phương trình tuyến tính hai ẩn hai phương trình.

- Ta quan tâm đến việc giải phương trình trên cho trường hợp d không là số chính phương. Ta có nếu (x, y) là nghiệm của phương trình reftq thì $(\pm x, \pm y)$ cũng là nghiệm của phương trình, vì thế ta cũng chỉ cần tìm các nghiệm không âm của phương trình 6.3 mà thôi.

Bài tập 6.1. Cho d là một số nguyên dương, không có ước chính phương. Chứng minh rằng phân số liên tục biểu diễn $\sqrt{d}$ tuần hoàn, và có dạng sau

$$\langle a_0, \overline{a_1, \ldots, a_{n-1}, 2a_0} \rangle$$

Bài tập 6.2. Cho d là một số nguyên dương không có ước chính phương và có phân số liên tục của $\sqrt{d}$ được biểu thị như bài trên. Gọi p_k và q_k là hai số nguyên dương nguyên tố cùng nhau thỏa mãn tính chất

$$\frac{p_k}{q_k} = \langle a_0, a_1, \ldots, a_k \rangle.$$

Đặt

$$(x_1, y_1) = \begin{cases} (p_{n-1}, q_{n-1}) & \text{nếu n chẵn} \\ (p_{2n-1}, q_{2n-1}) & \text{nếu n lẻ.} \end{cases}$$

Chứng minh rằng (x_1, y_1) là nghiệm của phương trình $x^2 - dy^2 = 1$. Hơn nữa nó còn là nghiệm nhỏ nhất theo nghĩa nếu (x, y) là một nghiệm không âm của phương trình thỏa mãn $y > 0$ thì $y \geqslant y_1$.

Bài tập 6.3. Cho d là một số nguyên dương không có ước chính phương. Chứng minh rằng mọi nghiệm nguyên dương của phương trình $x^2 - dy^2 = 1$ được cho bởi (x_n, y_n) với $n = 1, 2, \ldots$ trong đó x_n, y_n là các số nguyên dương được định nghĩa bởi $x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)^n$ với (x_1, y_1) như ở trong bài tập trên.

Bài tập 6.4. Cho d như trong bài tập 6.2 và sử dụng các kí hiệu của bài tập đó. Chứng minh rằng

- Nếu n chẵn thì phương trình $x^2 - dy^2 = -1$ không có nghiệm nguyên dương.
- Nếu n lẻ thì $(u_0, v_0) = (p_{n-1}, q_{n-1})$ là nghiệm nhỏ nhất của phương trình $x^2 - dy^2 = -1$. Các nghiệm khác của phương trình có dạng

$$u_n = u_0 x_n + dv_0 y_n, \quad v_n = v_0 x_n + u_0 y_n,$$

trong đó (x_n, y_n) là các nghiệm của phương trình $x^2 - dy^2 = 1$ như trong bài trên.

Bài tập 6.5. Cho p là một số nguyên tố. Chứng minh rằng phương trình $x^2 - py^2 = -1$ có nghiệm nguyên dương khi và chỉ khi $p = 2$ hoặc $p \equiv 1 \mod 4$.

Bài tập 6.6. Cho p là một số nguyên tố chia cho 4 dư 3, chứng minh rằng liên phân số của $\sqrt{p}$ có chu kì chẵn.

Bài tập 6.7. Cho $m \geqslant 2$ không phải là một số chính phương. Chứng minh rằng tồn tại vô hạn bộ gồm m+1 số nguyên dương liên tiếp sao cho mỗi số đều có thể viết thành tổng của m số chính phương (0 cũng tính là một số chính phương, các số chính phương không nhất thiết phải phân biệt).

Bài tập 6.8. Cho N là một số nguyên khác 0. Chứng minh rằng nếu phương trình $x^2 - dy^2 = N$ có nghiệm nguyên thì nó có vô số nghiệm.

Bài tập 6.9. Giải phương trình nghiệm nguyên dương sau:

$$x + y + z - 2\sqrt{xyz} = 1.$$

Bài tập 6.10. Chứng minh rằng có vố số số nguyên dương n sao cho số nguyên nhỏ nhất lớn hơn hoặc bằng $\sqrt{2}n$ là một số chính phương.

CHƯƠNG 7

Phương trình nghiệm nguyên

Trong bài giảng này chúng ta sẽ trình bày việc giải các phương trình nghiệm nguyên dựa trên **phương pháp giảm vô hạn của Fermat**.

Cho P là một tính chất liên quan đến các số nguyên không âm và đặt $(P(n))_{n\geqslant 1}$ là dãy các mệnh đề,

$$P(n)\text{: “số } n \text{ thỏa mãn tính chất } P.\text{”}$$

Fermat đưa ra một phương pháp được biết đến với tên *phương pháp giảm vô hạn* rất hiệu quả trong việc chứng minh mệnh đề $P(n)$ sai với mọi n đủ lớn.

Cho k là một số nguyên không âm. Giả sử rằng :

- *khi mà $P(m)$ đúng với một số nguyên $m > k$, thì sẽ phải có một số nguyên j nhỏ hơn, $m > j > k$ thỏa mãn tính chất $P(j)$ đúng.*

Khi đó $P(n)$ sai với mọi $n > k$.

Hay nói một cách khác, nếu có một số n thỏa mãn $P(n)$ đúng, ta có thể xây dựng được một dãy vô hạn các số nguyên không âm $n > n_1 > n_2 > \dots$ mà tất cả các phần tử của dãy này đều lớn hơn k, nhưng điều này là không thể xảy ra; một dãy giảm vô hạn như vậy không tồn tại.

Trong bài giảng này ta sẽ đề cập đến hai cách để sinh ra dãy giảm vô hạn được nhắc đến ở trên đó là:

1. Lũy thừa.

2. Phương pháp nhảy Vieta.

7.1 Luỹ thừa

Phương pháp sử dụng lũy thừa để xây dựng dãy giảm bắt nguồn từ một hệ quả trực tiếp của tính duy nhất của phân tích một số tự nhiên thành tích các số nguyên tố (sai khác thứ tự sắp xếp các số nguyên tố).

Mệnh đề 7.1. *Cho $x, y, z \in \mathbb{N}$ là các số tự nhiên, thỏa mãn tính chất* $\text{UCLN}(x, y) = 1$ *và $xy = z^n$. Khi đó tồn tại hai số nguyên $u, v \in \mathbb{Z}$ sao cho $x = u^n, y = v^n$.*

Phương pháp sử dụng lũy thừa thường được dùng khi giải các phương trình dạng Fermat.

Bài tập 7.1. Tìm các nghiệm nguyên dương của phương trình Pythagore:

$$x^2 + y^2 = z^2$$

Lời giải phác thảo. Ta có:

$$x^2 + y^2 = z^2 \Rightarrow z^2 - x^2 = y^2 \Rightarrow (z - x)(z + x) = y^2$$

Ta có thể giả sử rằng x, y, z đôi một nguyên tố cùng nhau. (Vì nếu p là ước chung lớn nhất của x, y thì từ phương trình ta cũng thu được p phải là ước của z. Bằng việc lấy x, y, z đem chia cho p, ta thu được được một nghiệm mới (x, y, z) của phương trình mà lúc này x, y, z đôi một nguyên tố cùng nhau.)

Do x, y, z đôi một nguyên tố cùng nhau nên ta dễ dàng kiểm tra được rằng ước chung lớn nhất của $z - x$ và $z + x$ chỉ có thể là 1 hoặc 2.

Xét trường hợp $\text{UCLN}(z - x, z + x) = 1$. Áp dụng mệnh đề 7.1 cho phương trình $(z - x)(z + x) = y^2$. Khi đó tồn tại hai số $u, v \in \mathbb{Z}+$ sao cho (giả sử $y > 0$):

$$\begin{cases} z - x = u^2 \\ z + x = v^2 \\ y = uv \end{cases} \Rightarrow \begin{cases} x = \frac{v^2 - u^2}{2} \\ y = uv \\ z = \frac{v^2 + u^2}{2} \end{cases}$$

Ta thu được dạng nghiệm tổng quát cho phương trình nghiệm nguyên $x^2 + y^2 = z^2$.

Lời giải này chưa đầy đủ vì chưa xét hết các trường hợp chẵn, lẻ. Các trường hợp còn lại đều có thể giải tương tự như trên. □

Định lý 7.2 (Euler)**.** *Phương trình $x^3+y^3=z^3$ không có nghiệm nguyên nằm trong tập các số khác 0.*

Phác thảo chứng minh. Chúng ta có thể tìm được chứng minh chi tiết của định lý này trên "Wikipedia: Proof of Fermat's theorem for specific exponents". Ý tưởng của chứng minh đó là nếu (x, y, z) là một nghiệm nguyên dương của phương trình thì ta luôn có thể xây dựng được một nghiệm nguyên dương mới nhỏ hơn bằng cách sử dụng lũy thừa. Từ đó áp dụng phương pháp giảm vô hạn để thu được điều phải chứng minh.

Bằng lập luận giống bài tập phía trên, nếu phương trình có nghiệm $(x \neq 0, y \neq 0, z \neq 0)$ thì nó cũng sẽ có nghiệm (x, y, z) thỏa mãn tính chất x, y, z đôi một nguyên tố cùng nhau. Ta dễ kiểm tra rằng trong 3 số x, y, z phải có đúng một số chẵn và hai số còn lại phải là số lẻ. Không mất tính tổng quát ta có thể giả sử z là số chẵn. (Chú ý việc phương trình $x^3+y^3=z^3$ có nghiệm tương đương với phương trình $x^3+y^3+z^3=0$ có nghiệm và ta có tương ứng 1-1 giữa nghiệm của hai phương trình. Khi nhìn vào phương trình $x^3+y^3+z^3=0$ ta thấy được vai trò của x, y, z là như nhau.) Lúc này x, y là hai số lẻ. Đặt $x+y=2u$ và $x-y=2v$, phương trình được viết lại như sau:

$$\begin{aligned}(u+v)^3+(u-v)^3 &= z^3\\ 2u(u^2+3v^2) &= z^3\end{aligned}$$

Do UCLN$(x, y)=1$ nên UCLN$(2u,\ u^2+3v^2)$ chỉ có thể là 1 hoặc 3.

Giả sử UCLN$(2u,\ u^2+3v^2)=1$, áp dụng mệnh đề 7.1 ta được

$$u^2+3v^2=s^3.$$

(Trong trường hợp còn lại ta cũng tìm được một bộ ba số w, v, s sao cho $3w^2+v^2=s^3$.)

Bước khó nhất trong việc xây dựng được một nghiệm mới của phương trình đó là chứng minh khẳng định sau:

"Giả sử $u^2+3v^2=s^3$, khi đó ta luôn tìm được hai số $e, t \in \mathbb{Z}$ sao cho:

$$s=e^2+3t^2."$$

Ta nhận thấy rằng $m^2+3n^2=(m+\sqrt{-3}n)(m-\sqrt{-3}n)$ có dạng như một chuẩn của một số $m+\sqrt{-3}n$. Điều này gợi ý ta xét mở rộng trường

bậc 2 của $\mathbb{Q}$ là

$$K := \mathbb{Q}[\sqrt{-3}] := \{m + n\sqrt{-3} \mid m, n \in \mathbb{Q}\}.$$

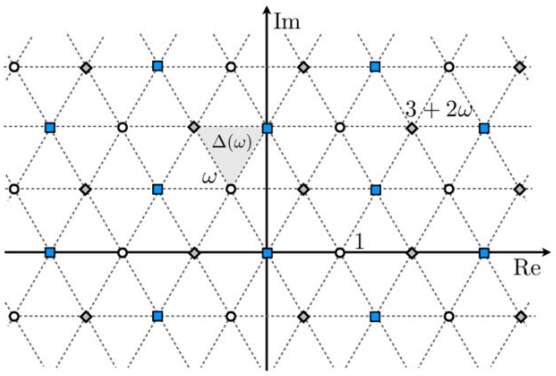
Phép nhân của trường này được cho bởi công thức

$$(m + \sqrt{-3}n)(m' + \sqrt{-3}n') = \underbrace{(mm' - 3nn')}_{\in\mathbb{Q}} + \sqrt{-3}\underbrace{(mn' + nm')}_{\in\mathbb{Q}}.$$

Vành các số nguyên của trường này là vành các số nguyên Eisenstein

$$\mathbb{Z}_K := \{m + nj \mid m, n \in \mathbb{Z}\}.$$

Trong đó $j = \frac{1+\sqrt{-3}}{2}$ là căn nguyên thủy bậc 3 của đơn vị.



Hình 7.1: Hình các số nguyên Eisenstein trên mặt phẳng phức

Giống như vành các số nguyên Gauss, chuẩn trên vành các số nguyên Eisenstein chính là bình phương của giá trị tuyệt đối trên trường số phức $N(x+yj) = |x+jb|^2 = x^2 - xy + y^2$. Ta đồng nhất các số nguyên Eisenstein với số phức tương ứng. Hình 7.1 chính là hình ảnh của các số Eisenstein trên mặt phẳng phức.

Dễ nhận thấy, mọi số phức bất kì luôn sẽ nằm trong (hoặc trên cạnh) của một tam giác đều cạnh 1 có 3 đỉnh là các số nguyên Eisenstein. Do đó với mọi $z \in \mathbb{C}$ ta luôn tìm được $a \in \mathbb{Z}_K$ sao cho

$$|z - a| < 1.$$

Với hai số nguyên Eisenstein $a, b \in \mathbb{Z}_K$ thỏa mãn $b \neq 0$, khi đó ta luôn tìm được $q \in \mathbb{Z}_K$ sao cho

$$\left|\frac{a}{b} - q\right| < 1.$$

Lấy $r = a - bq$, khi đó ta có $|r| < |n|$ (điều này tương đương với $N(r) < N(n)$). Chúng ta vừa chứng minh rằng cho trước $a, b \in \mathbb{Z}_K$ thỏa mãn $b \neq 0$, luôn tồn tại $q, r \in \mathbb{Z}_K$ sao cho

$$a = qb + r$$

với $N(r) < N(b)$. Hay nói cách khác trên vành các số nguyên Eisenstein tồn tại phép chia Euclid. Mặc dù phần thương và phần dư của phép chia không duy nhất nhưng chúng ta vẫn có được thuật toán Euclid để tìm ước chung lớn nhất của hai số Eseinstein và thu được tính phân tích duy nhất thành tích các thừa số Eisenstein nguyên tố (một số Eisenstein được gọi là nguyên tố nếu nó không thể viết thành tích của hai số Eisentein khác đơn vị) của các số nguyên Eisenstein modulo một phần tử đơn vị (hay còn gọi là phần tử nghịch đảo được)

$$\mathbb{Z}_K^* := \{1, j, j^2, -j, -j^2, -1\}.$$

Tính phân tích duy nhất dẫn đến, nếu $a, b, c \in \mathbb{Z}_K$ thỏa mãn $ab = c^3$ và $\text{UCLN}(a, b) = 1$ thì ta luôn tìm được hai số $p, q \in \mathbb{Z}_K^*$ và hai số $\alpha, \beta \in \mathbb{Z}_K^*$ sao cho

$$a = p^3\alpha, b = q^3\beta.$$

Quay lại chứng minh khẳng định. Đặt $a = u + \sqrt{-3}v = (u - v) + 2vj \in \mathbb{Z}_K$. Từ giả thiết ta có $N(a) = ab = s^3$ với $b = u - \sqrt{-3}v = (u + v) - 2vj \in \mathbb{Z}_K$. Mặt khác ta có thể chứng minh được rằng $\text{UCLN}(a, b) = 1$, nên do tính phân tích duy nhất của vành $\mathbb{Z}_K$ tồn tại $p \in \mathbb{Z}_K$ và $\alpha \in \mathbb{Z}_k^*$ sao cho $a = p^3\alpha$. Ta có $s^3 = N(a) = N(p)^3$. Vậy $N(p) = s$. □

Tương tự với chứng minh của định lý Euler ở trên, để chứng minh bài toán Fermat: "Phương trình $x^p + y^p = z^p$ không có nghiệm tầm thường (tức là không có nghiệm nằm trong tập các nguyên khác 0) với $p > 2$ là một số nguyên tố", ta xét trường cyclotomic (trường chia đường tròn) $\mathbb{Q}[\zeta_p]$ với ζ_p là căn nguyên thủy bậc p của 1. Ta nhận thấy rằng nếu có thể chứng minh được rằng: "nếu $N(x) = r^p$ kéo theo sự tồn tại của một phần tử y của vành các nguyên của $\mathbb{Q}[\zeta_p]$ thỏa mãn tính chất $N(y) = r$" thì bài toán Fermat sẽ được giải quyết. Rất đáng tiếc là về mặt tổng quát điều này không đúng. Với $p > 5$, vành các nguyên của trường $\mathbb{Q}[\zeta_p]$ không còn là một vành Euclid nữa.

Trong lý thuyết số đại số, chúng ta có một khái niệm **số lớp** (class number) cho phép ta biết được vành cần xét có phải là vành Euclid hay

không. Gọi N_p là số lớp của vành các nguyên của trường $\mathbb{Q}[\zeta_p]$. Khi đó vành sẽ là Euclid nếu $N_p = 1$ và sẽ không là Euclid nếu $N_p > 1$.

Một số nguyên tố p được gọi là chính quy nếu p không là ước của N_p. Kummer đã chứng minh rằng bài toán Fermat đúng với mọi số nguyên tố chính quy.

Nhận xét 7.3. *Đa số các số nguyên tố nhỏ đều chính quy, nên giải được bài toán Fermat cho nhiều số nguyên tố.*

Bài toán mở: Một câu hỏi được đặt ra là liệu vô hạn p nguyên tố chính quy theo nghĩa của Kummer hay không?

7.2 Phương pháp nhảy Vieta

Bài tập 7.2 (IMO 1988)**.** Cho a, b là hai số nguyên dương thỏa mãn tính chất $ab+1 \mid a^2+b^2$. Chứng minh rằng $\frac{a^2+b^2}{ab+1}$ là một số chính phương.

Lời giải. Ta nhận thấy bộ $(a, b) = (a, 0)$ với $a > 0$ thỏa mãn tính chất $ab + 1 = 1$ là ước của $a^2 + b^2 = a^2$. Với bộ này hiển nhiên ta có $\frac{a^2+b^2}{ab+1} = \frac{a^2}{1}$ là một số chính phương.

Giả sử (a, b) là hai số nguyên dương thỏa mãn tính chất đề bài; ta sẽ biến đổi cặp (a, b) đưa về dạng suy biến nhắc ở trên sao cho giữ nguyên giá trị của $\frac{a^2+b^2}{ab+1}$.

Đặt $\frac{a^2+b^2}{ab+1} = k$. Nhân cả hai vế của đẳng thức với $ab + 1$ ta thu được phương trình

$$a^2 - kab + (b^2 - k) = 0 \tag{7.1}$$

Đây là một phương trình bậc 2 với biến số a và tham số b, k. Với b và k cố định, nếu phương trình trên có một nghiệm nguyên a thì nó cũng phải có một nghiệm nguyên khác.

Giả sử $a \geqslant b > 0$ và phương trình $x^2 - kbx + b^2 - k = 0$ có một nghiệm $x_1 = a$. Khi đó nghiệm còn lại của phương trình là $x_2 = kb - a = \frac{b^2-k}{a} < b$. Cặp mới (b, x_2) cũng vẫn thỏa mãn điều kiện của bài toán và

$$\frac{a^2 + b^2}{ab + 1} = \frac{x_2^2 + b^2}{x_2 b + 1}.$$

Cách xây dựng này vẫn tiếp tục được thực hiện khi mà cặp (a, b) vẫn còn thỏa mãn tính chất $a \geqslant b > 0$. Tuy nhiên điều này không thể thực

hiện vô hạn lần được, nó phải dừng lại. Hay đến một bước nào đó thì $b = 0$ (chính là dạng suy biến).

□

Bài tập 7.3. Cho $x, y \in \mathbb{Z}^+$ là các số nguyên dương thỏa mãn tính chất $xy \mid x^2 + y^2 + 1$. Chứng minh rằng $\frac{x^2+y^2+1}{xy} = 3$.

Bài tập 7.4 (IMO 2007)**.** Cho $a, b \in \mathbb{Z}^+$ là hai số nguyên dương. Chứng minh rằng nếu $4ab - 1 \mid (4a^2 - 1)^2$, thì $a = b$.

Bài tập về Phương trình dạng Fermat

Bài tập 7.5. Xét phương trình Pythagore sau:

$$x^2 + y^2 = z^2. \tag{7.2}$$

Một nghiệm (x_0, y_0, z_0) được gọi là *nghiệm nguyên thủy* nếu x_0, y_0, z_0 đôi một nguyên tố cùng nhau. Chứng minh rằng một nghiệm nguyên thủy (x, y, z) trong tập hợp các số nguyên dương của phương trình trên với y là số chẵn có dạng:

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2$$

trong đó m, n là các số nguyên dương nguyên tố cùng nhau thỏa mãn tính chất $m > n$ và $m + n$ là số lẻ. Từ đó suy ra phương trình trên có nghiệm nguyên dạng

$$x = k(m^2 - n^2), \quad y = 2kmn, \quad z = k(m^2 + n^2),$$

(chúng ta có thể đối vai trò của x và y) trong đó $k, m, n \in \mathbb{Z}$.

Bài tập 7.6. Chứng minh rằng phương trình sau

$$x^4 + y^4 = z^2$$

không có nghiệm trong tập các số nguyên khác 0. Điều này dẫn đến phương trình

$$x^4 + y^4 = z^4 \tag{7.3}$$

không có nghiệm trong tập các số nguyên khác 0.

Bài tập 7.7. Cho n là một số nguyên dương. Chứng minh rằng phương trình Diophante

$$x^2 + 3y^2 = n$$

có nghiệm nếu mọi ước nguyên tố của n có dạng $3k - 1$ phải có số mũ chẵn.

Bài tập 7.8. Chứng minh rằng phương trình Diophante

$$x^2 + 3y^2 = z^3$$

có nghiệm (x_0, y_0, z_0) với z_0 là một số lẻ và x_0, y_0 nguyên tố cùng nhau khi và chỉ khi tồn tại hai số nguyên α, β thỏa mãn tính chất $\alpha \not\equiv \beta \mod 2$, $\text{UCLN}(\alpha, 3\beta) = 1$, và

$$x_0 = \alpha(\alpha^2 - 9\beta^2), \quad y_0 = 3\beta(\alpha^2 - \beta^2), \quad z_0 = \alpha^2 + 3\beta^2.$$

Bài tập 7.9. Chứng minh rằng phương trình Diophante

$$x^3 + y^3 = z^3 \tag{7.4}$$

không có nghiệm trong tập các số nguyên khác 0.

Các phương trình (7.4),(7.3) là trường hợp đặc biệt của phương trình Fermat:

$$x^n + y^n = z^n, \tag{7.5}$$

trong đó n là một số nguyên dương lớn hơn 2 và x, y, z là các số nguyên khác 0.

Định lý Fermat lớn (còn được biết với tên là định lý cuối cùng của Fermat- **FLT**) khẳng định rằng phương trình (7.5) không có nghiệm trong tập các số nguyên khác 0. Vào khoảng năm 1630, bên lề cuốn sách Số học của Diophantus, Fermat đã viết rằng:

"*Tôi đã tìm được lời giải cho bài toán nhưng lề sách này quá nhỏ để có thể viết ra được lời giải.*"

Fermat chỉ đưa ra chứng minh chi tiết cho trường hợp $n = 4$. Trường hợp tổng quát đã làm đau đầu rất nhiều nhà toán học và phải mãi đến năm 1994, bài toán mới được giải trọn vẹn bởi Andrew Wiles.

Bài tập 7.10. Chứng minh rằng nếu phương trình Fermat không có nghiệm trong tập các số nguyên khác 0 với n=k nào đó thì điều đó cũng đúng với n=kl với l là một số nguyên dương bất kì.

Áp dụng bài tập trên, cho phép ta chỉ cần chứng minh bài toán cuối cùng của Fermat cho trường hợp n=p là một số nguyên tố. Giả sử phương trình

$$a^p + b^p = c^p$$

có nghiệm trong các số nguyên khác 0. Khi đó áp dụng định lý nhỏ của Fermat ta có

$$a + b \equiv c \mod p.$$

Nếu ta chỉ xét các bộ nghiệm nguyên thủy (nghĩa là các a,b,c đôi một nguyên tố cùng nhau) thì chúng có một trong 2 dạng sau:

(I) p không là ước của bất kì a, b, c nào.

(II) p là ước của duy nhất một trong 3 số a, b, c.

Bài tập 7.11. Cho p, q là hai số nguyên tố lẻ phân biệt sao cho

- nếu $x^p + y^p + z^p \equiv 0 \mod q$ thì x, y hoặc $z \equiv 0 \mod q$,
- phương trình $t^p \equiv p \mod q$ (biến là t) không có nghiệm;

khi đó phương trình $a^p + b^p = c^p$ không có nghiệm loại (I).

Bài tập 7.12. Cho p là số nguyên tố lẻ sao cho $2p+1$ cũng là số nguyên tố. Chứng minh rằng phương trình $x^p + y^p = z^p$ không có nghiệm dạng (I).

Một trong những phát triển quan trọng trong quá trình tìm lời giải cho bài toán FLT đó là mối quan hệ giữa FLT và lý thuyết về các đường cong elliptic, đây là một vấn đề trung tâm của nghiên cứu toán học hiện đại.

Cho K là một trường (ví dụ như $K = \mathbb{R}, \mathbb{C}, \mathbb{Q}, ...$) một đường cong elliptic là tập hợp các nghiệm $(x, y) \in K^2$ của phương trình

$$y^2 = x^3 + ax^2 + bx + c$$

với $a, b, c \in K$ thỏa mãn tính chất $a^2b^2 - 4a^3c - 4b^3 + 18abc - 27c^2 \neq 0$ ($D = a^2b^2 - 4a^3c - 4b^3 + 18abc - 27c^2$ chính là biệt thức của đa thức $x^3 + ax^2 + bx + c$, biệt thức này cho phép chúng ta kiểm tra xem đa thức có nghiệm bội hay không). Taniyama - Shimura - Weil đưa ra một giả thuyết (sau được chứng minh bởi Andrew Wiles vào năm 1994) rằng những đường cong elliptic này có tính chất *modular* (ta không đề cập sau vào khái niệm này ở đây).

Frey chỉ ra rằng nếu phương trình $a^p + b^p = c^p$ với p là một số nguyên tố lẻ có nghiệm nguyên dương khi đó đường cong

$$y^2 = x(x - a^p)(x + b^p)$$

là một đường cong elliptic. Tuy nhiên Ribet chứng minh được rằng đường cong này thì không có tính chất modular. vì thế đường cong này không tồn tại, nên FLT phải đúng.

CHƯƠNG 8

Giải phương trình đa thức một ẩn - lý thuyết Galois

Bài giảng này chúng ta sẽ sử dụng lý thuyết Galois để giải thích ý nghĩa của lời giải phương trình bậc hai, bậc ba một biến. Từ đó có một cách nhìn tổng quan về việc giải một phương trình đa thức một biến.

Định nghĩa 8.1.

- Một phương trình đa thức bậc n một biến là phương trình có dạng

$$t^n - a_1 t^{n-1} + \cdots + (-1)^n a_n = 0,$$

trong đó $a_1, \cdots, a_n \in k$ là các tham số trên một trường k (để tránh những phiền toái không cần thiết chúng ta yêu cầu thêm k phải chứa căn bậc ba nguyên thủy của đơn vị) và t là một ẩn số.

- Giải phương trình là tìm một công thức tổng quát biểu đạt ẩn số t theo các tham số $a_1, \cdots, a_n$. Công thức là biểu thức của $a_1, \cdots, a_n$ sử dụng bốn phép toán thông thường $(+, -, \times, :)$ và khai căn.

Nhận xét 8.2. *Trong định nghĩa trên ta thấy có một số vấn đề sau:*

- *Ta đã biết rằng phương trình đa thức bậc n có thể có đến n nghiệm, vậy thì ta muốn tìm công thức tổng quát để biểu đạt cho nghiệm nào?*
- *Khái niệm công thức viết ở trên rất không ổn. (Liệu một công thức như vậy có tồn tại hay không?) Đây chính là khởi đầu của lý thuyết Galois.*

Ta cần đặt lại bài toán như sau:

Giả sử $x_1, x_2, \cdots, x_n$ là các nghiệm của phương trình (không nhất thiết phải phân biệt):

$$t^n - a_1 t^{n-1} + \cdots + (-1)^n a_n = 0$$

Áp dụng định lý Bezout ta có:

$$t^n - a_1 t^{n-1} + \cdots + (-1)^n a_n = (t - x_1)(t - x_2) \cdots (t - x_n).$$

So sánh hệ số của hai đa thức trong hai vế của đẳng thức trên ta thu được công thức Vieta (Viète):

$$\begin{cases} a_1 = x_1 + x_2 + \cdots + x_n \\ a_2 = x_1 x_2 + \cdots + x_{n-1} x_n \\ \cdots \\ a_n = x_1 x_2 .. x_n \end{cases}$$

- Đặt $K = k(a_1, a_2, \cdots, a_n)$ là trường tất cả các phân thức hữu tỉ n biến $a_1, a_2, \cdots, a_n$.
- Đặt $L = k(x_1, x_2, \cdots, x_n)$ là trường tất cả phân thức hữu tỉ n biến $x_1, x_2, \cdots, x_n$.
- Đặt $\mathfrak{S}_n$ là nhóm các hoán vị của tập hợp $\{1, 2, \cdots, n\}$. Nhóm này còn được gọi là nhóm đối xứng của n phần tử.

Từ công thức Vieta ta thấy rằng K là một trường con của trường L. Với mọi $\sigma \in \mathfrak{S}_n$ cảm sinh cho ta một tự đẳng cấu trường (ánh xạ bảo toàn các phép toán cộng và nhân của trường):

$$\sigma : L \to L$$

$$x_i \mapsto x_{\sigma(i)}.$$

Ta có: mọi đa thức $P(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ bất biến đối với tác động của $\mathfrak{S}_n$ (nghĩa là $P(x_1, \ldots, x_n) = P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ với mọi $\sigma \in \mathfrak{S}_n$) đều có thể biểu đạt như một đa thức của $a_1, a_2, \cdots, a_n$ (xem thêm bài tập 8.5). Do đó K không chỉ là trường con của L mà nó còn là trường con các phần tử bất biến (dưới tác động của $\mathfrak{S}_n$) của L. Điều này kéo theo L là một mở rộng Galois của K và L là một K-không gian véc tơ có $n!$ chiều.

Ví dụ 8.3. *Đa thức $a_1^2 + a_2$ là một đa thức bất biến (khi xét nó là đa thức của các biến $x_1, \cdots, x_n$).*

Lúc này bài toán giải phương trình đa thức một biến có thể quy về việc nghiên cứu mở rộng trường L/K.

8.1 Phương trình bậc hai

Ta sẽ tìm hiểu công thức nghiệm của phương trình bậc 2 tổng quát

$$x^2 - a_1 x + a_2 = 0$$

từ góc độ mở rộng trường. Trong trường hợp $n = 2$, trường $L = k(x_1, x_2)$ là một không gian véc tơ hai chiều trên trường $K = k(a_1, a_2)$. Nhóm $\mathfrak{S}_2$ có hai phần tử là phép đồng nhất id và phép hoán vị $\sigma = (1, 2)$ tác động lên L theo công thức $\sigma(x_1) = x_2$ và $\sigma(x_2) = x_1$. Ta có thể coi $\sigma : L \to L$ là tự đồng cấu K-tuyến tính của không gian véc tơ L thỏa mãn tính chất $\sigma^2 = 1$. Dựa vào ánh xạ tuyến tính này, ta có thể phân tích L tổng trực tiếp của hai không gian con

$$L = L_+ \oplus L_-,$$

với $L_+ = \{x \in L \mid \sigma(x) = x\} = K$ và $L_- = \{x \in L \mid \sigma(x) = -x\}$. (Tổng trực tiếp được hiểu là với mọi phần tử $x \in L$ ta luôn có một và chỉ một cách viết $x = x_+ + x_-$ sao cho $x_+ \in L_+$ và $x_- \in L_-$.) Hơn nữa, ta để ý rằng nếu $x \in L_-$ thì $x^2 \in L_+$ (do $\sigma(x^2) = \sigma(x)^2 = (-x)^2 = x^2$).

Bây giờ x_1 viết được duy nhất thành tổng của một phần tử thuộc L_+ và một phần tử thuộc L_- như sau

$$\begin{aligned} x_1 &= \underbrace{\frac{x_1 + x_2}{2}}_{\in K} + \underbrace{\frac{x_1 - x_2}{2}}_{\in L_-} \\ &= \frac{a_1}{2} + \frac{x_1 - x_2}{2}. \end{aligned}$$

Theo nhận xét trên ta có

$$\Delta := (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1 x_2 = a_1^2 - 4a_2^2$$

là một phần tử thuộc K. Điểm qua trong ở đây là Δ là một phần tử thuộc K còn công thức tường minh của nó như một đa thức của a_1, a_2 thực ra không quá quan trọng.

Nghiệm x_1 viết được thành tổng của một phần tử thuộc K và một phần tử có bình phương thuộc vào K. Như vậy ta đã viết được x_1 như là một biểu thức đại số của các biến a_1, a_2 với bốn phép toán thông thường và căn bậc hai.

8.2 Phương trình bậc ba

Trong trường hợp $n = 3$, trường $L = k(x_1, x_2)$ là một không gian véc tơ 6 chiều trên trường $K = k(a_1, a_2)$ với x_1, x_2, x_3 là nghiệm của phương trình bậc ba tổng quát:

$$t^3 - a_1 t^2 + a_2 t - a_3 = 0.$$

Nhóm $\mathfrak{S}_3$ là một nhóm có 6 phần tử. Rất đáng tiếc là nhóm này không giao hoán. Một phần tử $\sigma \in \mathfrak{S}_3$ biến phần tử $x_1 \mapsto x_{\sigma(1)}$, $x_2 \mapsto x_{\sigma(2)}$, $x_3 \mapsto x_{\sigma(3)}$ sẽ được thể hiện bởi bảng sau

$$\begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix}.$$

Nếu biểu diễn một phép hoán vị σ như một đồ thị có hướng với ba đỉnh là x_1, x_2, x_3, các cạnh có hướng của đồ thị (các mũi tên) là các $\overrightarrow{x_i x_{\sigma(i)}}$ thì đồ thị sẽ là hợp rời của các chu trình. Sử dụng cách thể hiện bằng chu trình ta có phân loại các phần tử của nhóm $\mathfrak{S}_3$ như sau:

- Loại 1: chỉ gồm phần tử đơn vị $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$; đồ thị của nó gồm 3 chu trình có độ dài 1.
- Loại 2: gồm 3 phần tử $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$; đồ thị của chúng gồm một chu trình có độ dài 2 và một chu trình có đội dài 1.
- Loại 3: gồm 2 phần tử $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$; đồ thị của chúng chỉ có một chu trình có độ dài 3.

Đồng cấu dấu $\text{sgn} : \mathfrak{S}_3 \to \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$ gán cho 3 phần tử loại 2 dấu -1 và 3 phần tử còn lại dấu 1. Hạt nhân của đồng cấu dấu

$$\ker(\text{sgn}) := \{\sigma\mathfrak{S}_3 \in |\text{sgn}(\sigma) = 1\}$$

là nhóm thay phiên $\mathfrak{A}_3 \simeq \mathbb{Z}/3\mathbb{Z}$. Nhóm này có 3 phần tử là:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Ta có dãy khớp sau:

$$1 \to \mathfrak{A}_3 \to \mathfrak{S}_3 \xrightarrow{\text{sgn}} \{\pm 1\} \to 1.$$

Dãy khớp này cho phép ta chuyển từ việc nghiên cứu mở rộng trường L/K chịu tác động của nhóm $\mathfrak{S}_3$ (không giao hoán) về nghiên cứu các mở rộng trường trung gian chỉ chịu tác động của nhóm $\mathfrak{A}_3$ hoặc nhóm $\{\pm 1\}$ đơn giản hơn (và quan trọng là chúng giao hoán). Cụ thể ta gọi M là trường con của L được định như sau:

$$M := \{x \in L \mid \zeta(x) = x,\ \forall\sigma \in \mathfrak{A}_3\}.$$

Theo lý thuyết Galois, M là một K-không gian hai chiều và L là một M-không gian véc tơ 3 chiều. Hơn nữa mở rộng L/M chịu tác động của nhóm $\mathfrak{A}_3$ và mở rộng M/K chịu tác động của nhóm $\{pm1\}$.

Gọi ε là phần tử của $\{\pm 1\}$ tác động không tầm thường lên M/K. Với lập luận tương tự như khi làm việc với đa thức bậc hai, M có thể viết thành tổng trực tiếp của hai K-không gian con 1 chiều

$$M = M_+ \oplus M_-.$$

Trong đó $M_+ = \{x \in M|\varepsilon(x) = x\} = K$ và $M_- = \{x \in M|\varepsilon(x) = -x\}$. Do M_- là một không gian véc tơ 1 chiều nên các véc tơ của nó sẽ là một bội số của một véc tơ khác 0 bất kì. Việc có thể xây dựng được một véc tơ khác 0 của M_- sẽ giúp ta hiểu nhiều hơn về mở rộng M/K. Giả sử $x \in M_- \subset L$, khi đó ta có $\sigma(x) = \text{sgn}(\sigma)x$ với mọi $\sigma \in \mathfrak{S}_3$. Cách thông thường để xây dựng các đa thức có tính chất này, đó là bắt đầu từ một đa thức bất kì $x \in L$ và xét tổng đan dấu:

$$\sum_{\sigma\in\mathfrak{S}_3} \text{sgn}(\sigma)\sigma(x) \in M_-.$$

Lấy $x = x_1x_2^2$, ta được phần tử

$$\delta = \sum_{\sigma\in\mathfrak{S}_3} \operatorname{sgn}(\sigma)\sigma(x) = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1) \in M_-.$$

Bình phương của $\delta \in M_-$ là phần tử

$$\Delta = \delta^2 \in K$$

. Phần tử Δ này còn được gọi là **biệt thức** và hiển nhiên nó có thể viết được dưới dạng như một đa thức của a_1, a_2, a_3.

Với mở rộng L/M ta cũng có thể làm tương tự. Ta kí hiệu $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ là phần tử sinh của nhóm luân phiên $\mathfrak{A}_3$. Vì M bất biến dưới tác động của nhóm $\mathfrak{A}_3$ nên ta có thể xem tác động của σ lên L như một đồng cấu M-tuyến tính thỏa mãn tính chất $\sigma^3 = 1$. Do đó ta có thể tách L thành tổng trực tiếp của 3 M-không gian véc tơ con có số chiều bằng 1:

$$L = L_0 \oplus L_1 \oplus L_2,$$

với L_i là không gian các véc tơ $x \in L$ sao cho $\sigma(x) = \rho^i x$ với mọi $i \in \{0, 1, 2\}$ và $\rho = e^{\frac{2i\pi}{3}}$ là căn bậc ba nguyên thủy của đơn vị đã được cho từ đầu. Hiển nhiên rằng $L_0 = M$ và nếu $x \in L_i$ thì ta luôn có $x^3 \in L_0$. Bằng giải thức Lagrange ta có thể xây dựng các phần tử sinh của M-không gian véc tơ L_1 và L_2:

$$\xi_1 = \rho^2x_1 + \rho x_2 + x_3 \in L_1, \quad \xi_2 = x_1 + \rho x_2 + \rho^2 x_3 \in L_2.$$

Vì $\xi_1 \in L_1$, $\xi_2 \in L_2$ nên $\xi_1^3 \in M$ và $\xi_2^3 \in M$. Ta lại có $M = K \oplus K\delta$, nên tồn tại $\alpha_1, \beta_1, \alpha_2, \beta_2 \in K$ sao cho

$$\xi_1^3 = \alpha_1 + \beta_1\delta, \quad \xi_2^3 = \alpha_2 + \beta_2\delta. \tag{8.1}$$

Đến đây việc giải phương trình bậc ba coi như đã hoàn thành. Để tìm công thức cho nghiệm x_1 chẳng hạn, ta chỉ cần viết nó thành tổ hợp M-tuyến tính của 1, ξ_1 và ξ_2:

$$x_1 = \frac{a_1}{3} + \rho\frac{\xi_1}{3} + \rho^2\frac{\xi_2}{3}.$$

Rồi dùng các đẳng thức ở (8.1) để viết nó về dạng căn thức liên quan đến các biến a_1, a_2, a_3.

Điểm mấu chốt của giải phương trình bậc ba nằm ở cấu trúc của nhóm đối xứng $\mathfrak{S}_3$

$$1 \to \mathfrak{A}_3 \to \mathfrak{S}_3 \to \{\pm 1\} \to 1.$$

8.3 Phương trình bậc bốn

Giống như trong các trường hợp trên, để giải phương trình bậc bốn, ta cần nghiên cứu cấu trúc của nhóm $\mathfrak{S}_4$. Nhóm này là một nhóm có 24 phần tử và cũng là một nhóm không giao hoán. Ta cần phải biểu diễn $\mathfrak{S}_4$ như một mở rộng liên tiếp của các nhóm giao hoán. Nghĩa là ta cần phải tìm dãy liên tiếp những nhóm con chuẩn tắc

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_k = \mathfrak{S}_4$$

sao cho G_i/G_{i-1} là các nhóm giao hoán.

Xét đồng cấu dấu $\operatorname{sgn} : \mathfrak{S}_4 \to \{\pm 1\}$. Hạt nhân của đồng cấu này là nhóm thay phiên $\mathfrak{A}_4$ có 12 phần tử. Các phần tử của nhóm này gồm:

- Loại 1: phép hoán vị đồng nhất; đồ thị của nó gồm 4 chu trình có độ dài 1.
- Loại 2: Ba phép hoán vị có đồ thị là hợp của hai chu trình có độ dài 2. (Do ta chỉ có 3 cách chia tập $\{1, 2, 3, 4\}$ thành 2 tập con mà mỗi tập có đúng 2 phần tử).
- Tám phép hoán vị có đồ thị là hợp của một chu trình độ dài 3 và một chu trình độ dài 1. (Có 4 cách để chia tập $\{1, 2, 3, 4\}$ thành 2 tập con mà một tập có 3 phần tử và tập còn lại có 1 phần tử. Trong mỗi cách chia tập, ta lại có 2 cách để tạo ra chu trình có độ dài 3.)

Gọi V_3 là nhóm con của $\mathfrak{A}_4$ gồm các phép hoán vị thuộc loại 1 và 2 kể trên. Ta có $V_3 \simeq (\mathbb{Z}/2\mathbb{Z})^2$ và $\mathfrak{A}_4/V_3 \simeq \mathbb{Z}/3\mathbb{Z}$.

Ta thu được dãy liên tiếp các nhóm con chuẩn tắc (thỏa mãn yêu cầu phía trên) như sau:

$$1 \trianglelefteq V_3 \trianglelefteq \mathfrak{A}_4 \trianglelefteq \mathfrak{S}_4.$$

Từ đó ta xây dựng được các mở rộng trung gian

$$K \subset K_1 \subset K_2 \subset L,$$

với K_1 là trường các phần tử của L bất biến dưới tác động của nhóm $\mathfrak{A}_4$ và K_2 là trường các phần tử của L bất biến dưới tác động của nhóm V_3. Khi đó mở rộng K_1/K là mở rộng bậc 2 chịu tác động của nhóm $\mathbb{Z}/2\mathbb{Z}$, K_2/K_1 là mở rộng bậc 3 chịu tác động của nhóm $\mathbb{Z}/3\mathbb{Z}$ và L/K_2 là mở rộng bậc 4 chịu tác động của nhóm $(\mathbb{Z}/2\mathbb{Z})^2$. (Một mở rông L/K có bậc là n nếu như L là một K-không gian véc tơ n chiều.) Ta có thể tiếp tục lập luận như trên để thấy rằng đa thức bậc 4 có thể giải được bằng căn thức.

Phương pháp này không thực hiện được với phương trình bậc năm trở lên vì nhóm luân phiên $\mathfrak{A}_n$ của $\mathfrak{S}_n$ với $n \geqslant 5$ là một nhóm đơn. Điều này dẫn đến nhóm $\mathfrak{S}_n$ không thể biểu diễn được như mở rộng liên tiếp của các nhóm giao hoán.

Bài tập về Giải phương trình bậc thấp, nhóm Galois

Nhóm đối xứng và đa thức đối xứng

Cho tập hợp $T \neq \emptyset$. Khi ấy tập hợp $S(T)$ các song ánh (các phép thế) của T cùng với phép toán hợp thành lập thành một nhóm. Đặc biệt khi $T = \{1, 2, \ldots, n\}$ thì nhóm $S(T)$ được ký hiệu là S_n và được gọi là *nhóm đối xứng* trên n phần tử.

Với mỗi $\alpha \in S_n$ có thể biểu thị một cách tự nhiên như sau

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{pmatrix}.$$

Cho $x_1, x_2, \ldots, x_k$ là các phần tử phân biệt của $T = \{1, 2, \ldots, n\}$. Ta ký hiệu $(x_1, x_2, \ldots, x_k)$ là ánh xạ biến các phần tử khác x_i thành chính nó và biến x_i thành x_{i+1} (lấy modulo k). Phép thế này được gọi là một xích có độ dài k trên tập nền $x_1, \ldots, x_k$.

Bài tập 8.1. Mọi phép thế $\alpha \in S_n$ đều có thể phân tích thành tích của các xích có tập nền là rời rạc.

Bài tập 8.2. Biểu diễn các phép thế sau dưới dạng tích những xích rời rạc.

1. $$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 2 & 5 \end{pmatrix}.$$

2. $$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 3 & 1 & 6 \end{pmatrix}.$$

3.
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 2 & 4 & 1 \end{pmatrix}.$$

Cho $\alpha \in S_n$ là một phép thế, **dấu** của nó được định nghĩa bởi công thức
$$\operatorname{sgn}(\alpha) = \prod_{1 \leqslant i < j \leqslant n} \frac{\alpha(j) - \alpha(i)}{j - i}.$$
Một phép thế được gọi là chẵn nếu dấu của nó bằng 1, và là một phép thế lẻ nếu dấu của nó bằng -1.

Bài tập 8.3. Chứng minh rằng:

- $\operatorname{sgn}(\alpha \circ \beta) = \alpha\beta$.
- $\operatorname{sgn}((x_1, x_2, \ldots, x_k)) = (-1)^{k-1}$.

Bài tập 8.4. Cho $\alpha \in S_n$ là một phép thế. Chứng minh rằng α luôn có thể viết thành tích của các xích có độ dài 2 (không nhất thiết phải là rời rạc). Hơn thế nữa dù cách viết thế nào thì số lượng các xích phải luôn luôn chẵn hoặc luôn luôn lẻ.

Cho A là một vành giao hoán có đơn vị (ví dụ như $A = \mathbb{Z}$ tập hợp các số nguyên), một đa thức biến x lấy hệ số trên A là một hàm có dạng
$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$
trong đó n là một số tự nhiên nào đó, các $a_i \in A$. Kí hiệu $A[x]$ là tập hợp các đa thức có dạng như vậy. Ta hoàn toàn có thể đồng nhất đa thức $P(x)$ với bộ $(a_0, a_1, \ldots, a_n, \ldots)$ với các $a_i \in A$ và chỉ có hữu hạn các a_i là khác 0 (việc đồng nhất này có lợi thế đó là cho phép ta định nghĩa tổng và tích của 2 đa thức một cách dễ dàng hơn). Trên $A[X]$ ta có hai phép toán cộng và nhận đa thức như sau (chính là 2 phép toán cộng và nhân mà chúng ta đã biết)
$$(a_0, a_1, \ldots, a_n, \ldots) + (b_0, b_1, \ldots, b_n, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, \ldots),$$
$$(a_0, a_1, \ldots, a_n, \ldots).(b_0, b_1, \ldots, b_n, \ldots) = (c_0, c_1, \ldots, c_n, \ldots),$$
trong đó $c_i = \sum_{0 \leqslant k \leqslant i} a_k b_{i-k}$. Với hai phép toán này $A[x]$ của chúng ta là một vành giao hoán có đơn vị, vành này được gọi là vành các đa thức một biến lấy hệ số trên A.

Bằng quy nạp ta hoàn toàn có thể định nghĩa được vành các đa thức n biến $A[x_1, x_2, \ldots, x_n]$ lấy hệ số trên A là vành đa thức một biến lấy hệ số trên $A[x_1, \ldots, x_{n-1}]$, hay nói cách khác:

$$A[x_1, x_2, \ldots, x_n] = (A[x_1, x_2, \ldots, x_{n-1}])[x_n].$$

Một đa thức $P(x_1, x_2, \ldots, x_n) \in A[x_1, x_2, \ldots, x_n]$ được gọi là **đối xứng** nếu như ta hoán vị các biến $x_1, x_2, \ldots, x_n$ thì đa thức vẫn không thay đổi, hay nói một cách khác

$$P(x_1, x_2, \ldots, x_n) = P(x_{\alpha(1)}, x_{\alpha(2)}, \ldots, x_{\alpha(n)}) \quad \forall \alpha \in S_n.$$

Chúng ta có các đa thức n biến đối xưng *cơ bản* sau:

$$\begin{array}{rcccl}
a_1 & = & \sum_i x_i & = & x_1 + x_2 + \cdots + x_n \\
a_2 & = & \sum_{i<j} x_i x_j & = & x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\
& \ldots & & & \\
a_r & = & \sum_{i_1<i_2<\cdots<i_r} x_{i_1}x_{i_2}\ldots x_{i_r} & & \\
& \ldots & & & \\
a_n & = & x_1x_2\ldots x_n & & .
\end{array}$$

Bài tập 8.5 (Định lý về các đa thức đối xứng)**.** Chứng minh rằng mọi đa thức đối xứng $P(x_1, x_2, \ldots, x_n) \in A[x_1, x_2, \ldots, x_n]$ đều có thể viết được dưới dạng (duy nhất) một đa thức với các biến là các đa thức cơ bản ở trên với hệ số trên A, hay nói một cách khác $P \in A[a_1, a_2, \ldots, a_n]$. (Gợi ý: trên các đơn thức $x_1^{i_1}x_2^{i_2}\ldots x_n^{i_n}$ ta trang bị một quan hệ thứ tự như sau

$$x_1^{i_1}x_2^{i_2}\ldots x_n^{i_n} > x_1^{j_1}x_2^{j_2}\ldots x_n^{j_n}$$

nếu

$$\sum_k i_k > \sum_k j_k$$

hoặc $\sum_k i_k = \sum_k j_k$ thì phải có một chỉ số s nào đó thỏa mãn tính chất $i_k = j_k$ với mọi $k < s$ và $i_s > j_s$. Khi đó ta có thể chọn được $d_1, d_2, \ldots, d_n$ sao cho đơn thức lớn nhất của $a_1^{d_1}a_2^{d_2}\ldots a_n^{d_n}$ cũng là đơn thức lớn nhất của P. Bằng cách lấy P trừ đi một bội số của $a_1^{d_1}a_2^{d_2}\ldots a_n^{d_n}$ ta thu được đa thức mới có đơn thức lớn nhất nhỏ hơn đơn thức lớn nhất của P, từ đó nghĩ đến việc quy nạp.)

Đa thức bất khả quy

Cho A là một **miền phân tích duy nhất** (ví dụ như $A = \mathbb{Z}$ hoặc A là một trường như $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ hay $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ với p là một số nguyên tố,...). Một đa thức $P \in A[x]$ được gọi là **bất khả quy** nếu nó khác 0, không khả nghịch và không thể phân tích được thành tích của hai đa thức không khả nghịch có hệ số trong A.

Bài tập 8.6. Chứng minh rằng mọi đa thức $P \in A[x]$ đều có thể phân tích thành tích của các đa thức bất khả quy và phần tích này là duy nhất sai khác một cách sắp xếp các đa thức bất khả quy. (Chú ý ta coi hai đa thức bất khả quy sai khác một hằng số khả nghịch của A là như nhau).

Trong phần cuối này chúng ta quan tâm đến hai trường hợp hay gặp trong các kì thi học sinh giỏi quốc gia đó là $A = \mathbb{Z}$. Một trong những khó khăn khi làm việc trên vành $\mathbb{Z}[x]$ là ta không thể lúc nào cũng lấy các hệ số chia cho hệ số đầu của đa thức được, mà ta chỉ có thể lấy các hệ số chia cho ước chung lớn nhất của chúng. Chính sự phức tạp này dẫn chúng ta đến định nghĩa sau:

Định nghĩa 8.4. Cho $f = \sum_{i=0}^{n} a_i x^i \neq 0$ với $a_i \in \mathbb{Z}$. Ta gọi **lượng** của f là ước chung lớn nhất của các a_i và ký hiệu là $\text{cont}(f)$. Hay nói cách khác $\text{cont}(f) := \text{UCLN}(a_1, a_2, \ldots, a_n)$. Một đa thức f có $\text{cont}(f) = 1$ được gọi là một đa thức **nguyên thủy**.

Dễ dàng ta thấy $f = \text{cont}(f)g$ với g là một đa thức với hệ số nguyên có lượng là 1.

Bài tập 8.7 (Bổ đề Gauss)**.** Chứng minh rằng $\text{cont}(fg) = \text{cont}(f)\text{cont}(g)$.

Bài tập 8.8. Cho $f \in \mathbb{Z}[x]$. Chứng minh rằng f bất khả quy trên $\mathbb{Z}[x]$ khi và chỉ khi nó bất khả quy trên $\mathbb{Q}[x]$.

Bài tập 8.9 (Tiêu chuẩn Perron)**.** Giả sử

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

với bậc $n \geqslant 2, a_0 \neq 0$. Chứng minh rằng nếu

- $|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_1| + |a_0|$ thì $f(x)$ là đa thức bất khả quy trên $\mathbb{Z}[x]$.

- $|a_{n-1}| \geqslant 1 + |a_{n-2}| + \cdots + |a_1| + |a_0|$ và $f(\pm 1) \neq 0$ thì $f(x)$ là đa thức bất khả quy trên $\mathbb{Z}[x]$.

Bài tập 8.10 (IMO 1993)**.** Cho số tự nhiên $n > 1$. Chứng minh rằng đa thức $f(x) = x^n + 5x^{n-1} + 3$ là bất khả quy trong $\mathbb{Z}[x]$.

Bài tập 8.11. Đa thức $f(x) = x^{62} + 2013x^{61} + 2x^{60} + 3x^{59} + \cdots + 61x + 62$ bất khả quy trong $\mathbb{Z}[x]$.

Bài tập 8.12 (Tiêu chuẩn Osada)**.** Cho $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x \pm p$ là đa thức với các hệ số nguyên và p là số nguyên tố. Chứng minh rằng

- Nếu $p > 1 + |a_1| + \cdots + |a_{n-1}|$ thì $f(x)$ là bất khả qui.
- Nếu $p \geqslant 1 + |a_1| + \cdots + |a_{n-1}|$ và các nghiêm của đơn vị không phải là nghiệm của $f(x)$ thì $f(x)$ là bất khả qui.

Bài tập 8.13 (Tiêu chuẩn Osada mở rộng)**.** Cho $f(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x \pm pr$ là đa thức với các hệ số nguyên, p là số nguyên tố và $r \in \mathbb{Z}$, $r \neq 0$. Nếu $p > |r|^{r-1} + |a_1r^{n-2}| + \cdots + |a_{n-2}r| + |a_{n-1}|$ thì $f(x)$ là bất khả qui trong $\mathbb{Z}[x]$.

Bài tập 8.14. Nếu $4|a| + 2|b| + |c| < 1001$ thì đa thức $q(x) = x^4 + ax^3 + bx^2 + cx - 2018$ bất khả quy trong $\mathbb{Z}[x]$.

Bài tập 8.15. Đa thức $p(x) = x^9 + x^8 + \cdots + x^2 + x + 11$ luôn luôn là bất khả quy.

Bài tập 8.16. Chứng minh rằng mọi đa thức với hệ số nguyên luôn có thể viết dưới dạng tổng của hai đa thức hệ số nguyên bất khả quy trên $\mathbb{Z}$.

Bài tập 8.17 (Tiêu chuẩn Polya)**.** Cho $f(x)$ là đa thức bậc n với các hệ số nguyên. Đặt $m = \left[\dfrac{n+1}{2}\right]$. Giả sử cho n số nguyên khác nhau $d_1, \ldots, d_n$ có $|f(d_i)| < \dfrac{m!}{2^m}$ và các số d_i đều không là nghiệm của $f(x)$. Chứng minh rằng $f(x)$ là đa thức bất khả qui.

Bài tập 8.18. Với các số nguyên phân biệt $a_1, a_2, \ldots, a_n$, ký hiệu đa thức $f(x) = (x - a_1)(x - a_2)\ldots(x - a_n)$. Chứng minh rằng $f(x) - 1$ là đa thức bất khả quy trên $\mathbb{Z}$.

Bài tập 8.19 (Tiêu chuẩn Eisenstein)**.** Cho $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0, a_n \neq 0$, là đa thức với các hệ số nguyên và p là số nguyên tố sao cho a_n không chia hết cho p và các a_i với $i < n$ chia hết cho p, nhưng a_0 không chia hết cho p^2. Khi đó $f(x)$ là đa thức bất khả qui trên $\mathbb{Z}$.

Bài tập 8.20 (Tiêu chuẩn Eisenstein suy rộng)**.** Cho $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $a_n \neq 0$, $n > 1$, là đa thức với các hệ số nguyên và p là số nguyên tố sao cho a_n không chia hết cho p và các a_i chia hết cho p với $i = 0, 1, \ldots, k$ và a_0 không chia hết cho p^2. Nếu $f(x)$ biểu diễn được thành tích của hai đa thức với hệ số nguyên, $f(x) = g(x)h(x)$, thì bậc của một trong hai đa thức $g(x)$ hoặc $h(x)$ không nhỏ hơn $k + 1$.

Bài tập 8.21. Cho $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ là đa thức với các hệ số nguyên và p là số nguyên tố sao cho a_n không chia hết cho p nhưng $a_0, a_1 \ldots, a_k$ chia hết cho p, a_0 không chia hết cho p^2. Khi đó $f(x)$ có nhân tử bất khả qui bậc $\geqslant k + 1$.

Bài tập 8.22. Với bất kỳ số nguyên tố p đa thức $f(x) = 1 + x + \cdots + x^{p-1}$ là bất khả quy trên $\mathbb{Z}$.

Bài tập 8.23. Với bất kỳ số nguyên dương n đa thức $f(x) = 1 + x + \dfrac{x^2}{2!} + \cdots + \dfrac{x^n}{n!}$ là bất khả quy trên $\mathbb{Q}$.

Cho $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ là đa thức với các hệ số nguyên. p là một số nguyên tố. Ta ký hiệu $\overline{f}_p(x) = \overline{a}_n x^n + \overline{a}_{n-1}x^{n-1} + \cdots + \overline{a}_0 \in \mathbb{F}_p[x]$. Trong đó $\overline{a}_i$ là phần dư của phép chia a_i cho p.

Bài tập 8.24 (Tiêu chuẩn rút gọn modulo p)**.** Cho $f \in \mathbb{Z}[x]$. Giả sử rằng tồn tại số nguyên tố p sao cho $\deg(f) = \deg(\overline{f}_p)$ và $\overline{f}_p$ bất khả quy trong $\mathbb{F}_p[x]$ thì f là một đa thức bất khả quy.

Bài tập 8.25 (Tiêu chuẩn Berlekamp)**.** Cho $f \in \mathbb{F}_p[x]$ bậc n thỏa mãn tính chất $\text{UCLN}(f, f') = 1$. Gọi V là tập hợp các đa thức có bậc nhỏ hơn n lấy hệ số trên $\mathbb{F}_p$. Ta xét ánh xạ tuyến tính $T : V \to V; g \mapsto g^p \mod f$. Ở đây $g^p \mod f$ là phần dư nhận được từ phép chia g^p cho đa thức f.

Xét hệ phương trình

$$\begin{cases} (a_{1,1}-1)x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n = 0 \\ a_{2,1}x_1 + (a_{2,2}-1)x_2 + \cdots + a_{2,n}x_n = 0 \\ \cdots \\ a_{n,1}x_1 + a_{n,2}x_2 + \cdots + (a_{n,n}-1)x_n = 0 \end{cases}$$

với $a_{i,j}$ là các hệ số của

$$T(x^i) = a_{1,i+1} + a_{2,i+1}x + \cdots + a_{n,i+1}x^{n-1}.$$

Chứng minh rằng f là đa thức bất khả quy khi và chỉ khi nghiệm tổng quát của hệ phương trình trên chỉ có một biến tự do.

Bài tập 8.26. Chứng minh rằng $f = x^5 + x^4 + 1 \in \mathbb{F}_2[x]$ là đa thức bất khả quy.

CHƯƠNG 9

Phân bố số nguyên tố

Trong bài giảng này chúng ta trình bày về sự phân bố của các số nguyên tố. Tài liệu tham khảo cho bài giảng này là chương 7: "Định lý Chebyshev về phân bố của số nguyên tố" trong uốn sách "Giới thiệu về lý thuyết số giải tích" của Chandrasekharan (xem [3]).

Định lý 9.1 (Định lý về số nguyên tố)**.** *Cho x là một số thực dương. Ta kí hiệu $\pi(x)$ là số các số nguyên tố nhỏ hơn hoặc bằng x. Khi đó ta có:*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

Nhận xét 9.2.

- *Để có thể đánh giá tốt hơn về sự phân bố của số nguyên tố ta cần phải sử dụng nhiều công cụ về giải tích hơn. Đánh giá tốt nhất về sự phân bố của số nguyên tố liên quan đến giả thuyết của Riemann. Đây là một bài toán rất khó và hiện nay vẫn chưa có lời giải.*
- *Qua công thức xuất hiện trong định lý về phân bố số nguyên tố ở trên, ta thấy rằng số các số nguyên tố có nhiều hơn ta nghĩ.*

$$\begin{aligned}
&\pi(x) \approx x/\log x;\\
&\pi(x) \gg x^{1/2},\, x^{2/3};\\
&\pi(x) \gg x^{\alpha},\ \forall \alpha < 1;\\
&\lim_{x\to\infty} \frac{\pi(x)}{x^{\alpha}} = \infty,\ \forall \alpha < 1.
\end{aligned}$$

Trong bài giảng này chúng ta sẽ không trình bày cách chứng minh của định lý về số nguyên tố. Chúng ta chỉ tìm hiểu về dạng yếu của nó được phát biểu và chứng minh bởi Chebyshev.

Định lý 9.3 (Chebyshev)**.** *Luôn tồn tại hai số thực dương* $a, A \in \mathbb{R},\ 0 < a < A$ *sao cho*

$$a\frac{x}{\log x} < \pi(x) < A\frac{x}{\log x}$$

đúng với mọi $x > 0$.

Nhận xét 9.4. *Để chứng minh được định lý về số nguyên tố, ta cần phải chứng minh được định lý của Chebyshev (được phát biểu ở trên). Sau đó ta mới sử dụng các công cụ hiện đại của giải tích phức như hàm zeta, ... để chứng minh* $\lim\limits_{x\to\infty}\frac{\pi(x)}{x/\log x} = 1$ *(xem thêm [3, p. 65-70])*

Ý tưởng của Chebyshev là ta có thể thay hàm đếm các số nguyên tố $\pi(x) = \sum_{p\leqslant x} 1$ bằng những hàm dễ thao tác hơn. Cụ thể là Chebyshev đã thay hàm $\pi(x)$ bằng các hàm:

$$\theta(x) = \sum_{p\leqslant x} \log(p),$$
$$\psi(x) = \sum_{p^n\leqslant x} \log(p).$$

Ví dụ 9.5. *Với* $x = 10$ *ta có giá trị của các hàm phía trên là:*

$$\pi(10) = 4$$
$$\theta(10) = \log(2) + \log(3) + \log(5) + \log(7)$$
$$\psi(10) = 3\log(2) + 2\log(3) + \log(5) + \log(7)$$

Định lý 9.6. *Xét các giới hạn trên và dưới sau:*

$$\ell_1 = \underline{\lim_{x\to\infty}}\frac{\pi(x)}{x/\log x};\quad L_1 = \overline{\lim_{x\to\infty}}\frac{\pi(x)}{x/\log x}$$
$$\ell_2 = \underline{\lim_{x\to\infty}}\frac{\theta(x)}{x};\quad L_2 = \overline{\lim_{x\to\infty}}\frac{\theta(x)}{x}$$
$$\ell_3 = \underline{\lim_{x\to\infty}}\frac{\psi(x)}{x};\quad L_3 = \overline{\lim_{x\to\infty}}\frac{\psi(x)}{x}$$

Khi đó ta có

$$\ell_1 = \ell_2 = \ell_3,$$
$$L_1 = L_2 = L_3.$$

Chứng minh. Từ định nghĩa của các hàm $\pi(x), \theta(x), \psi(x)$ ta có

$$\theta(x) \leqslant \psi(x) \leqslant \pi(x)\log(x).$$

(Bất đẳng thức cuối thu được là do

$$\begin{aligned}\psi(x) = \sum_{p^n \leqslant x} \log(p) \quad &\leqslant \textstyle\sum_{p^n \leqslant x} \log(x) = \left(\sum_{p^n \leqslant x} 1\right)\log(x) \\ &\leqslant \left(\textstyle\sum_{p \leqslant x} 1\right)\log(x) = \pi(x)\log(x).)\end{aligned}$$

Điều này dẫn đến

$$\overline{\lim_{x\to\infty}} \frac{\theta(x)}{x} \leqslant \overline{\lim_{x\to\infty}} \frac{\psi(x)}{x} \leqslant \overline{\lim_{x\to\infty}} \frac{\pi(x)}{x/\log x}.$$

Để chứng minh bất đẳng thức ngược lại, ta cố định một số $0 < \alpha < 1$ và chỉ xét các số nguyên tố $x^\alpha < p \leqslant x$. Ta có

$$\begin{aligned}\theta(x) &\geqslant \sum_{x^\alpha < p \leqslant x} \log(p) \\ &> \log(x^\alpha) \sum_{x^\alpha < p \leqslant x} 1 = \alpha\log(x) \sum_{x^\alpha < p \leqslant x} 1 = \alpha\log(x)(\pi(x) - \pi(x^\alpha)).\end{aligned}$$

Mặt khác ta lại có $\pi(x^\alpha) < x^\alpha$ nên

$$\theta(x) \geqslant \alpha\pi(x)\log(x) - \alpha x^\alpha \log(x).$$

Đem chia cả hai vế của bất đẳng thức cho $x > 0$ ta được:

$$\frac{\theta(x)}{x} > \alpha\frac{\pi(x)}{x/\log x} - \alpha\frac{\log(x)}{x^{1-\alpha}}.$$

Cho x tiến tới ∞, do $0 < 1-\alpha < 1$ nên $\lim_{x\to\infty} \frac{\log(x)}{x^{1-\alpha}} = 0$, vì thế ta có bất đẳng thức sau đúng với mọi $0 < \alpha < 1$:

$$\overline{\lim_{x\to\infty}} \frac{\theta(x)}{x} \geqslant \alpha \overline{\lim_{x\to\infty}} \frac{\pi(x)}{x/\log x}.$$

Lại cho α tiến tới 1, ta thu được bất đẳng thức cần chứng minh:

$$\overline{\lim_{x\to\infty}} \frac{\theta(x)}{x} \geqslant \overline{\lim_{x\to\infty}} \frac{\pi(x)}{x/\log x}.$$

Vậy ta vừa chứng minh được $L_1 = L_2 = L_3$.

Bài tập: Chứng minh $\ell_1 = \ell_2 = \ell_3$.

□

Nhận xét 9.7. *Sự tồn tại của hai số thực dương $0 < a < A$ trong định lý của Chebysev tương đương với* $\begin{cases} \underline{\lim}\limits_{x\to\infty} \frac{\pi(x)}{x/\log x} > 0 \\ \overline{\lim}\limits_{x\to\infty} \frac{\pi(x)}{x/\log x} < +\infty. \end{cases}$

Chứng minh định lý Chebyshev. Áp dụng Định lý 9.6 ta có

$$\ell = \underline{\lim_{x\to\infty}} \frac{\pi(x)}{x/\log x} = \underline{\lim_{x\to\infty}} \frac{\psi(x)}{x}, \quad L = \overline{\lim_{x\to\infty}} \frac{\pi(x)}{x/\log x} = \overline{\lim_{x\to\infty}} \frac{\theta(x)}{x}.$$

Để đánh giá ℓ và L ta sử dụng mẹo nhỏ sau đây:

Đặt $N := \binom{2n}{n} = \frac{(2n)!}{n!n!} = \frac{(n+1)\cdots(2n)}{n!}$. Ta để ý rằng tử số của N không chia hết cho p và mẫu số của nó thì lại chia hết cho p với mọi số nguyên tố $n < p < 2n$. Do đó $\prod\limits_{n<p<2n} p \mid N$. Điều này dẫn đến

$$\sum_{n<p<2n} \log(p) \leqslant \log(N). \tag{9.1}$$

- Ta sẽ chứng minh rằng: $\frac{\theta(x)}{x} < 4\log(2)$. Điều này kéo theo

$$\overline{\lim_{x\to\infty}} \frac{\pi(x)}{x/\log x} = \overline{\lim_{x\to\infty}} \frac{\theta(x)}{x} \leqslant 4\log(2).$$

Đầu tiên ta sẽ đánh giá giá trị của $N = \binom{2n}{n}$. Sử dụng khai triển nhỉ thức Newton ta thu được

$$\binom{2n}{n} < (1+1)^{2n} = \sum_{i=1}^{2n} \binom{2n}{i} < (2n+1)\binom{2n}{n}.$$

Điều này dẫn đến:

$$\frac{2^{2n}}{2n+1} < N = \binom{2n}{n} \leqslant 2^{2n}. \tag{9.2}$$

Kết hợp (9.1) và (9.2) ta được

$$\theta(2n) - \theta(n) = \sum_{n<p<2n} \log(p) \leqslant \log(N) \leqslant 2n\log 2.$$

Cho $n = 2^i$ với $i \in \{0, 1, \ldots, m\}$ rồi cộng cả hai vế các bất đẳng thức nhận được, ta có:

$$\theta(2^m) - \theta(1) \leqslant (\log(2)) \sum_{r=1}^{m} 2^r = 2^{m+1} \log 2.$$

Với mọi số thực $x > 1$, ta luôn tìm được một số nguyên dương m sao cho $2^{m-1} \leqslant x < 2^m$. Do đó ta có

$$\theta(x) < \theta(2^m) < 2^{m+1} \log(2) \leqslant 4x \log(2).$$

Chia cả hai vế của bất đẳng thức với $x > 0$ ta thu được bất đẳng thức cần chứng minh.

- Ta sẽ chứng minh rằng: $\underline{\lim}_{x\to\infty} \frac{\psi(x)}{x} \geqslant \log 2$.

  Ta sẽ sử dụng phát biểu dễ chứng minh sau: Số mũ lớn n lớn nhất để p^n là ước của $m!$ trong đó p là một số nguyên tố là

$$\left\lfloor \frac{m}{p} \right\rfloor + \left\lfloor \frac{m}{p^2} \right\rfloor + \cdots .$$

Với $p \leqslant 2n$ số mũ lớn nhất của p xuất hiện trong cách biểu diễn thành các thừa số nguyên tố của:

+ tử số của N là:
$$\lfloor \frac{2n}{p} \rfloor + \lfloor \frac{2n}{p^2} \rfloor + \cdots ;$$

+ của mẫu số của N là:
$$2 \left(\lfloor \frac{2n}{p} \rfloor + \lfloor \frac{2n}{p^2} \rfloor + \cdots \right).$$

Vậy số mũ của p trong N là:

$$\nu_p = \sum_{r \geqslant 1}^{M_p} \left(\left\lfloor \frac{2n}{p^r} \right\rfloor - 2 \left\lfloor \frac{n}{p^r} \right\rfloor \right),$$

với $M_p = \left\lfloor \frac{\log(2n)}{\log(p)} \right\rfloor$. Mặt khác với mọi $y > 0$ ta luôn có: $\lfloor 2y \rfloor - 2\lfloor y \rfloor \in \{0, 1\}$ nên

$$N = \prod_{p \leqslant 2n} p^{\nu_p} \leqslant \prod_{p \leqslant 2n} p^{M_p}.$$

Lấy logarit cả hai vế ta được

$$\log(N) \leqslant M_p \sum_{p \leqslant 2n} \log(p). \tag{9.3}$$

Ta lại có

$$\psi(2n) = \sum_{p \leqslant 2n} \left\lfloor \frac{\log(2n)}{\log p} \right\rfloor \log(p) = \sum_{p \leqslant 2n} M_p \log(p). \tag{9.4}$$

Kết hợp (9.2), (9.3) và (9.4) ta có

$$\psi(2n) \geqslant \log(N) > 2n \log(2) - \log(2n+1).$$

Thay $n = \left\lfloor \frac{x}{2} \right\rfloor$ với x là một số thực dương bất kì vào bất đẳng thức ta có

$$\psi(x) \geqslant \psi(2n) > (x-2)\log 2 - \log(x+1).$$

Chia cả hai vế bất đẳng thức cho $x > 0$ ta nhận được:

$$\frac{\psi(x)}{x} > \frac{x-2}{x}\log(2) - \frac{\log(x+1)}{x}.$$

Do $\lim\limits_{x\to\infty} \dfrac{x-2}{x} = 1$ và $\lim\limits_{x\to\infty} \dfrac{\log(x+1)}{x} = 0$ nên bất đẳng thức trên kéo theo:

$$\varliminf_{x\to\infty} \frac{\psi(x)}{x} \geqslant \log(2).$$

□

Bài tập về Phân bố số nguyên tố

Bài tập 9.1. Cho n là một số nguyên dương. Chứng minh rằng $C_{2n}^{n} \geqslant \frac{4^n}{2n}$.

Bài tập 9.2. Cho p là một số nguyên tố, gọi $r(p,n)$ là bậc p-adic của C_{2n}^{n} (nghĩa là số nguyên dương lớn nhất sao cho p^r là ước của C_{2n}^{n}). Chứng minh rằng $p^{r(p,n)} \leqslant 2n$.

Bài tập 9.3. Chứng minh rằng nếu p là số nguyên tố lẻ và $\frac{2n}{3} < p \leqslant n$, thì $r(p,n) = 0$.

Bài tập 9.4. Cho x là một số thực lớn 3. Ký hiệu $f(x)$ là tích các số nguyên tố nhỏ hơn hoặc bằng x. Chứng minh rằng $f(x) < 2^{2x-3}$.

Bài tập 9.5 (Định đề của Bertrand)**.** Chứng minh rằng với $n \geqslant 2$, luôn tồn tại một số nguyên tố thỏa mãn tính chất $n < p < 2n$.

Bài tập 9.6. Chứng minh các bất đẳng thức sau:

- Nếu n là số nguyên dương chẵn khi đó ta có
$$C_{\frac{3n}{2}}^{n} < \left(\frac{135}{20}\right)^{\frac{n}{2}}.$$
- Nếu n là số nguyên dương chẵn thỏa mãn tính chất $n > 152$ khi đó
$$C_{\frac{3n}{2}}^{n} > \left(\frac{13}{2}\right)^{\frac{n}{2}}.$$
- Nếu n là số nguyên dương lẻ và $n > 7$ thì
$$C_{\frac{3n+1}{2}}^{n} < \left(\frac{135}{20}\right)^{\frac{n-1}{2}}.$$
- Nếu $n > 945$ thì
$$\left(\frac{13}{2\sqrt{27}}\right)^{n} > (3n)^{\frac{\sqrt{3n}}{2}}.$$

Bài tập 9.7. Chứng minh rằng:

- Nếu n là một số nguyên dương chẵn khi đó

$$\prod_{\frac{n}{2}<p\leqslant\frac{3n}{4}} p.\prod_{n<p\leqslant\frac{3n}{2}} p < C^n_{\frac{3n}{2}}.$$

- Nếu n là số lẻ thì

$$\prod_{\frac{n+1}{2}<p\leqslant\frac{3n}{4}} p.\prod_{n<p\leqslant\frac{3n+1}{2}} p < C^n_{\frac{3n+1}{2}}.$$

Bài tập 9.8 (Bachraoui, 2006)**.** Chứng minh rằng với mọi số nguyên dương n lớn hơn 1, luôn tồn tại số nguyên tố thỏa mãn tính chất $2n < p < 3n$.

Bài tập 9.9. Chứng minh rằng với mọi số nguyên dương n lớn hơn 1, luôn tồn tại số nguyên tố thỏa mãn tính chất $n < p < \frac{3n+1}{2}$.

Bài tập 9.10 (xem [8])**.** Tất cả các số $k < 100000000$ thỏa mãn tính chất trong đoạn $(kn, (k+1)n)$ luôn có một số nguyên tố với mọi $n > 1$ là $1, 2, 3, 5, 9, 14$.

Tài liệu tham khảo

[1] T. Andreescu, D. Andrica, I. Cucurezeanu, *An Introduction to Diophantine Equations: A problem-based approach*, Birkhäuser, 2010.

[2] T. Andreescu, D. Andrica, Z. Feng, *104 Number Theory Problems: from the Training of the USA IMO Team*, Birkhäuser, 2006.

[3] K. Chandrasekharan, *Introduction to analytic number theory*, Grundlehren der mathematischen Wissenschaften, Vol. 148, 1968.

[4] G. A. Jones, J. M. Jones, *Elementary number theory*, Springer Undergraduate Mathematics Series, Springer, 2012.

[5] F. Lemmermeyer, *Reciprocity laws: From Euler to Eisenstein*, Springer-Verlag, 2000.

[6] I. Niven, H. S. Zuckerman, H. L. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley and Sons, New York, 1991. 5th edition.

[7] R. K. Pandley, A. Parashar, *On certain sums with quadratic expressions involving the Legendre symbol*, Journal of Integer Sequences, Vol. 21 (2018), Article 18.4.7.

[8] V. Shevelev, C. R. Greathouse IV, P. J. C. Moses,*On intervals* $(kn, k(n+1))$ *containing a prime for all* $n > 1$, Journal of Integers Sequences, Vol. 16 (2013), Article 13.7.3.