TRƯỜNG ĐẠI HỌC ĐÀ LẠT

GIÁO TRÌNH

LÝ THUYẾT SỐ

VŨ VĂN THÔNG

MỤC LỤC

1 SỐ NGUYÊN **3**

1.1 Vành số nguyên 3
1.2 Các tính chất cơ bản của $\mathbb{Z}$ 4
1.3 Phép chia trong $\mathbb{Z}$ 6
1.4 Biểu diễn số nguyên 7

2 ƯỚC CHUNG LỚN NHẤT. SỰ PHÂN TÍCH RA THỪA SỐ NGUYÊN TỐ. **13**

2.1 Ước chung lớn nhất 13
2.2 Thuật toán Euclid 15
2.3 Định lý cơ bản của số học 17
2.4 Phương trình Diophantus tuyến tính 19

3 ĐỒNG DƯ **25**

3.1 Khái niệm đồng dư 25
3.2 Các đồng dư tuyến tính 28
3.3 Định lý phần dư Trung hoa 30
3.4 Hệ các đồng dư tuyến tính 31
3.5 Định lý Wilson và định lý Euler 34

4 CÁC HÀM SỐ HỌC **43**

4.1 Nhận xét chung 43
4.2 Hàm Euler $\varphi(n)$. 46
4.3 Hàm tổng các ước $\sigma(n)$ và số các ước $\tau(n)$. 48
4.4 Hàm Möbius $\mu(n)$. 51

5 CĂN NGUYÊN THỦY **57**
5.1 Bậc của số nguyên và căn nguyên thuỷ 57
5.2 Căn nguyên thuỷ của số nguyên tố 61
5.3 Các số có căn nguyên thuỷ 64
5.4 Chỉ số số học 69

6 THẶNG DƯ BÌNH PHƯƠNG **75**
6.1 Thặng dư bình phương 75
6.2 Luật thuận nghịch bình phương 80
6.3 Ký hiệu Jacobi 84
6.4 Số giả nguyên tố Euler 87

7 SỐ b- PHÂN. PHÂN SỐ LIÊN TỤC **97**
7.1 Số b-phân 97
7.2 Phân số liên tục hữu hạn 102
7.3 Phân số liên tục vô hạn 108
7.4 Vài ứng dụng của phân số liên tục 118

8 MỘT VÀI PHƯƠNG TRÌNH DIOPHANTUS PHI TUYẾN **125**
8.1 Các bộ ba Pythagoras 125
8.2 Tổng của hai số chính phương 126
8.3 Tổng của bốn số chính phương 128
8.4 Phương trình Pell 131

1

SỐ NGUYÊN

1.1 Vành số nguyên

Vành số nguyên $\mathbb{Z}$ là mở rộng nhỏ nhất của tập số tự nhiên $\mathbb{N}$ cùng với các phép toán cộng và nhân sao cho phương trình $a+x=b$ luôn luôn có nghiệm. Nghiệm duy nhất x của phương trình $a+x=b$ được ký hiệu là $b-a$.

Định lý 1.1. *Có vành $\mathbb{Z}$ với các phép toán cộng (ký hiệu: +), nhân ($\cdot$) và ánh xạ $f:\mathbb{N}\longrightarrow\mathbb{Z}$ sao cho:*

1. *f vừa là đơn cấu nửa nhóm cộng vừa là đơn cấu nửa nhóm nhân.*
2. *Các phần tử của $\mathbb{Z}$ đều có dạng $f(a)-f(b)$ với $a,b\in\mathbb{N}$.*

Chứng minh. Quan hệ hai ngôi ϱ trên tích Descartes $\mathbb{N}\times\mathbb{N}$ xác định bởi:
$(a,b)\varrho(c,d)$ nếuu $a+d=b+c$ là quan hệ tương đương.
Ta ký hiệu tập thương $\mathbb{N}\times\mathbb{N}/\varrho$ là $\mathbb{Z}$ và gọi nó là vành (?!) số nguyên. Như vậy, mỗi số nguyên là một lớp tương đương và nếu nó chứa đại diện (m,n) ta sẽ tạm ký hiệu nó là $\overline{(m,n)}$.

Phép cộng và nhân trên $\mathbb{Z}$ được định nghĩa như sau:

$\overline{(a,b)}+\overline{(c,d)}=\overline{(a+c,b+d)}$.

$\overline{(a,b)}\cdot\overline{(c,d)}=\overline{(ac+bd,ad+bc)}$.

Xem như bài tập, yêu cầu đọc giả tự kiểm tra tính đúng đắn của định nghĩa các phép toán nêu trên và chứng tỏ rằng $(\mathbb{Z},+,\cdot)$ là một vành giao hoán với phần tử trung hoà của phép cộng và của phép nhân tương ứng là

$0 = \overline{(0,0)}$, $1 = \overline{(1,0)}$.

Ánh xạ $f : \mathbb{N} \longrightarrow \mathbb{Z}$ xác định bởi: $f(n) = \overline{(n,0)}$.

1. Dễ dàng thấy rằng f là đơn ánh và:

$$f(a+b) = \overline{(a+b,0)} = \overline{(a,0)} + \overline{(b,0)} = f(a) + f(b)$$

$$f(a \cdot b) = \overline{(ab,0)} = \overline{(a,0)} \cdot \overline{(b,0)} = f(a) \cdot f(b)$$

2. Giả sử $x = \overline{(a,b)} \in \mathbb{Z}$. Khi đó:

$$x = \overline{(a,0)} + \overline{(0,b)} = \overline{(a,0)} - \overline{(b,0)} = f(a) - f(b).$$

■

Nhận xét:

1) Ta đồng nhất mỗi số tự nhiên n với ảnh $f(n) \in \mathbb{Z}$; do đó $\mathbb{N} \subset \mathbb{Z}$.

2) Nếu $a, b \in \mathbb{N}, a > b$ thì số nguyên $x = \overline{(a,b)} = \overline{(a-b,0)} = f(a-b)$; do có sự đồng nhất nên x chính là số tự nhiên $n = a - b$ và ta gọi nó là số nguyên dương, ta viết $x = n$.

Nếu $a, b \in \mathbb{N}, a < b$ thì số nguyên $x = \overline{(a,b)} = -\overline{(b-a,0)} = -f(b-a)$; như vậy x chính là số đối của số tự nhiên $n = b - a$ và ta gọi nó là số nguyên âm, ta viết: $x = -n$.

Số nguyên $x = \overline{(n,n)}$ chính là số 0.

1.2 Các tính chất cơ bản của $\mathbb{Z}$

Vành R được gọi là một miền nguyên nếuu với mọi $x, y \in R : x \neq 0, y \neq 0$ kéo theo $xy \neq 0$.

Định lý 1.2. *$\mathbb{Z}$ là miền nguyên, đếm được, chứa $\mathbb{N}$ như là nửa nhóm con cộng và nửa nhóm con nhân. Mọi vành cực tiểu chứa $\mathbb{N}$ như là nửa nhóm con cộng và nửa nhóm con nhân đều đẳng cấu vành với $\mathbb{Z}$.*

Chứng minh. Ta đã biết vành số nguyên $\mathbb{Z}$ gồm các số tự nhiên n và các số đối $-n$; từ đây dễ dàng suy ra rằng $\mathbb{Z}$ là miền nguyên, đếm được, cực tiểu chứa $\mathbb{N}$ như là nửa nhóm con cộng và nửa nhóm con nhân.

Giả sử X là một vành cực tiểu có ánh xạ $g : \mathbb{N} \longrightarrow X$ vừa là đơn cấu nửa nhóm cộng vừa là đơn cấu nửa nhóm nhân. Vậy thì X chỉ gồm các phần tử $g(n)$ và $-g(n), n \in \mathbb{N}$. Dễ dàng thấy rằng ánh xạ $\varphi : \mathbb{Z} \longrightarrow X, \pm n \longmapsto \pm g(n)$ là một đẳng cấu vành. ■

Vành giao hoán R cùng với một quan hệ thứ tự toàn phần $\leq$ được gọi là vành được sắp thứ tự nếuu với mọi $x, y \in R$ đều thỏa :

1. $\forall z \in R\ (x \leq y \Rightarrow x + z \leq y + z)$
2. $0 \leq x, 0 \leq y \Rightarrow 0 \leq xy$

Trên $\mathbb{Z}$ ta đưa ra quan hệ 2-ngôi $\leq$ như sau: $x \leq y$ nếuu $y - x \in \mathbb{N}$. Dễ thấy đây là quan hệ thứ tự trên $\mathbb{Z}$ và là mở rộng của quan hệ thứ tự trên $\mathbb{N}$.

Định lý 1.3. *$\mathbb{Z}, \leq$ là một vành được sắp thứ tự Archimed.*

Chứng minh. Xem như bài tập cho đọc giả ■

Trị tuyệt đối của số nguyên x, ký hiệu là $|x|$, được định nghĩa:

$$|x| = \begin{cases} x & \text{nếu } x \geq 0 \\ -x & \text{nếu } x \leq 0 \end{cases}$$

Các tính chất về trị tuyệt đối xem như đã rõ.

Định lý 1.4. *Giả sử M là tập không rỗng các số nguyên. Khi đó:*

1. *Nếu M bị chặn trên thì M chứa số lớn nhất.*
2. *Nếu M bị chặn dưới thì M chứa số nhỏ nhất.*

Chứng minh. Chúng tôi chỉ chứng minh cho trường hợp tập M là bị chặn trên.

Đặt $A = M \cap \mathbb{N}$. Nếu $A \neq \emptyset$ phần tử lớn nhất b của A sẽ là phần tử lớn nhất của M. Ngược lại, thì số $-b$ sẽ là phần lớn nhất của M với $b = \min \{-x : \ x \in M \}$.

Đọc giả tự chứng minh cho trường hợp tập M bị chặn dưới. ■

1.3 Phép chia trong $\mathbb{Z}$

Chúng ta nói rằng số nguyên a chia hết cho số nguyên $b \neq 0$, hay a là bội của b, ký hiệu $a \ \vdots \ b$, nếuu có số nguyên c để $a = bc$. Trong trường hợp này ta cũng nói là b chia chia hết a, hay b là ước (thừa số) cùa a, ký hiệu $b \mid a$. Ngược lại, ta nói rằng a không chia hết cho b, hay b không chia hết a, ký hiệu $b \nmid a$.

Ví dụ 1.3.1. $6 \mid 12$; $-5 \mid 20$; $7 \mid -49$; $-8 \mid -16$; $15 \mid 0$; $8 \nmid 12$; $-3 \nmid 8$; $4 \nmid -9$; $-12 \nmid -18$.

□

Dễ dàng chứng minh được định lý sau:

Định lý 1.5. *Giả sử a, b là các số nguyên. Khi đó:*

1. *Nếu $b \mid a$ và $a > 0, b > 0$ thì $1 \leq b \leq a$.*
2. *Nếu $b \mid a$ và $c \mid b$, thì $c \mid a$.*
3. *Nếu $b \mid a$ và $c \neq 0$ thì $bc \mid ac$.*
4. *Nếu $c \mid a$ và $c \mid b$, thì $c \mid (ma + nb)$ với các số nguyên m, n bất kỳ.*

Định lý 1.6. *Giả sử a, b là các số nguyên, $b \neq 0$. Khi đó tồn tại duy nhất các số nguyên q, r thỏa: $a = bq + r$ và $0 \leq r < |b|$.*

Chứng minh. Tập các số nguyên $M = \{bx : x \in \mathbb{Z} \, ; bx \leq a\}$ là không rỗng và bị chặn trên, theo định lý 1.4, M có số lớn nhất là bq. Ta có $bq \leq a$ và $a < bq + |b|$; suy ra $0 \leq r = a - bq < |b|$.

Giả sử ta có các biểu diễn: $a = bq_1 + r_1 = bq_2 + r_2; 0 \leq r_1, r_2 < |b|$. Thế thì: $|b| \cdot |q_1 - q_2| = |r_1 - r_2| < |b|$; suy ra $q_1 = q_2$ và do đó $r_1 = r_2$. ■

Khi $a = bq + r, 0 \leq r < |b|$ ta nói q là thương và r phần dư của phép chia a cho b. Hiển nhiên $b \mid a$ khi và chỉ khi $r = 0$.

Ví dụ 1.3.2. Phép chia 133 cho 21 có thương là 6 và phần dư là 7. Phép chia -50 cho 8 có thương là -7 và phần dư là 6. Phép chia 50 cho -8 có thương là -6 và phần dư là 2. Phép chia -133 cho -21 có thương là 7 và phần dư là 14.

□

Số nguyên 1 có đúng một ước dương. Mỗi số nguyên lớn hơn 1 đều có ít nhất hai ước dương vì nó chia hết cho 1 và chính nó.

Số nguyên lớn hơn 1 mà nó có đúng hai ước dương, được gọi là số nguyên tố.

Số nguyên lớn hơn 1 và không là số nguyên tố, được gọi là hợp số.

1.4 Biểu diễn số nguyên

Chúng ta đã quen với việc biểu diễn các số nguyên trong hệ đếm thập phân (hệ đếm cơ số mười). Bây giờ chúng ta sẽ chỉ ra rằng mỗi số nguyên $b > 1$ đều có thể được sử dụng làm cơ số cho việc biểu diễn các số nguyên. Và vì mỗi số nguyên âm là số đối của số nguyên dương nên định lý sau đây là căn bản.

Định lý 1.7. *Giả sử $b > 1$ là một số nguyên. Thế thì, mọi số nguyên dương n đều viết được một cách duy nhất dưới dạng*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

trong đó k là số nguyên không âm, các a_j là số nguyên với $0 \leq a_j \leq b-1$ và hệ số đầu tiên $a_k \neq 0$.

Chứng minh. Từ định lý 1.6 ta có:

$n = bq_0 + a_0, \quad 0 \leq a_0 \leq b-1.$

Nếu $q_0 \neq 0$, tiếp tục chia q_0 cho b ta được:

$q_0 = bq_1 + a_1, \quad 0 \leq a_1 \leq b-1.$

Tiếp tục quá trình này đến lúc đạt được:

$q_1 = bq_2 + a_2, \quad 0 \leq a_2 \leq b-1,$

$q_2 = bq_3 + a_3, \quad 0 \leq a_3 \leq b-1,$

$\vdots$

$q_{k-2} = bq_{k-1} + a_{k-1}, \quad 0 \leq a_{k-1} \leq b-1,$

$q_{k-1} = b.0 + a_k, \quad 0 \leq a_k \leq b-1.$

Dễ dàng suy ra:

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

với $0 \leq a_j \leq b-1,\ a_k = q_{k-1} \neq 0.$

Ta sẽ chứng minh tính duy nhất của biểu diễn bằng qui nạp theo số nguyên dương n.

Trường hợp $n = 1$ ta chỉ có biểu diễn duy nhất với $k = 0,$ và $a_0 = 1$. Giả sử ta có

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 = c_m b^m + c_{m-1} b^{m-1} + \cdots + c_1 b + c_0. \quad (*)$$

Do định lý 1.6: phần dư của phép chia n cho b là duy nhất, nên $a_0 = c_0$. Do $a_0 = c_0$ nên từ (*) ta suy ra:

$$n_1 = a_k b^{k-1} + a_{k-1} b^{k-2} + \cdots + a_1 = c_m b^{m-1} + c_{m-1} b^{m-2} + \cdots + c_1.$$

Dễ chứng tỏ được rằng $n_1 < n$, vậy theo giả thiết qui nạp ta có: $m = k$ và $a_1 = c_1, \cdots, a_k = c_k$. ■

Hệ quả 1.7.1. *Mọi số nguyên dương đều là tổng các lũy thừa khác nhau của* 2.

Chứng minh. Theo định lý 1.7 với $b = 2$, ta có

$$n = a_k 2^k + a_{k-1} 2^{k-1} + \cdots + a_1 2 + a_0,$$

với k là số tự nhiên, các a_j bằng 0 hoặc 1, $a_k \neq 0$. ■

Nhận xét:

1) Số nguyên dương $n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$ trong định lý 1.7 thường được viết là $(a_k a_{k-1} \cdots a_1 a_0)_b$.

2) Việc đổi số nguyên dương $(a_k a_{k-1} \cdots a_1 a_0)_q$ trong hệ đếm cơ số q sang cơ số b được thực hiện hoàn toàn tương tự như thuật toán tìm biểu diễn của số nguyên dương trong định lý 1.7 chỉ lưu ý là khi chia cho b (trong hệ $q-$phân) thì b đã được viết trong hệ $q-$phân, sau đó các số dư phải được đổi sang hệ $b-$phân để biểu diễn số trong hệ $b-$phân.

Ví dụ 1.4.1. Chúng ta cần đổi số thập phân 610 sang hệ nhị phân. Vì trong hệ thập phân nhị vẫn được viết là 2 nên ta thực hiện liên tiếp các phép chia cho 2 trong hệ thập phân:

$$106 = 2 \cdot 53 + 0,$$
$$53 = 2 \cdot 26 + 1,$$
$$26 = 2 \cdot 13 + 0,$$
$$13 = 2 \cdot 6 + 1,$$
$$6 = 2 \cdot 3 + 0,$$
$$3 = 2 \cdot 1 + 1,$$
$$1 = 2 \cdot 0 + 1.$$

Thuật chia dừng vì thương đã bằng 0. Các số dư viết trong hệ nhị phân tương ứng là: $c_0 = 0,\ c_1 = 1,\ c_2 = 0,\ c_3 = 1,\ c_4 = 0,\ c_5 = 1,\ c_6 = 1$; vậy số đã cho có biểu diễn trong hệ nhị phân là 1101010.

□

Ví dụ 1.4.2. Chúng ta cần đổi số thập phân 2003 sang hệ thập lục phân. Vì số thập lục trong hệ thập phân được viết là 16 nên ta thực hiện liên tiếp các phép chia cho 16 trong hệ thập phân:

$$2003 = 16 \cdot 125 + 3,$$

$$125 = 16 \cdot 7 + 13,$$

$$7 = 16 \cdot 0 + 7.$$

Thuật chia dừng vì thương đã bằng 0. Các số dư viết trong hệ thập lục phân tương ứng là: $c_0 = 3,\ c_1 = D,\ c_2 = 7$; vậy số đã cho có biểu diễn trong hệ thập lục phân là $7D3$.

□

BÀI TẬP CHƯƠNG I