QUAN HỆ CHIA HẾT TRÊN TẬP SỐ NGUYÊN

TRẦN HÀ SƠN

ĐẠI HỌC KHOA HỌC TỰ NHIÊN-ĐHQG TPHCM

Ngày 4 tháng 10 năm 2024

Overview

Hệ cơ số

Định lý

Giả sử b là một số nguyên lớn hơn 1, Khi đó mọi số nguyên n có thể được viết duy nhất dưới dạng

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

trong đó a_j là số nguyên thỏa $0 \leq a_j \leq b-1$, $j = 0, 1, \cdots, k$ và hệ số đầu tiên $a_k \neq 0$.

Ví dụ

$(1994)_{10} = (11111001010)_2 = (16246)_8$

Quan hệ chia hết trên tập số nguyên

Định nghĩa

Số nguyên a được gọi là chia hết cho một số nguyên b, hay b chia hết a nếu tồn tại một số nguyên c sao cho $a = bc$. Khi a chia hết cho b, ta kí hiệu là $a \vdots b$ hoặc $b|a$ và b được gọi là ước của a còn a được gọi là bội của b.

Lưu ý

a chia hết cho 0 khi và chỉ khi a bằng 0 nên bội của 0 là 0 còn tập các ước của 0 là tâp số nguyên $\mathbb{Z}$.

Quan hệ chia hết trên tập số nguyên

Tính chất

Số nguyên có các tính chất cơ bản như sau:

1. $1|a$ *với mọi* $a \in \mathbb{Z}$, $a|a$ *với mọi* $a \in \mathbb{Z}$.
2. *Nếu* $a|b$ *và* $b|c$ *thì* $a|c$.
3. *Nếu* $b \neq 0$ *và* $a|b$ *thì* $|a| \neq |b|$.
4. *Nếu* $a|b_i$ *thì* $a|\sum_{i=1}^{n} b_i x_i$ *với mọi* $x_i \in \mathbb{Z}$.
5. *Nếu* $a|b$ *và* $b|a$ *thì* $a = b$ *hoặc* $a = -b$.
6. *Quan hệ chia hết trong* $\mathbb{Z}$ *có tính phản xạ, bắc cầu nhưng không có tính đối xứng.*
7. *Quan hệ chia hết trong* $\mathbb{Z}$ *có tính phản đối xứng.*

Lưu ý

a chia hết cho 0 khi và chỉ khi a bằng 0 nên bội của 0 là 0 còn tập các ước của 0 là tâp số nguyên $\mathbb{Z}$.

Phép chia với dư

Định lý

Với mỗi cặp số nguyên a và $b \neq 0$, luôn luôn tồn tại duy nhất cặp số nguyên q, r với $0 \leq r < |b|$ sao cho

$$a = bq + r.$$

Lưu ý

a chia hết cho 0 khi và chỉ khi a bằng 0 nên bội của 0 là 0 còn tập các ước của 0 là tâp số nguyên $\mathbb{Z}$.

Khái niệm ước chung

Định nghĩa

Cho các số $a_1, a_2, \ldots, a_n$. Số nguyên d được gọi là một ước chung của các a_i nếu $d|a_i$ với mọi $i = 1, 2, \ldots, n$.

Lưu ý

- Nếu $a_1, a_2, \ldots, a_n$ không đồng thời bằng 0 thì ước chung của chúng là một tập hữu hạn khác rỗng.
- Nếu $a_1 = a_2 = \ldots = a_n = 0$ thì tập các ước chung của chúng là $\mathbb{Z}$.

Khái niệm ước chung lớn nhất

Định nghĩa

Cho các số $a_1, a_2, \ldots, a_n$. Số nguyên d được gọi là một **ước chung lớn nhất** của các a_i nếu $d|a_i$ với mọi $i = 1, 2, \ldots, n$ và d chia hết cho mọi ước chung của chúng, kí hiệu là $d = gcd(a_1, a_2, \ldots, a_n)$ hoặc $d = (a_1, a_2, \ldots, a_n)$. Nếu $d = 1$ thì các số $a_1, a_2, \ldots, a_n$ được gọi là nguyên tố cùng nhau.

Lưu ý

- Nếu $a_1, a_2, \ldots, a_n$ không đồng thời bằng 0 thì ước chung lớn nhất d của chúng là một số khác 0 và $-d$ cũng là ước chung lớn nhất của $a_1, a_2, \ldots, a_n$.
- Nếu $a_1 = a_2 = \ldots = a_n = 0$ thì $(a_1, a_2, \ldots, a_n) = 0$.

Thuật toán Euclide

Định lý

Giả sử c và d là các số nguyên, đồng thời $c = dq + r$, trong đó q, r là các số nguyên. Khi đó

$$(c, d) = (d, r).$$

Định lý (Thuật toán Euclide)

Giả sử $r_0 = a, r_1 = b$ là các số nguyên không âm, $b \neq 0$. Ta áp dụng liên tiếp thuật toán chia:

$$r_j = r_{j+1} q_{j+1} + r_{j+1}$$

thỏa $0 < r_{j+2} < r_{j+1}, j = 0, 1, \ldots, n-2, r_n = 0$. Khi đó $(a, b) = r_{n-1}$ (r_n là phần dư khác 0 cuối cùng của phép chia).

Thuật toán Euclide

Ví dụ (Thuật toán Euclide)

Tính $d = (24, 63)$.

Thuật toán Euclide

Định lý (Thuật toán Euclide)

Số phép chia cần thiết để thực hiện tìm ước chung lớn nhất của hai số nguyên a, b bằng thuật toán Euclide không vượt qua năm lần số chữ số thập phân của số bé trong hai số đã cho, nghĩa là

$$\log_{10} b \geq (n-1)\log_{10}\left(\frac{1+\sqrt{5}}{2}\right) > \frac{n-1}{5}.$$

Thuật toán Euclide

Hệ quả (Thuật toán Euclide)

Giả sử $a < b$, khi đó số phép tính bit cần thiết để thực hiện thuật toán Euclide là $O((\log_2 a)^3)$.

Thuật toán J.Stein

Lưu ý

Thuật toán dựa trên nhận xét đơn giản như sau:

- Nếu a và b cùng chẵn thì $(a, b) = 2(\frac{a}{2}, \frac{b}{2})$.
- Nếu a chẵn, b lẻ thì $(a, b) = (\frac{a}{2}, b)$.
- Nếu a, b đều lẻ thỉ $a - b$ chẵn và $(a, b) = (a - b, b)$.

Thuật toán Euclide mở rộng

Định lý

Ước chung lớn nhất của các số nguyên a và b là số nguyên dương d được biểu diễn dưới dạng tổ hợp tuyến tính của a và b. Nghĩa là tồn tại các số nguyên m, n sao cho

$$d = ma + nb.$$

Nhận xét

Dựa vào thuật toán Euclide, ta suy ra thiết kế sau:

- Bước 1: Gán $(x_0, y_0, r_0) = (1, 0, a)$ và $(x_1, y_1, r_1) = (0, 1, b)$.
- Bước k: Gán
  $(x_k, y_k, r_k) = (x_{k-2} - x_{k-1} * q_{k-1}, y_{k-2} - y_{k-1} * q_{k-1}, r_{k-2} - r_{k-1} * q_{k-1})$
  trong đó $q_{k-1} = \left[\frac{r_{k-2}}{r_{k-1}}\right]$.