§2. ƯỚC CHUNG - ƯỚC CHUNG LỚN NHẤT

A LÝ THUYẾT

Định nghĩa 2.3. Cho hai số nguyên a, b. Một số nguyên d là ước của a và b được gọi là ước chung của a và b.

Định nghĩa 2.4. Một số nguyên dương lớn hơn 1 chỉ có hai ước dương là 1 và chính nó được gọi là số nguyên tố.

Định nghĩa 2.5. Cho các số a, b khác 0, tập các ước chung của a và b là khác rỗng (vì luôn có số 1) và hữu hạn nên có số lớn nhất; khi đó số lớn nhất đó được gọi là ước chung lớn nhất của a và b. Kí hiệu là $\gcd(a;b)$, $UCLN(a;b)$ hay có thể chỉ đơn giản hơn là $(a;b)$.

Định nghĩa 2.6. Nếu ước chung lớn nhất của a và b bằng 1 thì a và b được gọi là nguyên tố cùng nhau.

Tính chất 2.3. Cho a, b là hai số nguyên.

(a) $(a;b) = (a;a-b)$.

(b) $d = (a;b)$ thì $(\frac{a}{a}, \frac{b}{d}) = 1$.

(c) Nếu $ax + by = m$ thì $(a,b) \mid m$.

Chứng minh.

(a) Đặt $d = (a,b), d' = (a, a-b)$. ta cần chứng minh $d = d'$. Ta có $d \mid a, d \mid b$ suy ra $d \mid (a-b)$. Do đó d là ước chung của a và $a-b$. Mà $d' = (a, a-b)$ nên theo định nghĩa ta có $d \leq d'$. (1)
Tương tự, $d' \mid a, d' \mid (a-b)$ suy ra $d' \mid [a-(a-b)]$ hay $d' \mid b$. Do đó d' là ước chung của a và b nên $d' \leq d$. (2)
Từ (1) và (2) ta có $d = d'$.

(b) Đặt $a = d \cdot a', b = d \cdot b'$, ta chứng minh $(a', b') = 1$. Giả sử ngược lại $(a', b') = m > 1$. Khi đó $a = d \cdot a' = d \cdot m \cdot a'', b = d \cdot m \cdot b''$, suy ra $md (> d)$ là ước chung của a, b vô lý vì d là ước chung lớn nhất của a và b. Vậy $(a', b') = \frac{a}{d}, \frac{b}{d} = 1$.

(c) Đặt $d = (a,b)$ ta có $d \mid a, d \mid b \Rightarrow\ d \mid (xa + yb)$ hay $d \mid m$.

Tính chất 2.4. Cho hai số nguyên a và b, d là nguyên dương, khi đó d là ước chung lớn nhất của a, b khi và chỉ khi d chia hết cho mọi ước chung khác của a và b.

Chứng minh. Gọi $e > 0$ là một ước chung của a và b, ta chứng minh $e \mid d$. Đặt $a = a' \cdot d, b = b' \cdot d$ khi đó $(a', b') = 1$.

Giả sử $d = qe + r$, trong đó $0 \leq r \leq e - 1$, ta có $a = a'(qe + r) = a'qe + a'r, b = b'(qe + r) = b'qe + b'r$.

Khi đó $e \mid a'r, e \mid b'r$, đặt $k = (e; r)$ ta có $e = k \cdot e', r = k \cdot r'$ và $(e'; r') = 1$.

Khi đó $ke' \mid a'kr'$, suy ra $e' \mid a'r'$ mà $(e'; r') = 1$ nên $e' \mid a'$.

Chứng minh tương tự thì $e' \mid b'$, suy ra $e' = 1$, $e = k$, $r = e \cdot r'$, suy ra $r = 0$, hay $d' \mid d$.

Tính chất 2.5. Cho a, b là hai số nguyên, khi đó với mọi số nguyên dương c thì $(ca; cb) = c \cdot (a; b)$.

Chứng minh. Đặt $d = (a; b)$ và $d' = (ac; bc)$, ta cần chứng minh $d' = cd$.

Ta có $d \mid a, d \mid b$ suy ra $dc \mid ac, dc \mid bc$, suy ra $dc \mid d'$ (1).

Mặt khác $c \mid ac, c \mid bc$ suy ra $c \mid d'$, đặt $d' = c \cdot d_1$ ta có $cd_1 \mid ac, cd_1 \mid bc$ suy ra $d_1 \mid a, d_1 \mid b$, do đó $d_1 \mid d$, suy ra $d' \mid cd$ (2)

Từ (1) và (2) ta có $d' = cd$ ta có điều cần chứng minh.

Tính chất 2.6. **Thuật toán Euclide tìm ước chung lớn nhất của hai số nguyên dương a và b.**

Đầu tiên ta chia a cho b được $r_1 (0 \leq r_1 < b)$, chia b cho r_1 được dư $r_2 (0 \leq r_2 < r_1)$, cứ tiếp tục như thế ta được dãy giảm các số nguyên không âm: $b, r_1, r_2, ...$ Do đó sẽ tồn tại n sao cho $r_{n+1} = 0$.

Khi đó ta có

$a = bq + r_1 (0 \leq r_1 < b)$

$b = r_1 q_1 + r_2 (0 \leq r_2 < r_1)$

$r_1 = r_2 q_2 + r_3 (0 \leq r_3 < r_2)$

....

$r_{n-2} = r_{n-1} qn - 1 + r_n (0 \leq r_n < r_{n-1})$

$r_{n-1} = r_n q_n$

Theo định lý 8 ta có $(a, b) = (b, r_1) = (r_1, r_2) = ...(r_n - 1, r_n) = r_n$.

Định lí 2.4. Cho a, b là các số nguyên và $d = \gcd(a; b)$. Khi đó tồn tại x, y nguyên sao cho

$$d = xa + yb$$

Chứng minh. Đặt $\mathrm{T} = \{xa + yb \mid x, y \in Z, xa + yb > 0\}$. Không mất tính tổng quát, ta có thể giả sử $a \neq 0$.

- Nếu $a > 0$, ta có $1.a + 0.b = a > 0$, suy ra $a \in T$.
- Nếu $a < 0$, ta có $-a = (-1).a + b.0 = -a > 0$, suy ra $-a \in T$. Vậy $T \neq \emptyset$.

- Khi đó T có phần tử nhỏ nhất, ta đặt $e = xa + yb$. Giả sử $a = ek + r$, với $0 \leq r < e$, suy ra $r = a - ek = a - (xa + yb).k = a(1 - xk) + b.yk$.

- Nếu $r > 0$ thì $r \leq e$ mâu thuẫn vì e là phần tử nhỏ nhất của T.

- Vậy $r = 0$ suy ra $e \mid a$. Chứng minh tương tự ta có $e \mid b$ do đó $e \mid d$.

- Mặt khác $d \mid a, d \mid b$ suy ra $d \mid (xa + yb)$ hay $d \mid e$. Từ đó ta có $d = e$.

Hệ quả 2.3. Cho các số a, b nguyên, gọi d là ước chung lớn nhất của a và b. Chứng minh rằng mọi ước khác của a và b đều là ước của d.

Chứng minh. Gọi $e \mid a, e \mid b$ là ước chung của a, b. Ta cần chứng minh $e \mid d$. Thật vậy theo tính chất trên thì tồn tại các số nguyên x, y sao cho $d = x \cdot a + y \cdot b$, hơn nữa $e \mid a, e \mid b$ nên $e \mid (x \cdot a + y \cdot b)$ hay $e \mid d$.

Hệ quả 2.4. Cho a, b là các số nguyên tố cùng nhau, khi đó tồn tại các số nguyên x, y sao cho

$$xa + yb = 1$$

Định lí 2.5. Cho các số nguyên a, m, n.

(a) Nếu $m \mid a, n \mid a$ và m, n nguyên tố cùng nhau thì $mn \mid a$.

(b) Nếu $a \mid mn$ và $(a, m) = 1$ thì $a \mid n$.

Chứng minh.

- Vì $m \mid a, n \mid a$ nên có hai số x, y sao cho $a = mx = ny$. Vì $(m, n) = 1$ nên có hai số nguyên u, v thõa mãn $um+vn = 1$. Nhân a vào hai vế ta có: $a = nym+mxvn = mn(uy+vx)$. Do đó $mn \mid a$.

- Vì $(a, m) = 1$ nên có hai nguyên x, y sao cho $ax + my = 1$. Suy ra $n = anx + mny$. Mà $a \mid mn$ nên ta có $a \mid (anx + mny)$ hay $a \mid n$.

Hệ quả 2.5. Cho b, c là ước của a và $(b; c) = 1$ thì $b \cdot c$ cũng là ước của a.

Chứng minh. Do b, c nguyên tố cùng nhau nên tồn tại x, y sao cho

$$x \cdot b + y \cdot c = 1(*)$$

Hơn nữa $b \mid a, c \mid a$ nên có các số nguyên m, n thỏa

$$a = m \cdot b = n \cdot c(**)$$

Từ (*) nhân 2 vế cho a ta có

$$a = x \cdot b \cdot (nc) + y \cdot c \cdot (mb) = (xn + ym) \cdot (bc)$$

Do đó $bc \mid a$.

Từ trên ta quy nạp thì có tính chất sau:

Tính chất 2.7. Cho nguyên a và k số nguyên $m_1, m_2, \cdots, m_k$ đôi một nguyên tố cùng nhau và là ước của a, khi đó tích $m_1 \cdot m_2 \cdots m_k$ cũng là ước của a.

Chứng minh. Quy nạp theo k

B VÍ DỤ

Ví dụ 2.6. Tìm hai số nguyên dương biết ước chung lớn nhất là 6 và tổng bằng 72.

Ví dụ 2.7. Chứng minh rằng với mọi n thì ước chung lớn nhất của $22n + 11$ và $33n + 16$ là 1.

Ví dụ 2.8. Chứng minh rằng với mọi số nguyên dương n thì các phân số sau tối giản:

(a) $\dfrac{n}{3n+1}$.

(b) $\dfrac{4n+7}{5n+9}$.

Ví dụ 2.9. Chứng minh rằng nếu a, b nguyên tố cùng nhau thì $a - b, a^2 + ab + b^2$ có ước chung lớn nhất là 1 hoặc 3.

Ví dụ 2.10. Chứng minh rằng nếu a, b nguyên dương, $(a, b) = 1$ và $ab = n^2$ với n nguyên dương thì tồn tại x, y sao cho $a = x^2, b = y^2$.

C BÀI TẬP RÈN LUYỆN

Bài 2.25. Chứng minh rằng với mọi số nguyên n thì $(22n + 7, 33n + 10) = 1$.

Bài 2.26. Chứng minh rằng với mọi số nguyên dương n thì các phân số sau là tối giản:

(a) $\dfrac{5n+7}{12n+18}$

(b) $\dfrac{n^2+5n+1}{n+5}$

Bài 2.27. Chứng minh rằng không có các số nguyên a, b thỏa mãn $(a, b) = 3$ và $a + b = 65$.

Bài 2.28. Chứng minh rằng có vô số cặp số nguyên a và b với $\gcd(a, b) = 5$ và $a + b = 65$.

Bài 2.29. Cho dãy u_n thỏa $u_1 = 1, u_2 = 1, u_{n+1} = u_n + u_{n-1}$ với mọi $n > 1$. Chứng minh rằng $\gcd(u_{n+1}, u_n) = 1$, với mọi số nguyên dương n.

Bài 2.30. Cho $\gcd(a, b) = d$, và x và y là các số nguyên sao cho $a = xd$ và $b = yd$, hãy chỉ ra rằng $\gcd(x; y) = 1$.

Bài 2.31. Chứng minh rằng nếu $\gcd(a; b) = 1$ và $\gcd(a; c) = 1$, thì $\gcd(a; bc) = 1$.