§2. Ước chung – Bội chung

1. Ước chung – Ước chung lớn nhất

Định nghĩa. Cho hai số nguyên a và b. Số nguyên q được gọi là ước chung của a và b nếu a, b đều chia hết cho q.

Định nghĩa. Số dương d được gọi là ước chung lớn nhất của a và b nếu d > 0 và chia hết cho mọi ước chung khác của a và b. Kí hiệu d = gcd(a,b) hay d = (a,b).

Định nghĩa. Nếu ước chung lớn nhất của a và b bằng 1 ta nói a và b nguyên tố cùng nhau.

Định lý. Nếu $d = \gcd(a,b)$ thì $\gcd\left(\frac{a}{d},\frac{b}{d}\right) = 1$.

Định lý. Cho a, b là các số nguyên dương. Khi đó tồn tại các số nguyên x, y sao cho $xa + yb = \gcd(a,b)$.

Chứng minh. Xét tập $A = \{m = xa + yb | x, y \in Z, xa + yb > 0\}$

Ta có $A \neq \emptyset$ vì $1.a + 0.b = a > 0$ và $A \subset N$ nên tồn tại $k = \min A$. Ta chứng minh $k = d$

Giả sử $a = kq + r, 0 \leq r < k$ khi đó $r = a - kq = a - q(xa + yb) = (1 - xq)a - yqb$ mà $r < k$, suy ra $r = 0$. Do đó $k|a$, tương tự ta cũng có $k|b$.

Giả sử m là một ước bất kì của a, b. Khi đó $m|xa + yb$, suy ra $m|k$. Vậy k là ước chung lớn nhất của a, b.

Hệ quả 1. Khi a, b nguyên tố cùng nhau thì tồn tại các số nguyên x, y sao cho

$$xa + yb = 1$$

Hệ quả 2. Chứng minh rằng nếu a|bc và (a,b) = 1 thì a|c

Hệ quả 3. Nếu p nguyên tố và $p|a_1a_2 \dots a_n$ thì tồn tại i sao cho $p|a_i$.

2. Bội chung – Bội chung nhỏ nhất

Định nghĩa. Cho hai số nguyên a, b. Số m được gọi là bội chung của a và b nếu a|m và b|m.

Định nghĩa. Số M được gọi là bội chung nhỏ nhất của a và b nếu m nguyên dương, bội chung của a và b và là ước của mọi bội chung khác. Kí hiệu $lcm(a,b)$

Định lý. Nếu $m = lcm(a,b)$ thì $\gcd\left(\frac{m}{a},\frac{m}{b}\right) = 1$

Định lý. Chứng minh rằng $lcm(a,b) = \frac{ab}{\gcd(a,b)}$

Bài tập.

1) Đặt $d = \gcd(m,n)$. Chứng minh rằng $\gcd(a^m - 1, a^n - 1) = a^d - 1$ với mọi số nguyên dương a.
2) Chứng minh rằng nếu các số nguyên dương x, y nguyên tố cùng nhau và xy là một số chính phương thì x, y là số chính phương.
3) Tìm tất cả các bộ số nguyên dương phân biệt (m, p , k) thỏa: $\gcd(m,n)^2 = m + n, \gcd(m,k)^2 = m + k, \gcd(n,k)^2 = n + k$
4) Cho dãy $(a_n): a_1 = a_2 = 1, a_{n+1} = a_n + a_{n-1}, \forall n \geq 2$. Chứng minh rằng $\gcd(a_{n+1}, a_n) = 1, \forall n$
5) Cho dãy các số tự nhiên $a_1, a_2, \ldots$ thỏa $\gcd\left(a_i, a_j\right) = \gcd(i,j)$, $\forall i \neq j$
   Chứng minh rằng $a_i = i, \forall i$
6) Tìm tất cả các bộ ba số (x, y, n) các số nguyên dương thỏa:
   $$\gcd(x, n+1) = 1, x^n + 1 = y^{n+1}$$
7) Tìm tất cả các số nguyên dương n sao cho $2n^2 + n - 1$ là lũy thừa của một số nguyên tố.
8) Tìm tất cả các số nguyên dương n sao cho n ccó thể biểu diễn dưới dạng
   $$n = lcm(a,b) + lcm(b,c) + lcm(a,c)$$
   Trong đó a, b, c là các số nguyên dương.
9) Chứng minh rằng $\frac{\gcd(m,n)}{n}.C_m^n$ là một số nguyên với mọi số nguyên dương $n < m$.
10) Tìm ước chung lớn nhất của tất cả các số $\left\{n^{13} - n \mid n \in \mathbb{Z}\right\}$