Họ và tên: Trần Hoàng Linh **MSSV:** 22127233

BÀI TẬP TUẦN 1

Bài 1: Hãy chứng minh rằng mọi hợp số n đều có ước nguyên tố nhỏ hơn $\sqrt{n}$.

Chứng minh:

Vì n là hợp số nên n có thừa số a $(1 < a < n)$ hay

$$n = ab\ (b > 1) \quad (1)$$

Giả sử: $a > \sqrt{n}$ và $b > \sqrt{n}$ thì $ab > \sqrt{n} * \sqrt{n} = n$ (*mâu thuẫn với* (1))

Do đó: $a < \sqrt{n}$ hoặc $b < \sqrt{n}$

Vì cả a và b đều là ước của n. Nên n có ước nguyên dương không vượt quá $\sqrt{n}$

Theo định lý cơ bản của số học thì ước của này là số nguyên tố hoặc là tích của các số nguyên tố.

Vậy trong cả 2 trường hợp n đều có ước nguyên tố nhỏ hơn $\sqrt{n}$.

Bài 2: Áp dụng thuật toán Euclide, hãy tìm ước chung lớn nhất của các cặp số sau:

a) $a = 252, b = 198$
b) $a = 16261, b = 85652$
c) $a = 139024789, b = 93278890.$

a) $a = 252, b = 198$

$$252 = 198 * 1 + 54$$
$$198 = 54 * 3 + 36$$
$$54 = 36 * 1 + 16$$
$$36 = 18 * 2 + 0$$

Như vậy $(252,198) = 18$

b) $a = 16261, b = 85652$

$$16261 = 85652 * 0 + 16261$$
$$85652 = 16261 * 5 + 4347$$
$$16261 = 4347 * 3 + 3220$$
$$4347 = 3220 * 1 + 1127$$
$$3220 = 1127 * 2 + 966$$
$$966 = 161 * 6 + 0$$

Như vậy $(16261, 85652) = 161$

c) $a = 139024789, b = 93278890.$

$$139024789 = 93278890 * 1 + 45745899$$
$$93278890 = 45745899 * 2 + 1787092$$
$$45745899 = 1787092 * 25 + 1068599$$
$$1787092 = 1068599 * 1 + 718493$$
$$1068599 = 718493 * 1 + 350106$$
$$718493 = 350106 * 2 + 18281$$
$$350106 = 18281 * 19 + 2767$$
$$18281 = 2767 * 6 + 1679$$
$$2767 = 1679 * 1 + 1088$$
$$1679 = 1088 * 1 + 591$$
$$1088 = 591 * 1 + 497$$
$$591 = 497 * 1 + 94$$
$$497 = 94 * 5 + 27$$
$$94 = 27 * 3 + 13$$
$$27 = 13 * 2 + 1$$
$$13 = 1 * 13 + 0$$

Như vậy $(139024789, 93278890) = 1$

Bài 3: Áp dụng thuật toán Eudlide mở rộng, với các cặp (a, b) ở bài tập 2, hãy tìm một cặp số (x, y) thỏa

$$ax + by = d,$$

Trong đó d là ước chung nhỏ nhất của a và b

a) $a = 252, b = 198$

$$(x_0, y_0, d_0) = (1, 0, 252)$$
$$(x_1, y_1, d_1) = (0, 1, 198)$$
$$(x_2, y_2, d_2) = (1, -1, 54)$$
$$(x_3, y_3, d_3) = (-1, 4, 36)$$
$$(x_4, y_4, d_4) = (4, -5, 18)$$

Vậy cặp (x, y) thỏa $252x + 198y = 18$ là $(x, y) = (4, -5)$

b) $a = 16261, b = 85652$

$$(x_0, y_0, d_0) = (1, 0, 16261)$$

$$(x_1, y_1, d_1) = (0, 1, 85652)$$

$$(x_2, y_2, d_2) = (1, -1, 16261)$$

$$(x_3, y_3, d_3) = (-1, 3, 4347)$$

$$(x_4, y_4, d_4) = (3, -4, 3220)$$

$$(x_5, y_5, d_5) = (-4, 15, 1127)$$

$$(x_6, y_6, d_6) = (15, -79, 966)$$

$$(x_7, y_7, d_7) = (-79, 15, 161)$$

Vậy cặp (x, y) thỏa $16261x + 85652y = 161$ là $(x, y) = (-79, 15)$

c) $a = 139024789, b = 93278890.$

$$(x\_0, y\_0, d_0) = (1, 0, 139024789)$$

$$(x_1, y_1, d_1) = (0, 1, 93278890)$$

$$(x_2, y_2, d_2) = (1, -2, 45745899)$$

$$(x\_3, y\_3, d_3) = (-2, 7, 1787092)$$

$$(x_4, y_4, d_4) = (7, -37, 1068599)$$

$$(x_5, y_5, d_5) = (-37, 44, 718493)$$

$$(x_6, y_6, d_6) = (44, -81, 350106)$$

$$(x_7, y_7, d_7) = (-81, 125, 18281)$$

$$(x_8, y_8, d_8) = (125, -206, 2767)$$

$$(x_9, y_9, d_9) = (-206, 1361, 1679)$$

$$(x_{10}, y_{10}, d_{10}) = (1361, -26065, 1088)$$

$$(x_{11}, y_{11}, d_{11}) = (-26065, 53491, 591)$$

$$(x_{12}, y_{12}, d_{12}) = (53491, -79556, 497)$$

$$(x_{13}, y_{13}, d_{13}) = (-79556, 133047, 94)$$

$$(x_{14}, y_{14}, d_{14}) = (133047, -3405731, 27)$$

$$(x_{15}, y_{15}, d_{15}) = (-3405731, 6944509, 13)$$

$$(x_{16}, y_{16}, d_{16}) = (6944509, -10350240, 1)$$

Vậy cặp (x, y) thỏa $139024789x + 93278890y = 1$ là $(x, y) = (6944509, -10350240)$

Bài 4. Từ bài tập số 2, hãy chứng minh rằng giả sử có hai số nguyên $a < b$, khi đó số các phép tính bit cần thiết để thực hiện thuật toán Euclide là $O((\log_2 a)^3)$.

Chứng minh:

Ta có độ phức tạp của thuật toán Euclide là $O(\log_2(\min(a, b))) = O(\log_2 a)$

Với mỗi bước thực hiện phép chia lấy dư $(b \ mod \ a)$ có độ phức tạp của 1 số n-bits là $O(n^2)$ với thuật toán chia cơ bản.

Vì vậy với mỗi bước của thuật toán Euclid cần $O(n^2) = O((\log_2 a)^2)$ do $n = \log_2 a$

Do đó tổng số phép toán bit là $O(\log_2 a).O((\log_2 a)^2) = O((\log_2 a)^3)$

Bài 5. Hãy chứng minh rằng có thể tìm ước chung lớn nhất của hai số nguyên dương bằng thuật toán sau:

$$(a, b) = \begin{cases} a & \text{nếu } a = b \\ 2(a/2, b/2) & \text{nếu } a \text{ và } b \text{ chẵn,} \\ (a/2, b) & \text{nếu } a \text{ chẵn }, b \text{ lẻ,} \\ (a - b, b) & \text{nếu } a \text{ và } b \text{ lẻ.} \end{cases}$$

Chứng minh:

Trường hợp 1: nếu $a = b$

Ta có:

- Tập hợp các ước của a là các số nguyên dương d sao cho $d|a$
- Tập hợp các ước của b cùng là các số nguyên dương d sao cho $d|b$

vì $a = b$ nên tập hợp các ước của a và b giống nhau

Vậy $gcd(a, b) = a$ hoặc $gcd(a, b) = b$

Trường hợp 2: nếu a và b chẵn

Vì a và b chẵn nên a, b có dạng:

$$a = 2k_1 \text{ và } b = 2k_2 \ (k_1, k_2 \in \mathbb{Z})$$

Dễ dàng nhận thấy 2 là ước chung của a và b nên

$$\gcd(a,b) = 2 * \gcd(k_1, k_2) = 2 * \gcd\left(\frac{a}{2}, \frac{b}{2}\right)$$

Trường hợp 3: nếu a chẵn, b lẻ

Ta có :

- a là số chẵn nên có dạng: $a = 2k \ (k \in \mathbb{Z})$
- b là số lẻ nên có dạng: $b = 2k + 1 \ (k \in \mathbb{Z})$

Nhận thấy 2 không là ước của b $(2 \nmid b)$ nên có thể loại bỏ 2 khỏi a:

Do đó:

$$\gcd(a,b) = \gcd\left(\frac{a}{2}, b\right)$$

Trường hợp 4: nếu a, b lẻ

Đặt $c = \gcd(a,b)$ hay $\begin{cases} c|a \\ c|b \end{cases}$

Tồn tại $c_1, c_2 \in \mathbb{Z}$ sao cho $a = c_1c$ và $b = c_2c$

Từ đó suy ra: $a - b = c_1c - c_2c = (c_1 - c_2)c$ hay $c|(a - b)$

Do $\begin{cases} c|b \\ c|(a-b) \end{cases} \Leftrightarrow c = \gcd(a - b, b)$

Vậy $\gcd(a,b) = \gcd(a - b, b)$