NHẬP MÔN MÃ HÓA MẬT MÃ

TUẦN 1: TÍNH CHẤT CHIA HẾT TRÊN VÀNH SỐ NGUYÊN

Ngày 7 tháng 10 năm 2024

Bài 1. Hãy chứng minh rằng mọi hợp số 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) $a = 139024789, b = 93278890$.

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

$$ax + by = d,$$

trong đó d là ước chung lớn nhất của a và b.

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 $O((\log_2 a)^3)$.

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

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

Bài 6. Hãy cài đặt thuật toán Euclide mở rộng bằng $C/C++$, Java hoặc Python. Kiểm tra chương trình với các cặp số (a, b) ở bài tập 2.

Bài 7. (**Cộng điểm khuyến khích**) Hãy sửa đổi chương trình ở **Bài 6** để nó trả về một số $x > 0$ ($ax + by = gcd(a, b)$) và x nhỏ nhất có thể.