BLOCKCHAIN VÀ ỨNG DỤNG

BÀI TẬP SỐ HỌC-THUẬT TOÁN

Ngày 17 tháng 11 năm 2023

1 Hàm Euler, định lý Fermat nhỏ và định lý Euler

1.1 Hàm Euler $\varphi(n)$

Số các số thuộc dãy $1, 2, 3, \ldots, n$ nguyên tố cùng nhau với n được kí hiệu là $\varphi(n)$, người ta gọi $\varphi(n)$ là hàm Euler.

Định lý 1. *Nếu p là một số nguyên tố thì*

$$\varphi(p) = p - 1, \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

với α là số nguyên dương.

Định lý 2. *Nếu một số nguyên dương $n > 1$ có phân tích tiêu chuẩn*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$

thì

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdots \varphi(p_s^{\alpha_s}).$$

1.2 Định lý Euler và định lý Fermat nhỏ

Định lý 3 (Euler). *Cho số tự nhiên $n > 1$ và số nguyên a nguyên tố cùng nhau với n. Khi đó*

$$a^{\varphi(n)} \equiv 1 \ (mod\ n).$$

Định lý 4 (Fermat). *Cho số nguyên tố p và một số nguyên a không chia hết cho p, khi đó*

$$a^{p-1} \equiv 1 \ (mod\ p).$$

Dễ thấy định lý Fermat nhỏ chính là hệ quả của định lý Euler trong trường hợp n là số nguyên tố. Người ta cũng sử dụng định lý Fermat ở dạng như sau:

Định lý 5 (Fermat). *Cho số nguyên tố p và một số nguyên a , khi đó*

$$a^p \equiv a \ (mod\ p).$$

Nhận xét. Từ các kết quả của định lý Euler và định lý Fermat, ta có thêm một cách giải phương trình đồng dư $ax \equiv b \ (mod\ n)$ trong trường hợp $(a, n) = 1$, nghiệm của phương trình này sẽ có dạng $x = a^{\varphi(n)-1} b \ (mod\ n)$.

2 Bài tập số học-thuật toán

Bài 1. Sử dụng thuật toán Euclide, hãy trình bày chi tiết các bước và đưa ra ước chung lớn nhất của các cặp số sau:

a) $a = 414, b = 662$;

b) $a = 252, b = 198$.

Bài 2. Cho trước hai số nguyên a, b, sử dụng thuật toán Euclide mở rộng, hãy trình bày các bước để tìm ra một cặp số (x_0, y_0) thỏa $ax_0 + by_0 = gcd(a, b)$.

a) $a = 63, b = 24$;

b) $a = 252, b = 54$.

Bài 3. Giải các phương trình đồng dư dạng $ax \equiv b \ (mod\ n)$ bằng cách duyệt trên một hệ thặng dư đầy đủ $\{0, 1, 2, \ldots, n-1\}$ để chỉ ra nghiệm:

a) $3x \equiv 7(mod\ 5)$,

b) $7x \equiv 0(mod\ 10)$,

c) $37x \equiv 20(mod\ 7)$,

d) $17x \equiv 5(mod\ 47)$,

e) $8x \equiv 20(mod\ 21)$

f) $7x \equiv 5(mod\ 20)$

Bài 4. Giải các phương trình Deophantine sau:

a) $252x + 198y = 54$

b) $13x - 21y = 12$

c) $3x + 31y = 15$

Gợi ý: Sử dụng thuật toán Euclide mở rộng.

Bài 5. Hãy sử dụng định lý Euler hoặc Fermat nhỏ để giải các phương trình ở **Bài** 3.

Deadline: **Các anh chị vui lòng scan file viết tay thành pdf và nộp bài trước 24h ngày 24-11-2023 theo đường link**

$$https://forms.gle/BmJ5Ce2PDGXJiTRA8$$