Chương III: Cơ sở toán học

Một số thuật toán

1. Thuật toán Euclid mở rộng

1.1 Tính chia hết của một số

- Vấn đề quan tâm: a có chia hết cho b hay không

=> a = b.q + r, 0 < r < b

- Bài toán: Tìm UCLN của hai số a và b

Định lý 3.1.1:

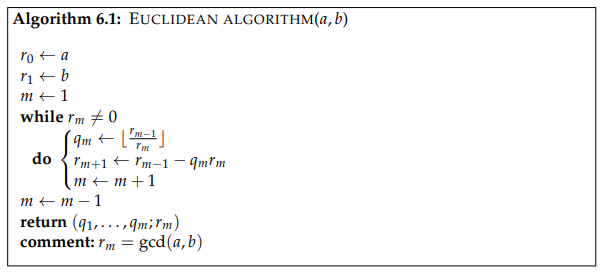
- Nếu b > 0 và b là ước của a thì gcd(a, b) = b

- Nếu a = b.q + r thì gcd(a,b) = gcd(b,r)

=> Quan hệ về BCNN và UCLN của hai số:

lcm(a,b) \* gcd(a,b) = a.b

Thuật toán Eclid tìm ước số chung lớn nhất của a và b

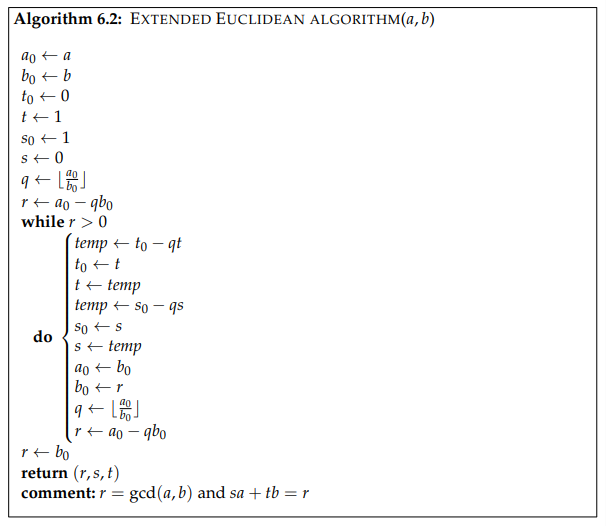


- Trong khi còn b > 0

Thuật toán Euclide mở rộng:

- Input: Hai số nguyên không âm a và b với a >= b

- Output: d = gcd(a,b) và hai số x,y sao cho a.x + b.y = d



=> BTVN: Tìm nghịch đảo theo modulo số có độ dài 32 bit

1.2 Đồng dư và phương trình đồng dư tuyến tính

Cho n là một số nguyên dương. Ta nói hai số nguyên a và b là đồng dư với nhau theo modun n, và viết:

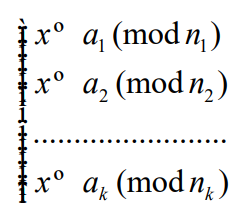
a b (mod n)

Phương trình đồng dư tuyến tính có dạng

a.x b (mod n)

trong đó a,b,n là các số nguyên, n > 0, x là ẩn số

Xét hệ các phương trình đồng dư tuyến tính, có dạng



Đính lý số dư Trung Quốc:

Giả sử các số nguyên n1, n2,....,nk là từng cặp nguyên tố với nhau. Khi đó, hệ phương trình đồng dư tuyến tính (2) có một nghiệm duy nhất theo modn :

Trong đó *Mi = Ni-1 mod ni* (Có *Mi* và *Ni* và *ni* nguyên tố với nhau)

1.3 Thặng dư thu gọn và phần tử nguyên thuỷ

Tập Zn = { 0,1,2,..., n −1} thường được gọi là tập các thặng dư đầy đủ theo modn, vì mọi số nguyên bất kỳ đều có thể tìm được trong Zn một số đồng dư với mình (theo modn ).

Tập Zn là đóng đối với các phép tính cộng, trừ và nhân theo modn , nhưng không đóng đối với phép chia, vì phép chia cho a theo modn chỉ có thể thực hiện được khi a và n 27 nguyên tố với nhau, tức khi gcd( a ,n ) =1.

Bây giờ ta xét tập Zn \* = { a ∈ Zn : gcd( a ,n ) = 1} , tức Zn \* là tập con của Zn bao gồm tất cả các phần tử nguyên tố với n. Ta gọi tập đó là tập các thặng dư thu gọn theo modn. Mọi số nguyên nguyên tố với n đều có thể tìm thấy trong Zn \* một đại diện đồng dư với mình theo modn .

Chú ý rằng nếu p là một số nguyên tố thì Zp \* = {1,2,...,p-1}. Tập Zn \* lập thành một nhóm con đối với phép nhân của Zn , vì 28 trong Zn \* phép chia theo modn bao giờ cũng thực hiện được, ta sẽ gọi Zn \* là nhóm nhân của Zn .

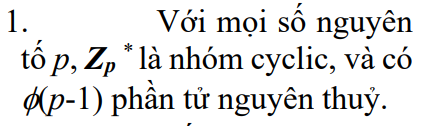
Theo đại số học, ta gọi số các phần tử trong một nhóm là cấp của nhóm đó. Ta ký hiệu φ(n) là số các số nguyên dương bé hơn n và nguyên tố cùng nhau với n. Như vậy, nhóm Zn \* có cấp φ(n) , và nếu p là số nguyên tố thì nhóm Zp \* có cấp p -1.

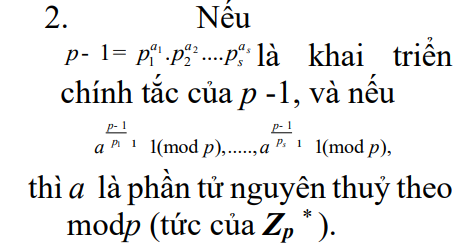
Ta nói một phần tử g ∈Zn \* có cấp m , nếu m là số nguyên dương bé nhất sao cho g m =1 29 trong Zn \* . Theo một định lý trong Đại số, ta có m ⏐ φ(n) . Vì vậy, với mọi b ∈Zn \* ta luôn có b φ(n ) ≡ 1 modn .

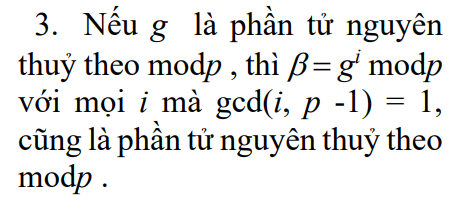
Nếu p là số nguyên tố, thì do φ(p) = p − 1, ta có với mọi b ∈Zp \* : 1 1 (mod ) p b p - º (3)

Nếu b có cấp p - 1, tức p - 1 là số mũ bé nhất thoả mãn công thức (3), thì các phần tử b, b 2 ,...., b P-1 đều khác nhau và theo modp, chúng lập thành Zp \* . Theo thuật ngữ đại số, khi đó ta nói Zp \* là một nhóm cyclic và b 30 là một phần tử sinh, hay phần tử nguyên thuỷ của nhóm đó.

Tính chất của các phần tử nguyên thuỷ:

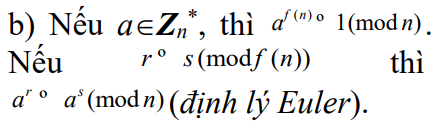






Ba tính chất đó là cơ sở giúp ta tìm các phần tử nguyên thuỷ theo modp , với p là số nguyên tố bất kỳ. Ngoài ra, ta cũng chú ý một số tính chất sau đây, có thể được sử dụng nhiều trong các chương sau:

a. Nếu p là số nguyên tố và gcd(a,p) = 1 thì ap-1 1 (modp) (định lý Fermat)



o =

1.4 Phương trình đồng dư bậc hai và thặng dư bậc hai