1`. Kiểm tra n là số nguyên tố hay hợp số.

Cách 1: kiểm tra tất cả các số x<n . Không tìm thấy số nào mà n chia hết thì nó là số nguyên tố

Cách 2: Kiểm tra các số nguyên tố x<n. Không tìm thấy số nào mà n chia hết thì nó là số nguyên tố.

Định lý : Nếu n là hợp số thì n có một số chia là số nguyên tố nhỏ hơn hoặc bằng sqrt(n).

CM: ta có a\*b=n. Giả sử a > sqrt(n) và b >sqrt( n). Thì ab > sqrt(n\* n) = n, trái với giả thiết. Vì vậy, hoặc là a ≤sqrt( n) hoặc b ≤ sqrt(n).

Cách 3 : Tìm có tồn tại số chia x mà x<sqrt(n). Nếu không có thì n là số nguyên tố.

Định lý : có vô số số nguyên tố

CM: Giả sử có hữu hạn số nguyên tố : a,b,...n. Khi đó ta có số Q=a\*b\*..\*n +1. Số Q này không chia hết cho bất kì số nào trong a,b,...n nên Q là số nguyên tố .

2. Tìm lcm ( least common multiple ), gcd (greatest common divisor)

Cách 1: dùng phương pháp phân tích ra các thừa số nguyên tố rồi khử.

Cách 2 : Euclid

gcd (503, 286) 503 = 1 × 286 + 217

= gcd (286, 217) 286 = 1 × 217 + 69

= gcd (217, 69) 217 = 3 × 69 + 10

= gcd (69, 10) 69 = 6 × 10 + 9

= gcd (10, 9) 10 = 1 × 9 + 1

= gcd (9, 1) = 1

3. Phương trình đồng dư và ứng dụng.

a đồng dư với b mô-đu-lô m nếu a − b chia hết cho m. Ta dùng a = b ( mod m) để kí hiệu sự đồng dư. Nếu a và b không đồng dư ta viết a ≠ b (mod m) .

❑Định lý: Nếu a và b là các số nguyên và m là một

số nguyên dương, thì a = b mod m khi và chỉ

khi a mod m = b mod m.

4. Đồng dư.

❑Định lý 1: Đặt m là một số nguyên dương. Các số

nguyên a và b đồng dư mô-đu-lô m khi và chỉ khi

tồn tại một số nguyên k sao cho a = b + mk.

❑Định lý 2: Đặt m là một số nguyên dương. Nếu

a = b (mod m) và c = d (mod m) thì:

a + c = b + d( mod m) và ac = bd (mod m) .

ĐỌC LẠI TRANG 301

Tuần 5 : mã hoá RSA

Ví dụ 