MỘT SỐ KẾT QUẢ TRÊN Z_p CỦA HỆ MÃ KHÓA CÔNG KHAI

Nguyễn Thanh Sơn
Trường Đại học Kỹ thuật
(Bài nhận ngày 14/05/1999)

TÓM TẮT : Bài báo này trình bày một số kết quả của lý thuyết số liên quan tới việc tìm phần tử sinh của nhóm Z_n^* và khảo sát tính chất các phần tử sinh này. Kết quả này ảnh hưởng trên hệ mật mã công khai ElGamal crystosystem trong việc tìm phần tử sinh.

I. MỘT SỐ KHÁI NIỆM VÀ KẾT QUẢ CỦA LÝ THUYẾT SỐ CÓ LIÊN QUAN

Định nghĩa :

Bậc của phần tử a trong nhóm nhân G là một số nguyên nhỏ nhất n sao cho $a^n = 1$.

Bậc của một nhóm nhân G là một số nguyên lớn nhất trong các bậc của mọi phần tử của G.

Ký hiệu nhóm G sinh bởi phần tử a : $G = < a >$.

Hệ quả :

Bậc của một nhóm chính là số phần tử của nhóm, do đó bậc của phần tử a chính là số phần tử của nhóm con sinh bởi a.

Định lý 1 : (Lagrange)

Nếu G là nhóm nhân bậc n thì mọi phần tử của G có bậc chia đúng cho n.

Hệ luận :

Z_n^* là nhóm nhân có bậc $\varphi(n)$, ie $x^{\varphi(n)} = 1 \bmod n$ với mọi x của Z_n^*.

Hệ luận : (Fermat)

Cho p nguyên tố, $x^p = x \bmod p$ với mọi x của Z_p^*.

Định lý2 :

Nếu p là nguyên tố thì Z_p^* là nhóm tuần hoàn, ie có phần tử sinh.

Các phần tử có bậc $p - 1$ là phần tử sinh.

Định lý3 :

Nếu α là phần tử sinh và $\gcd(i, p - 1) = 1$ thì α^i cũng là phần tử sinh.

Số phần tử sinh của Z_p với p nguyên tố là $\varphi(p - 1)$.

Nhận xét 1 :

Trong một nhóm nhân giao hoán, lấy hai phần tử x và y có bậc m và n tương ứng. Nếu m, n nguyên tố cùng nhau thì bậc của xy là mn.

Đinh lý 4 : (Euler's Criterion)

x là số chính phương iff $x^{(p-1)/2} = 1 \bmod p$, với p nguyên tố.

II. MỘT SỐ KẾT QUẢ TÁC GIẢ ĐẠT ĐƯỢC

Các Mệnh đề được khảo sát trong Z_p^* với p nguyên tố.

Mệnh đề 1.

$(p-1)^2 = 1$ nên $p-1$ không là phần tử sinh với $p > 3$.

Do đó $(p-1)$ có bậc 2.

Chứng minh :

$(p-1)^2 = p^2 - 2p + 1 = 1$.

Mệnh đề 2.

Phần tử $p-1$ có nghịch đảo là chính nó.

Chứng minh :

Do Mệnh đề 1.

Mệnh đề 3.

α là phần tử sinh iff $\alpha^{(p-1)/2} = p-1$ và $(\alpha^i \neq 1, \forall i \leq (p-1)/2)$.

Chứng minh :

$(\rightarrow)$ Vì α là phần tử sinh nên $\alpha^{(p-1)} = 1$.

Căn bậc 2 của $\alpha^{(p-1)}$ là 1 và $(p-1)$.

Nếu $\alpha^{(p-1)/2} = 1$ thì α không phải là phần tử sinh.

Vậy $\alpha^{(p-1)/2} = (p-1)$.

$(\leftarrow)$ Vì $(p-1)$ bậc 2 nên $\alpha^{(p-1)} = 1$.

Do đó bậc của α là một ước số của $(p-1)$.

Các giá trị $(p-1)/2 < i < (p-1)$ không thể là ước số của $(p-1)$.

Vậy α là phần tử sinh.

Mệnh đề 4.

Phần tử không sinh β có bậc $\leq (p-1)/2$.

Chứng minh :

Giả sử có phần tử không sinh β có bậc m với $m > (p-1)/2$.

Do định lý Lagrange $(p-1) = mk$ hay $(p-1)/k = m$.

$(p-1)/k > (p-1)/2$ mâu thuẫn.

Nhân xét 2 :

Để kiểm tra một phần tử β là không sinh ta tính β^k với k là ước số của $(p-1)$ và kiểm tra $\beta^k = 1$ hay không.

Được chứng minh từ định lý Lagrange và Mệnh đề 3.

Mênh đề 5.

Nghịch đảo của phần tử sinh cũng là phần tử sinh.

Chứng minh :

Lấy α là một phần tử sinh và β là nghịch đảo củaα, ie $\alpha.\beta = 1 \bmod p$.

Vì α là phần tử sinh nên có số nguyên $k < p - 1$ sao cho $\alpha^k = \beta$.

Giả sử β không là phần tử sinh thì có một số nguyên $n < p-1$ sao cho $\beta^n = 1$. Vì α là phần tử sinh nên $\alpha^n \neq 1$.

Tính $(\alpha.\beta)^n = \alpha^n.\beta^n = \alpha^n.1 = \alpha^n = 1$.

Mâu thuẫn với $\alpha^n \neq 1$.

Mênh đề 6.

Phần tử x và nghịch đảo của nó có cùng bậc.

Chứng minh :

Gọi bậc x là n và bậc của x^{-1} là m.

Nếu $n > m$, $(x.x^{-1})^m = (x^m)(x^{-1})^m = x^m = 1$, mâu thuẫn.

Nếu $n < m$, $(x.x^{-1})^n = (x^n)(x^{-1})^n = (x^{-1})^n = 1$, mâu thuẫn.

Mênh đề 7.

Nếu $(p-1)/2$ lẻ thì số phần tử sinh bằng số phần tử có bậc $(p-1)/2$.

Nếu α có bậc $(p-1)/2$ thì $\alpha(p-1)$ là phần tử sinh.

Chứng minh :

Lấy α là phần tử có bậc 2 và β có bậc $(p-1)/2$.

Vì $(p-1)/2$ là số lẻ nên $\gcd((p-1)/2, 2) = 1$.

Bội số chung nhỏ nhất của $(p-1)/2$ và 2 là $(p-1)$.

Do đó bậc của $\alpha.\beta$ là $(p-1)$.

Nên $\alpha.\beta$ là phần tử sinh.

Mênh đề 8.

Nếu x là số chính phương thì $x = \alpha^n$, với α là phần tử sinh và n là số chẵn. Do đó nếu số mũ n lẻ thì x không chính phương. Phần tử sinh không là số chính phương.

Số phần tử chính phương = số phần tử không chính phương = $(p-1)/2$.

Chứng minh :

Vì $(p-1)$ chẵn và nếu $\gcd(p-1, i) = 1$ nên i phải là số lẻ với mọi i.

Lấy α, β là hai phần tử sinh, ta có $\beta = \alpha^k$ thì k là số lẻ.

Nếu phần tử $x = \alpha^n$, với n lẻ thì với mọi phần tử sinh β khác $x = \beta^m$ thì m là số lẻ.

Do đó số x có dạng α^n, với n lẻ thì x không là số chính phương.

Vậy số phần tử không chính phương là $(p-1)/2$. Do đó số phần tử chính phương là $(p-1)/2$.

Mệnh đề 9.

Gọi $\alpha_1 < ... < \alpha_k$ là tất cả phần tử sinh của Z_p^* được xắp theo thứ tự tăng dần.

1. Nếu $(p-1)/2$ là số chẵn thì

a. $\alpha_1.(p-1) = \alpha_k$,

$\alpha_2.(p-1) = \alpha_{k-1}$,

...

$\alpha_{k-1}.(p-1) = \alpha_2$,

$\alpha_k.(p-1) = \alpha_1$.

b. $\alpha_1 + \alpha_k = \alpha_2 + \alpha_{k-1} = \alpha_3 + \alpha_{k-2} = ... = \alpha_{k/2} + \alpha_{k/2+1} = p$.

c. $(p-1).<\alpha_i> = <(p-1).\alpha_i>$.

d. Số phần tử sinh là số chẵn.

2. Nếu $(p-1)/2$ là số lẻ thì

a. $\alpha_i.(p-1)$ là phần tử có bậc $(p-1)/2$.

b. Số phần tử sinh bằng số phần tử có bậc $(p-1)/2$.

c. $(p-1).<\alpha_i> \neq <(p-1).\alpha_i>$.

d. $\alpha_1 + \alpha_k \neq p$.

Chứng minh :

1. $(\alpha_i.(p-1))^{(p-1)/2} = (\alpha_i^{(p-1)/2}.(p-1)^{(p-1)/2}$,

$= (p-1).(p-1)^{(p-1)/2}$ (do Mệnh đề 3),

$= (p-1)((p-1)^2)^n$ (vì $(p-1)/2 = 2n$),

$= (p-1)((p-1)^2)^n$ (vì $(p-1)$ bậc 2),

$= (p-1)$.

Vậy $\alpha_i.(p-1)$ là phần tử sinh.

Ta có $\alpha_i.(p-1) \neq \alpha_i$ (1)

Đặt $\alpha_n = \alpha_1.(p-1)$, $\alpha_{n-1} = \alpha_2.(p-1)$, ...

$\alpha_i.(p-1) = p\alpha_i - \alpha_i = -\alpha_i = p - \alpha_i$, (2)

$\alpha_n = p - \alpha_1$. (do 2) (3)

$\alpha_{n-1} = p - \alpha_2$. (do 2) (4)

$\alpha_{n-1} < \alpha_1$, (do 3, 4 và $\alpha_1 < \alpha_2$)

Do đó $\alpha_{n-i} < \alpha_i$, với mọi i.

$\alpha_{n-i} + \alpha_i = p$.

Vì p lẻ nên α_{n-i} và α_i không cùng chẵn hoặc cùng lẻ.

Do đó không có cặp α_{n-i} và α_i nào trùng với nhau.

$(p-1).<\alpha_i> = <(p-1).\alpha_i> = Z_p^*$.

Nên số phần tử sinh là số chẵn.

2. $(\alpha_i.(p-1))^{(p-1)/2} = (\alpha_i^{(p-1)/2}.(p-1)^{(p-1)/2}$,

$= (p-1).(p-1)^{(p-1)/2}$,

$= (p-1).(p-1).(p-1)^{2n}$ (vì $(p-1)/2 = 2n+1$),

$= ((p-1)^2)^{n+1}$,

$= (1)^{n+1}$ (vì $(p-1)$ bậc 2),

$= 1$.

Vậy $\alpha_i.(p-1)$ không là phần tử sinh, và dễ dàng chứng minh bậc là $(p-1)/2$.

Trong Z_{11}^* lấy $(p-1).<\alpha> = 10<2> = Z_{11}^* \neq$

$<(p-1).\alpha> = <10x2> = <9> = \{9, 4, 3, 5, 1\}$.

Ta có $2+8 \neq 11$.

II. THUẬT TOÁN

A. Tìm phần tử sinh đầu tiên với trường hợp (p –1)/2 là số chẵn

1. Vì các phần tử sinh đối xứng qua điểm (p–1)/2 nên thuật toán có thể thực hiện song song 2 quá trình :

a. Quá trình 1 kiểm tra x có phải là phần tử sinh với x từ 1 tới (p–1)/4.

b. Quá trình 2 kiểm tra x có phải là phần tử sinh với x từ (p–1)/2 giảm tới (p–1)/4.

Khi một trong hai quá trình tìm thấy kết quả thì dừng quá trình còn lại.

Nếu thuật toán thực hiện tuần tự thì kiểm tra x từ 1 tới (p–1)/4.

2 . Kiểm tra x có phải là phần tử sinh.

Do Mệnh đề 3 chỉ cần lấy lũy thừa (p – 1)/2 của x.

Khi tiến hành lũy thừa nếu kết quả bằng 1 trước khi giá trị lũy thừa đạt số mũ (p – 1)/2 thì dừng và kết luận x không phải là phần tử sinh do Mệnh đề 4.

```
i := 1;
repeat
  x := x^2 mod p;
  i := i+1;
until ( i = (p – 1)/4 ) or (x = 1).
if x <>1 then x := x.y mod p.
```

c. Nếu x = p–1 thì x là phần tử sinh, ngược lại là không. Giữ lại nội dung của i để biết bậc của x.

Ưu điểm của thuật toán :

- số phép tính lũy thừa chỉ là ≈ p/4 lần.

- giá trị luôn nhỏ hơn p (do lấy mod mỗi bước).

B. **Tìm tất cả phần tử sinh khi đã biết 1 phần tử sinh.**

a. Lấy nghịch đảo của phần tử sinh có được phần tử sinh.

b. Nếu a là phần tử sinh thì p–a cũng là phần tử sinh nếu (p – 1)/2 chẵn.

c. Lũy thừa i phần tử sinh cũng là phần tử sinh với gcd(i, p–1)=1.

SOME RESULTS ON Z_P OF PUBLIC-KEY CRYSTOSYSTEM

Nguyễn Thanh Sơn

ABSTRACT : This article discribed some results on Theory number. It related to primitive elements of Z_n^* and their relations. The results affected on the finding of primitive element of ElGamal crystosystem.

TÀI LIỆU THAM KHẢO

[1] Steven S. Skiena, The algorithm design manual, Springer-Verlag 1998.

[2] Kenneth H. Rosen, Elementary number theory and its applications, Addision-Wesley publishing company1993.

[3] Douglas R. Stinson, Crystography Theory and Practice, AT&T Bell Laboratories, 1995 by CRC Press, Inc.

[4] Ivan Niven, H.S. Zuckerman. An introduction to the theory of numbers. 1960. John Wiley & Sons, Inc.

[5] Kenneth H. Rosen. Elementary number theory and its applications. 1993. AT&T Bell Laboratories and Kenneth H. Rosen.

[6] R.L. Graham, D.E. Knuth, O. Patashnik. Concrete mathematics a foundation for computer science. 1989. Addition-Wesley Publishing Company.

[7] Acm computing surveys. Volume 11. 1979.

[8] D.W. Davies. Tuturial : The security of data in networks. IEEE computer society.

[9] William Starlings. Network and security principles and practice. 1995. Printice Hall.

[10] Charlie Kaufman, Radia Pereman, Mike Speciner. Network security private communication in a public world. 1995. Printice Hall.

[11] Albrecht Beutelspacher. Cryptology. 1994. The mathematical Association of America.