Chương III. Cơ sở toán học của ATTT

Bài 3.1. Thuật toán Euclid

1. Số học các số nguyên. Thuật toán Euclide.

Ta ký hiệu Z là tập hợp các số nguyên, $\boldsymbol{Z}$ = {.....,-2,-1,0,1,2,....},

và Z^+ là tập hợp các số nguyên không âm, $\boldsymbol{Z}^+$= {0,1,2,.....}. Trong mục này ta sẽ nhắc lại một số kiến thức về số học của các số nguyên cần cho việc trình bày lý thuyết mật mã. Vì để tập giáo trình không quá dài dòng, các kiến thức sẽ được nhắc đến chủ yếu là các khái niệm, các mệnh đề sẽ được sử dụng, v.v..., còn các phần chứng minh sẽ được lược bỏ, bạn đọc nào muốn tìm hiểu kỹ hơn có thể tham khảo các sách chuyên về Số học.

2.1.1. Tính chia hết của các số nguyên.

Tập hợp $\boldsymbol{Z}$ là đóng kín đối với các phép cộng, trừ và nhân, nhưng không đóng kín đối với phép chia: chia một số nguyên cho một số nguyên không phải bao giờ cũng được kết quả là một số nguyên! Vì vậy, trường hợp chia hết, tức khi chia số nguyên a cho số nguyên b được thương là một số nguyên q , $a = b.q$, có một ý nghĩa đặc biệt. Khi đó, ta nói *a chia hết cho b, b chia hết a, a* là *bội số* của *b, b* là *ước số* của *a*, và ký hiệu là $b \mid a$. Dễ thấy ngay rằng số 1 là ước số của mọi số nguyên bất kỳ, số 0 là bội số của mọi số nguyên bất kỳ, mọi số nguyên a là ước số, đồng thời là bội số, của chính nó.

Cho hai số nguyên bất kỳ a và b , $b > 1$. Thực hiện phép chia a cho b ta sẽ được hai số q và r sao cho

$$a = b.q + r\ ,\ 0 \le r < b\ .$$

Số q được gọi là *số thương* của phép chia a cho b, ký hiệu a div$b$, và số r được gọi là *số dư* của phép chia a cho b, ký hiệu a mod$b$. Thí dụ: 25 div 7 = 3 và 25 mod 7 = 4, -25 div 7 = -4 và -25 mod 7 = 3.

Một số nguyên d được gọi là *ước số chung* của hai số nguyên a và b nếu $d \mid a$ và $d \mid b$. Số nguyên d được gọi là *ước số chung lớn nhất* của a và b nếu $d > 0$, d là ước số chung của a và b, và mọi ước số chung của a và b đều là ước số của d . Ta ký hiệu ước số chung lớn nhất của a và b là gcd(a,b). Thí dụ gcd(12,18) = 6, gcd(-18, 27) = 3.

Dễ thấy rằng với mọi số nguyên dương a ta có gcd(a,0) = a , ta cũng sẽ qui ước xem rằng gcd(0, 0) = 0.

Một số nguyên $a > 1$ được gọi là *số nguyên tố*, nếu a không có ước số nào ngoài 1 và chính a ; và được gọi là *hợp số* , nếu không phải là nguyên tố. Thí dụ các số 2 ,3 , 5, 7 là số nguyên tố; các số 4, 6, 8, 10, 12, 14, 15 là hợp số. Hai số a và b được gọi là *nguyên tố với nhau*, nếu chúng không có ước số chung nào khác 1, tức là nếu gcd(a,b) = 1. Một số nguyên $n > 1$ bất kỳ đều có thể viết dưới dạng:

$$n = p_1^{\alpha_1}.p_2^{\alpha_2}\dots p_k^{\alpha_k}$$

trong đó p_1 , p_2 ,..., p_k là các số nguyên tố khác nhau, α_1 , α_2 ,..., α_k là các số mũ nguyên dương. Nếu không kể thứ tự các thừa số nguyên tố, thì dạng biểu diễn đó là duy nhất, ta gọi đó là *dạng khai triển chính tắc* của n . Thí dụ dạng khai triển chính tắc của 1800 là $2^3 3^2 5^2$.

Các số nguyên tố và các vấn đề về số nguyên tố có một vai trò quan trọng trong số học và trong ứng dụng vào lý thuyết mật mã, ta sẽ xét riêng trong một mục sau.

Định lý 3.1.1. *Nếu* $b > 0$ *và* $b \mid a$ *thì* $\gcd(a,b) = b$.

Nếu $a = bq + r$ *thì* $\gcd(a,b) = \gcd(b,r)$.

Một số nguyên m được gọi là *bội số chung* của a và b nếu $a \mid m$ và $b \mid m$. Số m được gọi là *bội số chung bé nhất* của a và b , và được ký hiệu là $\text{lcm}(a,b)$, nếu $m > 0$, m là bội số chung của a và b , và mọi bội số chung của a và b đều là bội của m . Thí dụ $\text{lcm}(14,21) = 42$.

Với hai số nguyên dương a và b bất kỳ ta có quan hệ

$$\text{lcm}(a,b).\gcd(a,b) = a.b.$$

Từ định lý 2.1.1 ta suy ra thuật toán sau đây thực hiện việc tìm ước số chung lớn nhất của hai số nguyên bất kỳ:

Thuật toán Euclide tìm ước số chung lớn nhất **:**

INPUT: hai số nguyên không âm a và b , với $a \geq b$.

OUTPUT: ước số chung lớn nhất của a và b.

1. Trong khi còn $b > 0$, thực hiện:

1.1. đặt $r \leftarrow a \bmod b$, $a \leftarrow b$, $b \leftarrow r$.

2. Cho ra kết quả (a).

Thí dụ: Dùng thuật toán Euclide tìm gcd(4864, 3458), ta lần lượt được các giá trị gán cho các biến a, b và r như sau:

$4864 = 1.\ 3458 + 1406$
$3458 = 2.\ 1406 + 646$
$1406 = 2.\ 646 + 114$
$646 = 5.\ 114 + 76$
$114 = 1.\ 76 + 38$
$76 = 2.\ 38 + 0$

a	b	r
4864	3458	
3458	1406	1406
1406	646	646
646	114	114
114	76	76
76	38	38
38	0	0

Và thuật toán cho ta kết quả: gcd(4864, 3458) = 38.

Ta biết rằng nếu $\gcd(a,b) = d$, thì phương trình bất định

$$a.x + b.y = d$$

có nghiệm nguyên (x,y), và một nghiệm nguyên (x,y) như vậy có thể tìm được bởi thuật toán Euclide mở rộng như sau:

Thuật toán Euclide mở rộng :

INPUT: hai số nguyên không âm a và b với $a \geq b$.

OUTPUT: $d = \gcd(a,b)$ và hai số x,y sao cho $a.x + b.y = d$.

1. Nếu $b = 0$ thì đặt $d \leftarrow a$, $x \leftarrow 1$, $y \leftarrow 0$, và cho ra (d,x,y).
2. Đặt $x_2 = 1$, $x_1 = 0$, $y_2 = 0$, $y_1 = 1$.
3. Trong khi còn $b > 0$, thực hiện:

   3.1. $q \leftarrow a \text{ div} b$, $r \leftarrow a \bmod b$, $x \leftarrow x_2 - qx_1$, $y \leftarrow y_2 - qy_1$.

   $a \leftarrow b$, $b \leftarrow r$, $x_2 \leftarrow x_1$, $x_1 \leftarrow x$, $y_2 \leftarrow y_1$ và $y_1 \leftarrow y$.
4. Đặt $d \leftarrow a$, $x \leftarrow x_2$, $y \leftarrow y_2$, và cho ra kết quả (d,x,y).

Thí dụ: Dùng thuật toán Euclide mở rộng cho các số $a = 4864$ và $b = 3458$, ta lần lượt được các giá trị sau đây cho các biến $a, b, q, r, x, y, x_1 , x_2 , y_1 , y_2$ (sau mỗi chu trình thực hiện hai lệnh 3.1 và 3.2) :

a	***b***	*Q*	***r***	***x***	***y***	x_1	x_2	y_1	y_2
4864	3458					0	1	1	0
3458	1406	1	1406	1	-1	1	0	-1	1
1406	646	2	646	-2	3	-2	1	3	-1
646	114	2	114	5	-7	5	-2	-7	3
114	76	5	76	-27	38	-27	5	38	-7
76	38	1	38	32	-45	32	-27	-45	38
38	0	2	0	-91	128	-91	32	128	-45

Ví dụ

a = 101, b= 16

Ta dễ thử lại rằng sau mỗi lần thực hiện chu trình gồm hai lệnh 3.1 và 3.2, các giá trị x,y,r thu được luôn thoả mãn $4864.x + 3458.y = r$, và do đó khi kết thúc các vòng lặp (ứng với giá trị $b = 0$), thực hiện tiếp lệnh 4 ta được kết quả $d = 38$, $x = 32$ và $y = -45$, cặp số (32,-45) thoả mãn: $4864.32 + 3458.(-45) = 38$.

2.1.2. 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 môđuyn n* , và viết $a \equiv b \pmod n$, nếu $n \mid a-b$ (tức cũng là nếu $a - b$ chia hết cho n , hay khi chia a và b cho n ta được cùng một số dư như nhau).

Thí dụ: $23 \equiv 8 \pmod 5$), vì $23 - 8 = 5.3$, $-19 \equiv 9 \pmod 7$ vì $-19 - 9 = -4 . 7$.

Quan hệ đồng dư (theo một môđuyn n) trên tập hợp các số nguyên có các tính chất phản xạ, đối xứng và bắc cầu, tức là một quan hệ tương đương, do đó nó tạo ra một phân hoạch trên tập hợp tất cả các số nguyên $\boldsymbol{Z}$ thành ra các lớp tương đương: hai số nguyên thuộc cùng một lớp tương đương khi và chỉ khi chúng cho cùng một số dư nếu chia cho n. Mỗi lớp tương đương như vậy được đại diện bởi một số duy nhất trong tập hợp $\boldsymbol{Z}_n = \{0, 1, 2, 3,...., n -1\}$, là số dư chung khi chia các số trong lớp đó cho n. Vì vậy, ta có thể đồng nhất $\boldsymbol{Z}_n$ với tập hợp tất cả các lớp tương đương các số nguyên theo mod$n$; trên tập đó ta có thể xác định các phép tính cộng, trừ và nhân theo mod$n$.

Thí dụ: $\boldsymbol{Z}_{25} = \{0, 1, 2, ..., 24\}$. Trong $\boldsymbol{Z}_{25}$, $15 + 14 = 4$, vì $15 + 14 = 29 = 4 \pmod{25}$. Tương tự, $15.14 = 10$ trong $\boldsymbol{Z}_{25}$.

Cho $a \in \boldsymbol{Z}_n$. Một số nguyên $x \in \boldsymbol{Z}_n$ được gọi là *nghịch đảo* của a theo mod n , nếu $a.x \equiv 1 \pmod n$. Nếu có số x như vậy thì ta nói a là khả nghịch, và ký hiệu x là $a^{-1} \bmod n$. Thí dụ $22^{-1} \bmod 25 = 8$, vì $22 .8 = 176 \equiv 1 \pmod{25}$. Từ định nghĩa ta có thể suy ra rằng a là khả nghịch theo mod$n$ khi và chỉ khi $\gcd(a,n) = 1$, tức là khi a và n nguyên tố với nhau.

Ta định nghĩa phép chia trong $\boldsymbol{Z}_n$ như sau: $a : b \pmod n = a.b^{-1} \bmod n$. Phép chia chỉ thực hiện được khi b là khả nghịch theo mod$n$. Thí dụ $15 : 22 \pmod{25} = 15.22^{-1} \bmod 25 = 20$.

Bây giờ ta xét các *phương trình đồng dư tuyến tính.*

Phương trình đồng dư tuyến tính có dạng

$$a.x \equiv b \pmod n, \qquad (1)$$

trong đó a, b, n là các số nguyên, $n > 0$, x là ẩn số. Phương trình đó có nghiệm khi và chỉ khi $d = \gcd(a,n) \mid b$, và khi đó nó có đúng d nghiệm theo mod$n$. Thực vậy, đặt $a' = a/d$, $b' = b/d$, $n' = n/d$, ta thấy phương trình đồng dư (1) tương đương với phương trình

$$a'.x \equiv b' \pmod{n'},$$

Vì $\gcd(a',n') = 1$, nên phương trình này có một nghiệm theo modn'

$$x = x_0 \equiv b'.a'^{-1} \pmod{n'},$$

và do đó phương trình (1) có d nghiệm theo mod$n$ là :

$$x = x_0 , x_0 + n', ... , x_0 + (d - 1)n' \pmod n.$$

Tất cả d nghiệm đó khác nhau theo mod$n$, nhưng cùng đồng dư với nhau theo modn'.

Bây giờ ta xét hệ thống các phương trình đồng dư tuyến tính. Một hệ như vậy có thể đưa về dạng

$$\begin{cases} x \equiv a_1 \bmod n_1 \\ x \equiv a_2 \bmod n_2 \\ \quad \ldots \\ x \equiv a_k \bmod n_k \end{cases} \qquad (2)$$

Ta ký hiệu: $n = n_1.n_2....n_k$, $N_i = n/n_i$. Ta có định lý sau đây:

Định lý 3.2.1 (định lý số dư Trung quốc). *Giả sử* ***các số nguyên*** $n_1, n_2,....,n_k$ *là từng cặp nguyên tố với nhau. Khi đó, hệ phương trình đồng dư tuyến tính* (2) *có một nghiệm duy nhất theo* mod*n :*

$x = \sum_{i=1}^{n} a_i N_i M_i \, mod \, n$

trong đó $M_i = N_i^{-1} \bmod n_i$ (có M_i vì N_i và n_i nguyên tố với nhau).

Nghiệm duy nhất nói trong định lý 3.2.1 được cho bởi biểu thức:

$x = \sum_{i=1}^{n} a_i N_i M_i \, mod \, n$

trong đó $M_i = N_i^{-1} \bmod n_i$ (có M_i vì N_i và n_i nguyên tố với nhau).

Thí dụ: Cặp phương trình

$x \equiv 3 \pmod 7$

và $x \equiv 7 \pmod{13}$

x=3*13*6+7*7*2 = 332mod91 =59

$x = \sum_{i=1}^{n} a_i N_i M_i \, mod \, n$

có một nghiệm duy nhất $x \equiv 59 \pmod{91}$.

Nếu $(n_1 , n_2) = 1$, thì cặp phương trình $x \equiv a \pmod{n_1}$ và $x \equiv a \pmod{n_2}$ có nghiệm duy nhất $x \equiv a \pmod{n}$ theo mod*n* với $n = n_1 n_2$.

Bài tập. Hãy giải hệ pt đồng dư tuyến tính sau :

$x \equiv 15 \pmod{43}$

$x \equiv 20 \pmod{53}$

x=42155mod2279=1133

1.3.Thặng dư thu gọn và phần tử nguyên thuỷ.

Tập $\boldsymbol{Z}_n = \{ 0,1,2,..., n-1\}$ thường được gọi là *tập các thặng dư đầy đủ theo* mod*n,* vì mọi số nguyên bất kỳ đều có thể tìm được trong $\boldsymbol{Z}_n$ một số đồng dư với mình (theo mod*n*). Tập $\boldsymbol{Z}_n$ là đóng đối với các phép tính cộng, trừ và nhân theo mod*n* , nhưng không đóng đối với phép chia, vì phép chia cho *a* theo mod*n* chỉ có thể thực hiện được khi *a* và *n* nguyên tố với nhau, tức khi gcd(*a* ,*n*) =1.

Bây giờ ta xét tập $\boldsymbol{Z}_n^* = \{ a \in \boldsymbol{Z}_n : \gcd(a, n) = 1\}$, tức $\boldsymbol{Z}_n^*$ là tập con của $\boldsymbol{Z}_n$ bao gồm tất cả các phần tử nguyên tố với *n*. Ta gọi tập đó là *tập các thặng dư thu gọn theo* mod*n.*

Mọi số nguyên nguyên tố với n đều có thể tìm thấy trong $\boldsymbol{Z}_n^*$ một đại diện đồng dư với mình theo mod$n$. Chú ý rằng nếu p là một số nguyên tố thì $\boldsymbol{Z}_p^* = \{1,2,...,p\text{-}1\}$.

Tập $\boldsymbol{Z}_n^*$ lập thành một nhóm con đối với phép nhân của $\boldsymbol{Z}_n$, vì trong $\boldsymbol{Z}_n^*$ phép chia theo mod$n$ bao giờ cũng thực hiện được, ta sẽ gọi $\boldsymbol{Z}_n^*$ là *nhóm nhân* của $\boldsymbol{Z}_n$.

Theo đại số học, ta gọi số các phần tử trong một nhóm là *cấp* của nhóm đó. Ta ký hiệu $\phi(n)$ là số các số nguyên dương bé hơn n và nguyên tố cùng nhau với n. Như vậy, nhóm $\boldsymbol{Z}_n^*$ có cấp $\phi(n)$, và nếu p là số nguyên tố thì nhóm $\boldsymbol{Z}_p^*$ có cấp p -1.

Ta nói một phần tử $g \in \boldsymbol{Z}_n^*$ có *cấp* m , nếu m là số nguyên dương bé nhất sao cho $g^m = 1$ trong $\boldsymbol{Z}_n^*$. Theo một định lý trong Đại số, ta có $m \mid \phi(n)$. Vì vậy, với mọi $b \in \boldsymbol{Z}_n^*$ ta luôn có $b^{\phi(n)} \equiv 1 \bmod n$.

Nếu p là số nguyên tố, thì do $\phi(p) = p - 1$, ta có với mọi $b \in \boldsymbol{Z}_p^*$:

$$b^{p-1} \equiv 1(mod\, p) \qquad (3)$$

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 mod$p$, chúng lập thành $\boldsymbol{Z}_p^*$. Theo thuật ngữ đại số, khi đó ta nói $\boldsymbol{Z}_p^*$ là một *nhóm cyclic* và b là một phần tử sinh, hay *phần tử nguyên thuỷ* của nhóm đó.

Ví dụ : p=13, kiểm tra xem α=2 có phải là phần tử nguyên thủy của Z_{13}* hay không?

$2^1 \bmod 13 = 2$	$2^2 \bmod 13 = 4$
$2^3 \bmod 13 = 8$	$2^4 \bmod 13 = 3$
$2^5 \bmod 13 = 6$	$2^6 \bmod 13 = 12$
$2^7 \bmod 13 = 11$	$2^8 \bmod 13 = 9$
$2^9 \bmod 13 = 5$	$2^{10} \bmod 13 = 10$
$2^{11} \bmod 13 = 7$	$2^{12} \bmod 13 = 1$

Trong lý thuyết số, người ta đã chứng minh được các tính chất sau đây của các phần tử nguyên thuỷ:

1. Với mọi số nguyên tố p, $\boldsymbol{Z}_p^*$ là nhóm cyclic, và có $\phi(p\text{-}1)$ phần tử nguyên thuỷ.
2. Nếu $p - 1 = p_1^{\alpha_1}.p_2^{\alpha_2}\ldots.p_s^{\alpha_s}$ là khai triển chính tắc của p -1, và nếu

$$a^{\frac{p-1}{p_1}} \neq 1(mod\, p), \ldots\ldots, a^{\frac{p-1}{p_s}} \neq 1(mod\, p),$$

thì a là phần tử nguyên thuỷ theo mod$p$ (tức của $\boldsymbol{Z}_p^*$).

3. Nếu g là phần tử nguyên thuỷ theo mod$p$, thì $\beta = g^i \bmod p$ với mọi i mà gcd(i, p - 1) = 1, cũng là phần tử nguyên thuỷ theo mod$p$.

Ba tính chất đó là cơ sở giúp ta tìm các phần tử nguyên thuỷ theo mod$p$, 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 $a^{p-1} \equiv 1 \pmod{p}$ (*định lý Fermat*).

b) Nếu $a \in \mathbf{Z}_n^*$, thì $a^{\varphi(n)} \equiv 1(mod\, n)$. Nếu $r \equiv s(mod\, \varphi(n))$ thì $a^r \equiv a^s(mod\, n)$ (*định lý Euler*).

Bài tập: Hãy tìm tất cả các phần tử nguyên thủy của nhóm nhân trong Z_{31}^*.

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

Ta xét phương trình đồng dư bậc hai có dạng đơn giản sau đây:

$$x^2 \equiv a(mod\, n),$$

trong đó n là một số nguyên dương, a là số nguyên với gcd(a,n) =1, và x là ẩn số. Phương trình đó không phải bao giờ cũng có nghiệm, khi nó có nghiệm thì ta nói a là một *thặng dư bậc hai* mod$n$; nếu không thì nói a là một *bất thặng dư bậc hai* mod$n$.

Tập các số nguyên nguyên tố cùng nhau với n được phân hoạch thành hai tập con: tập Q_n các thặng dư bậc hai mod$n$, và tập $\overline{Q_n}$ các bất thặng dư mod$n$.

Khi $n = p$ là số nguyên tố, ta có *tiêu chuẩn Euler* sau đây: Số a là thặng dư bậc hai mod$p$ nếu và chỉ nếu $a^{(p-1)/2} \equiv 1(mod\, p)$. Tiêu chuẩn đó được chứng minh như sau:

Giả sử có x sao cho $x^2 \equiv a(mod\, p)$, khi đó ta cũng sẽ có

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv x^{p-1} \equiv 1(mod\, p).$$

Ngược lại, giả sử $a^{(p-1)/2} \equiv 1(mod\, p)$. Khi đó $a \in Z_p^*$. Lấy b là một phần tử nguyên thuỷ mod$p$, ắt có một số i nào đó sao cho $a = b^i \, mod\, p$.Từ đó,

$$a^{(p-1)/2} \equiv b^{i(p-1)/2} \equiv 1(mod\, p).$$

Phần tử b có cấp p - 1, do đó (p - 1) chia hết i(p - 1)/2, i phải là số chẵn, i = 2j , và a có căn bậc hai là $\pm b^{\,j} \bmod p$.

Cho p là một số nguyên tố lẻ. Với mọi $a \geq 0$ ta định nghĩa *ký hiệu Legendre* $\left(\frac{a}{p}\right)$ như sau:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, khi \quad a \equiv 0(mod\, p)\,; \\ 1, khi \quad a \in Q_p\,; \\ -1, khi \quad a \notin Q_p. \end{cases}$$

Từ định nghĩa ta suy ra ngay *a là thặng dư bậc hai modp khi và chỉ khi* $\left(\frac{a}{p}\right)$= 1. Và theo tiêu chuẩn Euler nói trên, với mọi $a \geq 0$, ta có:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2}(mod\, p).$$

Bây giờ ta mở rộng ký hiệu Legendre để được *ký hiệu Jacobi* đối với mọi số nguyên lẻ $n \geq 1$ và mọi số nguyên $a \geq 0$, cũng được ký hiệu bởi $\left(\frac{a}{n}\right)$và được định nghĩa như sau: Giả sử a có khai triển chính tắc thành thừa số nguyên tố là $n = p_1^{\alpha_1}.p_2^{\alpha_2}\ldots.p_k^{\alpha_k}$thì

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}.\left(\frac{a}{p_2}\right)^{\alpha_2}\ldots.\left(\frac{a}{p_k}\right)^{\alpha_k}.$$

Khi $n = p$ là số nguyên tố thì giá trị của các ký hiệu Legendre và Jacobi là như nhau. Việc tính ký hiệu Legendre có thể phức tạp khi p rất lớn, trong khi việc tính ký hiệu Jacobi có thể thuận lợi hơn do có thể sử dụng các tính chất 1-4 sau đây:

1. Nếu $m_1 \equiv m_2(mod\, n)$, thì $\left(\frac{m_1}{n}\right) = \left(\frac{m_2}{n}\right)$.
2. $\left(\frac{2}{n}\right) = \begin{cases} 1, khi n \equiv \pm 1(mod\, 8), \\ -1, khi n \equiv \pm 3(mod\, 8). \end{cases}$
3. $\left(\frac{m_1.m_2}{n}\right) = \left(\frac{m_1}{n}\right).\left(\frac{m_2}{n}\right)$.
4. Nếu m và n đều là số lẻ, thì

$$\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right), khi m \equiv 3(mod\, 4) n \equiv 3(mod\, 4), \\ \left(\frac{n}{m}\right), khi m \equiv 1(mod\, 4) \vee n \equiv 1(mod\, 4). \end{cases}$$

Thí dụ: Dùng các tính chất đó, ta tính được:

$$\left(\frac{7411}{9283}\right) = \left(\frac{9283}{7411}\right) = \left(\frac{1872}{7411}\right) = \left(\frac{2}{7411}\right)^4.\left(\frac{117}{7411}\right) =$$
$$\left(\frac{117}{7411}\right) = -\left(\frac{7411}{117}\right) = -\left(\frac{40}{117}\right) = -\left(\frac{2}{117}\right)^3.\left(\frac{5}{117}\right) =$$
$$\left(\frac{5}{117}\right) = \left(\frac{117}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

9283 là một số nguyên tố. Do đó, giá trị -1 của ký hiệu Jacobi $\left(\frac{7411}{9283}\right)$ cũng là giá trị của cùng ký hiệu Legendre đó, và ta kết luận được rằng 7411 là bất thặng dư bậc hai mod 9283 , hay phương trình

$$x^2 \equiv 7411(mod\, 9\,283)$$

là vô nghiệm.

Bây giờ ta xét việc giải phương trình đồng dư bậc hai$x^2 \equiv a(mod\, n)$ (4)

trong một trường hợp đặc biệt khi $n = p$ là số nguyên tố có dạng $p = 4m + 3$, tức p đồng dư với 3 theo mod4, và a là một số nguyên nguyên tố với p. Theo tiêu chuẩn Euler ta biết phương trình (4) có nghiệm khi và chỉ khi $a^{(p-1)/2} \equiv 1(mod\, p)$. Khi đó ta có:

$$a^{\frac{p-1}{2}+1} \equiv a(mod\, p),$$

$$a^{2(m+1)} \equiv a(mod\, p),$$

do đó $x \equiv \pm a^{m+1} \pmod{p}$ là hai nghiệm của phương trình (4).

Bài 2. Số nguyên tố. Phân tích thành thừa số. Logarit rời rạc.

Trong tiết này ta sẽ xét ba bài toán có vai trò quan trọng trong lý thuyết mật mã, đó là ba bài toán:

- thử tính nguyên tố của một số nguyên,
- phân tích một số nguyên thành tích của các thừa số nguyên tố,
- và tính logarit rời rạc của một số theo một môđuyn nguyên tố.

1. Thử tính nguyên tố của một số.

Bài toán đặt ra rất đơn giản: Cho một số nguyên dương n bất kỳ. Hãy thử xem n có là số nguyên tố hay không? Bài toán được đặt ra từ những buổi đầu của số học, và trải qua hơn 2000 năm đến nay vẫn là một bài toán chưa có được những cách giải dễ dàng. Bằng những phương pháp đơn giản như phương pháp sàng Euratosthène, từ rất sớm người ta đã xây dựng được các bảng số nguyên tố đầu tiên, rồi tiếp tục bằng nhiều phương pháp khác tìm thêm được nhiều số nguyên tố lớn. Tuy nhiên, chỉ đến giai đoạn hiện nay của lý thuyết mật mã hiện đại, nhu cầu sử dụng các số nguyên tố và thử tính nguyên tố của các số mới trở thành một nhu cầu to lớn và phổ biến, đòi hỏi nhiều phương pháp mới có hiệu quả hơn. Trong mục này ta sẽ lược qua vài tính chất của số nguyên tố, sau đó giới thiệu một vài phương pháp thử tính nguyên tố của một số nguyên bất kỳ. Ta đã biết một số tính chất sau đây của các số nguyên tố và hợp số (trong các phát biểu dưới đây, ký hiệu $|A|$ chỉ cho số phần tử của tập hợp A):

1. <u>Tiêu chuẩn Euler-Solovay-Strassen:</u>

a) Nếu n là số nguyên tố, thì với mọi số nguyên dương a [n -1:

$$\left(\frac{a}{n}\right) \equiv a^{(n-1)/2}\, mod\, n.$$

b) Nếu n là hợp số , thì

$$\left|\left\{a : 1 \le a \le n-1, \left(\frac{a}{n}\right) \equiv a^{(n-1)/2}\, mod\, n\right\}\right| \le \frac{n-1}{2}.$$

2. <u>Tiêu chuẩn Solovay-Strassen-Lehmann :</u>

a) Nếu n là số nguyên tố, thì với mọi số nguyên dương a [n -1:

$$a^{(n-1)/2} \equiv \pm 1 (mod\, n).$$

b) Nếu n là hợp số, thì

$$\left|\{a : 1 \le a \le n-1, a^{(n-1)/2} \equiv \pm 1\, mod\, n\}\right| \le \frac{n-1}{2}.$$

3. Tiêu chuẩn Miller-Rabin :

a) Cho n là số nguyên lẻ, ta viết n - 1 = 2^e .u, với u là số lẻ. Nếu n là số nguyên tố, thì với mọi số nguyên dương a [n -1:

$$(a^u \equiv 1\, mod\, n) \vee \exists k < e (a^{2^k.u} \equiv -1\, mod\, n).$$

b) Nếu n là hợp số, thì $\left|\left\{a : 1 \le a \le n-1, (a^u \equiv 1\, mod\, n) \vee \exists k < e(a^{2^k.u} \equiv -1\, mod\, n)\right\}\right| \le \frac{n-1}{4}$.

Các tiêu chuẩn kể trên là cơ sở để ta xây dựng các thuật toán xác suất kiểu Monte-Carlo thử tính nguyên tố (hay hợp số) của các số nguyên. Chẳng hạn, từ tiêu chuẩn thứ nhất ta có *thuật toán Euler-Solovay-Strassen* sau đây:

Dữ liệu vào: số nguyên dương n và t số ngẫu nhiên $a_1,...,a_t$ (1[a_i[n -1),

1. **for** i = 1 **to** t do $\left|\left\{a : 1 \le a \le n-1, \left(\frac{a}{n}\right) \equiv a^{(n-1)/2}\, mod\, n\right\}\right| \le \frac{n-1}{2}$.
   $\left|\left\{a : 1 \le a \le n-1, \left(\frac{a}{n}\right) \equiv a^{(n-1)/2}\, mod\, n\right\}\right| \le \frac{n-1}{2}$.
2. **if** $\left(\frac{a_i}{n}\right) \equiv a_i^{(n-1)/2}\, mod\, n$, **then**
3. **answer** "n là số nguyên tố "
4. else
5. **answer** "n là hợp số " and **quit**

Thuật toán này nếu cho trả lời "n là hợp số " thì đúng n là hợp số, nhưng nếu nó cho trả lời "n là số nguyên tố " thì trả lời đó có thể sai với một xác suất ε nào đó. Như vậy, thuật toán đó là một thuật toán xác suất Monte-Carlo *thiên về có* nếu xem nó là thuật toán thử tính *là hợp số* ; còn nó là một thuật toán xác suất *thiên về không* nếu xem nó là thuật toán thử tính *nguyên tố* của các số nguyên.

Tương tự như vậy, dựa vào các tiêu chuẩn 2 và 3 ta cũng có thể xây dựng các thuật toán xác suất Solovay-Strassen-Lehmann và Miller-Rabin kiểu Monte-Carlo để thử tính nguyên tố (hay là hợp số) của các số nguyên. Hai thuật toán đó chỉ khác thuật toán Euler-Solovay-Strassen kể trên ở chỗ công thức trong hàng lệnh thứ 2 cần được thay tương ứng bởi

$$a^{(n-1)/2} \equiv \pm 1\, \boldsymbol{mod}\, n$$

hay

$$(a^u \equiv 1\, mod\, n) \vee \exists k < e (a^{2^k.u} \equiv -1\, mod\, n)$$ trong đó u và e được xác định bởi: n - 1 = 2^e.u , u là số lẻ.

Xác suất sai lầm ε khi nhận được kết quả "*n* là số nguyên tố " trong các thuật toán đó được tính như sau: Giả sử *n* là một số lẻ trong khoảng *N* và 2*N* , tức *N* <*n* < 2*N* . Gọi A là sự kiện "*n* là hợp số ", và B là sự kiện "thuật toán cho kết quả trả lời *n* là số nguyên tố ". Ta phải tính xác suất ε =*p* (A | B). Theo tính chất b) của tiêu chuẩn Euler-Solovay-Strassen, nếu *n* là hợp số, thì sự kiện

$$\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \bmod n$$

đối với mỗi *a* ngẫu nhiên (1[*a* [*n* - 1) có xác suất [1/2, vì vậy ta có

$$p\left(\frac{B}{A}\right) \leq \frac{1}{2^t}.$$

Theo công thức Bayes ta có

$$p\left(\frac{A}{B}\right) = \frac{p\left(\frac{B}{A}\right).p(A)}{p(B)} = \frac{p\left(\frac{B}{A}\right).p(A)}{p\left(\frac{B}{A}\right).p(A)+p\left(\frac{B}{\bar{A}}\right).p(\bar{A})}.$$

Theo định lý về số nguyên tố, số các số nguyên tố giữa *N* và 2*N* xấp xỉ $\frac{N}{\ln N} \approx \frac{n}{\ln n}$, số các số lẻ là $\frac{N}{2} \approx \frac{n}{2}$, do đó $p(\bar{A}) \approx \frac{2}{\ln n}$, và $p(A) \approx 1 - \frac{2}{\ln n}$. Dĩ nhiên ta có $p\left(\frac{B}{\bar{A}}\right) = 1$. Thay các giá trị đó vào công thức trên, ta được

$$p\left(\frac{A}{B}\right) \leq \frac{2^{-t}\left(1-\frac{2}{\ln n}\right)}{2^{-t}\left(1-\frac{2}{\ln n}\right)+\frac{2}{\ln n}} = \frac{\ln n-2}{\ln n-2+2^{t+1}}. \qquad (5)$$

Đánh giá đó cũng đúng đối với thuật toán Solovay-Strassen-Lehmann, còn đối với thuật toán Miler-Rabin thì ta được một đánh giá tốt hơn, cụ thể là

$$p\left(\frac{A}{B}\right) = \frac{\ln n-2}{\ln n-2+2^{2t+1}}. \qquad (6)$$

Chú ý rằng khi *t* =50 thì đại lượng ở vế phải của (5) $\approx 10^{-13}$, và vế phải của (6) $\approx 10^{-28}$; do đó nếu chọn cho dữ liệu vào thêm khoảng 50 số ngẫu nhiên a_i thì các thuật toán Euler-Solovay-Strassen và Solovay-Strassen-Lehmann sẽ thử cho ta một số là nguyên tố với xác suất sai lầm [10^{-13} và thuật toán Miller-Rabin với xác suất sai lầm [10^{-28} !

Ta có thể tính được rằng độ phức tạp tính toán về thời gian của các thuật toán xác suất kể trên là vào cỡ đa thức của log*n* , tức là đa thức của độ đài biểu diễn của dữ liệu vào

(là số n), tuy nhiên các thuật toán đó chỉ cho ta thử tính nguyên tố của một số với một xác suất sai lầm ε nào đó, dù ε là rất bé. Trong nhiều ứng dụng, ta muốn có được những số nguyên tố với độ chắc chắn 100% là số nguyên tố. Do đó, dù đã có các thuật toán xác suất như trên, người ta vẫn không ngừng tìm kiếm những thuật toán tất định để thử tính nguyên tố với độ chính xác tuyệt đối. Trong mấy chục năm gần đây, một số thuật toán đã được đề xuất, trong đó có những thuật toán đặc sắc như thuật toán thử tổng Jacobi, được phát hiện bởi Adleman, Pomerance và Rumely, sau đó được đơn giản hoá bởi Cohen và Lenstra; thuật toán thử bằng đường cong elliptic, được đề xuất bởi Goldwasser, Kilian, Adleman và Huang, được tiếp tục hoàn thiện bởi Atkin và Morain, các thuật toán này đã được dùng để tìm nhiều số nguyên tố rất lớn, thí dụ dùng thuật toán Atkin-Morain đã chứng tỏ được số $(2^{3539}+1)/3$ có 1065 chữ số thập phân là số nguyên tố.

Gần đây, vào tháng 8/2002, các nhà toán học Ân độ Agrawal, Kayal và Saxena đã đưa ra một thuật toán tất định mới thử tính nguyên tố có độ phức tạp tính toán thời gian đa thức khá đơn giản, thuật toán đó được mô tả như sau:

Thuật toán Agrawal-Kayal-Saxena:

Input: integer $n > 1$

1. if (n is of the form a^b, $b > 1$) ouput COMPOSITE;
2. r =2;
3. while ($r < n$) {
4. if (gcd(n , r)≠ 1) ouput COMPOSITE;
5. if (r is prime)
6. let q be the largest prime factor of r - 1;
7. if ($q \geq 4\sqrt{r}\, log\, n$) and ($n^{\frac{r-1}{q}} \neq 1 (mod\, r)$)
8. break;
9. $r \leftarrow r + 1$;

10. }

11. for a = 1 to $2\sqrt{r}\ log\ n$

12. if $((x-a)^n \neq (x^n - a)(mod x^r - 1, n))$ ouput COMPOSITE;

13. output PRIME;

Thuật toán này đã được một số nhà toán học kiểm nghiệm , đánh giá cao và xem là một thuật toán đẹp, có thể dùng cho việc kiểm thử tính nguyên tố của các số nguyên.

Trong thực tiễn xây dựng các giải pháp mật mã, thường có nhu cầu có các số nguyên tố rất lớn. Để tìm được các số như vậy, người ta thường chọn ngẫu nhiên một số rất lớn, rồi dùng trước cho nó một thuật toán xác suất chẳng hạn như thuật toán Miller-Rabin; nếu thuật toán cho ta kết quả "là số nguyên tố" với một xác suất sai ε nào đó, thì sau đó ta dùng tiếp một thuật toán tất định (chẳng hạn như thuật toán trên đây) để bảo đảm chắc chắn 100% rằng số đó là số nguyên tố. Thuật toán Agrawal-Kayal-Saxena trên đây được chứng tỏ là có độ phức tạp thời gian đa thức cỡ $O((\log n)^{12})$ khi thử trên số n ; và nếu số nguyên tố được thử có dạng Sophie Germain, tức dạng $2p+1$, thì độ phức tạp thời gian sẽ chỉ là cỡ $O((\log n)^6)$.

3. **Phân tích thành thừa số nguyên tố.**

Bài toán phân tích một số nguyên > 1 thành thừa số nguyên tố cũng được xem là một bài toán khó thường được sử dụng trong lý thuyết mật mã. Biết một số n là hợp số thì việc phân tích n thành thừa số mới là có nghĩa; do đó thường khi để giải bài toán phân tích n thành thừa số, ta thử trước n có là hợp số hay không (chẳng hạn bằng một trong các thuật toán ở mục trước); và bài toán phân tích n thành thừa số có thể dẫn về bài toán *tìm một ước số của n,* vì khi biết một ước số d của n thì tiến trình phân tích n được tiếp tục thực hiện bằng cách phân tích d và n/d.

Bài toán phân tích thành thừa số, hay bài toán tìm ước số của một số nguyên cho trước, đã được nghiên cứu nhiều, nhưng cũng chưa có một thuật toán hiệu quả nào để giải nó trong trường hợp tổng quát; do đó người ta có khuynh hướng tìm thuật toán giải nó trong những trường hợp đặc biệt, chẳng hạn khi n có một ước số nguyên tố p với p -1 là ***B***-mịn với một cận ***B*** >0 nào đó, hoặc khi n là số Blum, tức là số có dạng tích của hai số nguyên tố lớn nào đó ($n = p.q$).

Ta xét trường hợp thứ nhất với (p -1)-thuật tóan Pollard như sau: Một số nguyên n được gọi là ***B-mịn***, nếu tất cả các ước số nguyên tố của nó đều $\leq B$. ý chính chứa trong (p-1)-thuật toán Pollard là như sau: Giả sử n là B-mịn. Ký hiệu Q là bội chung bé nhất của tất cả các luỹ thừa của các số nguyên tố $\leq B$ mà bản thân chúng $\leq n$. Nếu $q^{\,l} \leq n$ thì $l \ln q \leq \ln n$, tức $l \leq \left\lfloor \frac{ln\, n}{ln\, q} \right\rfloor$ ($\lfloor x \rfloor$là số nguyên bé nhất lớn hơn x). Ta có

$$Q = \prod_{q \le B} q^{\lfloor \ln n / \ln q \rfloor},$$

trong đó tích lấy theo tất cả các số nguyên tố khác nhau $q \le B$. Nếu p là một thừa số nguyên tố của n sao cho p -1 là B-mịn, thì p -1 $\mid Q$, và do đó với mọi a bất kỳ thỏa mãn gcd(a,p) = 1, theo định lý Fermat ta có

$a^Q \equiv 1 \pmod{p}$). Vì vậy, nếu lấy d =gcd(a^Q - 1, n) thì $p \mid d$. Nếu $d = n$ thì coi như thuật toán không cho ta điều mong muốn, tuy nhiên điều đó chắc không xảy ra nếu n có ít nhất hai thừa số nguyên tố khác nhau. Từ những lập luận đó ta có:

(p - 1)-thuật toán Pollard phân tích thành thừa số :

INPUT: một hợp số n không phải là luỹ thừa của một số nguyên tố.

OUTPUT: một thừa số không tầm thường của n .

1. Chọn một cận cho độ mịn B.
2. Chọn ngẫu nhiên một số nguyên a , $2 \le a \le n$ - 1, và tính d = gcd(a,n). Nếu $d \ge 2$ thì cho ra kết quả (d).
3. Với mỗi số nguyên tố $q \le B$ thực hiện:

   Tính $l = \left\lfloor \frac{\ln n}{\ln q} \right\rfloor$.

   Tính $a \leftarrow a^{q^l} \bmod n$.
4. Tính d = gcd(a -1, n).
5. Nếu $1 < d < n$ thì cho ra kết quả (d). Nếu ngược lại thì thuật toán coi như không có kết quả.

Thí dụ: Dùng thuật toán cho số n = 19048567. Ta chọn B =19, và a =3, và tính được gcd(3,n) =1. Chuyển sang thực hiện bước 3 ta được bảng sau đây (mỗi hàng ứng với một giá trị của q) :

q	l	A
2	24	2293244
3	15	13555889
5	10	16937223
7	8	15214586
11	6	9685355
13	6	13271154
17	5	11406961
19	5	554506

Sau đó ta tính d =gcd(554506-1,19048567) = 5281. Vậy ta được một thừa số p = 5281, và do đó một thừa số nữa là $q = n/p$ = 3607. Cả hai thừa số đó đều là nguyên tố.

Chú ý rằng ở đây p -1 = 5280 = 2^5.3.5.11 , có tất cả các ước số nguyên tố đều ≤ 19, do đó chắc chắn thuật toán sẽ kết thúc có kết quả. Thuật toán sẽ kết thúc không có kết quả khi độ mịn B được chọn quá bé để không một thừa số nguyên tố p nào của n mà p -1 chỉ chứa các ước số nguyên tố ≤ B. Như vậy, có thể xem (p -1)-thuật toán Pollard phân tích n thành thừa số nguyên tố là có hiệu quả đối với những số nguyên n là B-mịn, người ta tính được thời gian cần để thực hiện thuật toán đó là cỡ $O(B \ln n / \ln B)$ phép nhân theo môđuyn.

Bây giờ ta xét trường hợp các số nguyên Blum, tức là các số có dạng $n = p.q$, tích của hai số nguyên tố lớn. Trước hết ta chú ý rằng nếu ta biết hai số nguyên khác nhau x và y sao cho $x^2 \equiv y^2 (mod\, n)$ thì ta dễ tìm được một thừa số của n . Thực vậy, từ $x^2 \equiv y^2 (mod\, n)$ ta có $x^2 - y^2 = (x + y)(x - y)$ chia hết cho n , do n không là ước số của $x + y$ hoặc $x - y$, nên gcd($x - y$, n) phải là một ước số của n, tức bằng p hoặc q .

Ta biết nếu $n = p.q$ là số Blum, thì phương trình đồng dư

$$x^2 \equiv a^2 (mod\, n)$$

có 4 nghiệm, hai nghiệm tầm thường là $x = a$ và $x = -a$. Hai nghiệm không tầm thường khác là $\pm b$, chúng là nghiệm của hai hệ phương trình đồng dư bậc nhất sau đây:

$$\begin{cases} x \equiv a (mod\, p) \\ x \equiv -a (mod\, q) \end{cases} \begin{cases} x \equiv -a (mod\, p) \\ x \equiv a (mod\, q) \end{cases}$$

Bằng lập luận như trên, ta thấy rằng nếu n là số Blum, a là một số nguyên tố với n, và ta biết một nghiệm không tầm thường của phương trình $x^2 \equiv a^2 (mod\, n)$, tức biết một $x \neq \pm a$ sao cho $x^2 \equiv a^2 (mod\, n)$ thì gcd($x - a$, n) sẽ là một ước số của n . Những điều trên đây là căn cứ cho một số phương pháp tìm ước số nguyên tố của một số nguyên dạng Blum; ý chung của các phương pháp đó là dẫn về việc tìm một nghiệm không tầm thường của một phương trình dạng $x^2 \equiv a^2 (mod\, n)$, chẳng hạn như phương trình $x^2 \equiv 1 (mod\, n)$.

Một trường hợp khá lý thú trong lý thuyết mật mã là khi ta biết hai số a ,b là nghịch đảo của nhau theo mod$\phi(n)$ (nhưng không biết $\phi(n)$), và tìm một phân tích thành thừa số của n. Bài toán được đặt ra cụ thể là: Biết n có dạng B**lum**, biết a và b sao cho $ab \equiv 1 (\text{mod}\, \phi(n))$. Hãy tìm một ước số nguyên tố của n , hay tìm một nghiệm không tầm thường của phương trình $x^2 \equiv 1 (mod\, n)$. Ta giả thiết ab - 1 = 2^s. r với r là số lẻ. Ta phát triển một thuật toán xác suất kiểu Las Vegas như sau: Ta chọn một số ngẫu nhiên v ($1 \leq v \leq n$ - 1). Nếu may

mắn *v* là bội số của *p* hay *q*, thì ta được ngay một ước số của *n* là gcd(*v*,*n*). Nếu *v nguyên tố với n* , thì ta tính các bình phương liên tiếp kể từ v^r, được $v^r, v^{2r}, v^{4r}, \ldots$ cho đến khi được $v^{2^t.r} \equiv 1(mod\, n)$ với một t nào đó. Số t như vậy bao giờ cũng đạt được, vì có $2^s . r \equiv 0 \pmod{\phi(n)}$ nên có $v^{2^s.r} \equiv 1(mod\, n)$. Như vậy, ta đã tìm được một số $x = v^{2^{t-1}.r}$ sao cho $x^2 \equiv 1(mod\, n)$. Tất nhiên có $x \neq 1 \pmod{n}$. Nếu cũng có $x \neq -1 \pmod{n}$ thì *x* là nghiệm không tầm thường của $x^2 \equiv 1(mod\, n)$, từ đó ta có thể tìm ước số của *n* . Nếu không thì thuật toán coi như thất bại, cho ta kết quả *không đúng.* Người ta có thể ước lượng xác suất cho kết quả *không đúng* với một lần thử với một số *v* là < 1/2, do đó nếu ta thiết kế thuật toán với *m* số ngẫu nhiên $v_1, \ldots v_m$, thì sẽ có thể đạt được xác suất cho kết quả *không đúng* là $< 1/2^m$!

Tính logarit rời rạc theo môđuyn nguyên tố.

Cho *p* là một số nguyên tố, và α là một phần tử nguyên thuỷ theo mod*p,* tức là phần tử nguyên thuỷ của nhóm Z_p^*. *Bài toán tính logarit rời rạc* theo mod*p* là bài toán tìm, với mỗi số $\beta \in Z_p^*$,một số *a* ($1 \leq a \leq p$ -1) sao cho $\beta = \alpha^a \bmod p$, tức là $a = \log_\alpha \beta \pmod{p-1}$. Một thuật toán tầm thường để giải bài toán này là thuật toán *duyệt toàn bộ* các số *a* từ 1 đến *p* - 1, cho đến khi tìm được *a* thoả mãn $\beta = \alpha^a \bmod p$. Tất nhiên, thuật toán này là không hiệu quả nếu *p* là số nguyên tố rất lớn. Một biến dạng của thuật toán đó với ít nhiều hiệu quả hơn là *thuật toán Shanks* sau đây:

Đặt $m = \left[\sqrt{p-1}\right]$. Ta tìm *a* dưới dạng $a = mj + i, 0 \leq j, i \leq m - 1$. Rõ ràng $\beta = \alpha^a \bmod p$ khi và chỉ khi $\alpha^{mj} \equiv \beta\alpha^i (mod\, p)$. Ta lập hai danh sách gồm các cặp (j, α^{mj}) và các cặp $(i, \beta\alpha^{-i})$ với *j* và i chạy từ 0 đến m - 1. Khi phát hiện ra có hai cặp từ hai danh sách đó có hai phần tử thứ hai bằng nhau là ta được kết quả $a = mj + i$, đó chính là giá trị $\log_\alpha \beta$ mà ta cần tìm. Thuật toán Shanks có độ phức tạp cỡ *O*(*m*) phép toán nhân và *O*(*m*) bộ nhớ (chưa kể $O(m^2)$ phép so sánh).

Một thuật toán khác, *thuật toán Polig-Hellman*, thường được dùng có hiệu quả trong trường hợp *p* -1 chỉ có các thừa số nguyên tố bé, có nội dung như sau: Giả thiết rằng *p* - 1 có dạng phân tích chính tắc là

$$p-1=\prod_{i=1}^{k} p_i^{c_i}.$$

Để tìm $a=\log_\alpha \beta \pmod{p-1}$, ta tìm các số a_i sao cho $a_i \equiv a \bmod p_i^{c_i}$ với $i = 1,...,k$. Sau khi tìm được các a_i như vậy, thì hệ phương trình $x \equiv a_i \bmod p_i^{c_i} \quad (i=1,\dots,k)$,được giải theo định lý số dư Trung quốc, sẽ cho ta lời giải $x \equiv a(\bmod p-1)$ cần tìm. Vậy, vấn đề là xác định các $a_i \bmod p_i^{c_i} \quad (i=1,\dots,k)$. Vấn đề này được phát biểu lại như sau: Giả sử q là một ước số nguyên tố của p - 1, và $q^c \mid p-1$ nhưng không còn $q^{c+1} \mid p-1$. Ta cần tìm $x = a \bmod q^c$. Ta biểu diễn x dưới dạng số q - phân như sau:

$$x=\sum_{i=0}^{c-1} x_i q_i \ (0 \le x_i \le q-1).$$

Vì $x = a \bmod q^c$ nên a viết được dưới dạng $a = x + q^c.s$, và vì $\alpha^{p-1} \equiv 1(\bmod p)$, nên ta có

$$\beta^{\frac{p-1}{q}} \equiv \alpha^{a\frac{p-1}{q}} \equiv (\alpha^{p-1})^{\frac{a}{q}} \equiv \alpha^{\frac{(p-1)x_0}{q}} (\bmod p).$$

Ta đặt $\gamma = \alpha^{(p-1)/q}$, và tính lần lượt $\gamma^0, \gamma^1, \gamma^2, \dots$, đồng thời so sánh với $\beta^{(p-1)/q} \bmod p$, ta sẽ tìm được i sao cho $\gamma^i \equiv \beta^{(p-1)/q} \bmod p$. Ta lấy số i đó là x_0, tức $x_0 = i$. Nếu $c = 1$ thì $x = x_0$, ta tìm xong x . Nếu $c > 1$ thì bằng cách đặt $\beta' = \beta\alpha^{-x_0}$ và $x' = log_\alpha \beta' \bmod q^c$ ta dễ thấy rằng

$$x'=\sum_{i=1}^{c-1} x_i q_i.$$

Từ đó ta suy ra

$$\beta'^{(p-1)/q^2} \equiv \alpha^{(p-1)x_1/q} \bmod p.$$

Tương tự như ở bước trên, tính lần lượt $\gamma^0, \gamma^1, \gamma^2, \dots$, đồng thời so sánh với $\beta'^{(p-1)/q^2}$, ta sẽ tìm được x_1.

Cứ làm như vậy, ta sẽ tìm được dần tất cả các giá trị x_i với $i = 0,1,...,c-1$, tức là tính được x. Sau khi tìm được tất cả các giá trị x ứng với mọi ước số nguyên tố q của p , thì theo một nhận xét ở trên, chỉ cần giải tiếp một hệ phương trình đồng dư bậc nhất theo các môđuyn từng cặp nguyên tố với nhau (bằng phương pháp số dư Trung quốc), ta sẽ tìm được số a cần tìm, $a = \log_\alpha \beta$ theo mod$p$.

Thí dụ: Cho $p = 29$ và $\alpha = 2$. Hãy tính $a = \log_2 18$ theo mod29. Ta có $p - 1 = 28 = 2^2 . 7^1$. Theo thuật toán Polig-Hellman, ta tìm lần lượt $a \bmod 4$ và $a \bmod 7$. Theo các bước tính toán như mô tả ở trên, ta sẽ tìm được $a \bmod 4 = 3$ và $a \bmod 7 = 4$ .Từ đó giải hệ phương trình

$$\begin{cases} x \equiv 3(\bmod 4), \\ x \equiv 4(\bmod 7) \end{cases}$$

ta được nghiệm $x \equiv 11 \pmod{28}$, tức được $11 = \log_2 18$ theo mod29. Thuật toán Polig-Hellman cho ta một cách tính logarit rời rạc khá hiệu quả, nhưng chỉ khi p -1 chỉ có các thừa số nguyên tố bé. Vì vậy, nếu p -1 có ít nhất một thừa số nguyên tố lớn thì thuật toán đó khó được thực hiện có hiệu quả, tức trong trường hợp đó bài toán tính logarit rời rạc theo mod$p$ vẫn là một bài toán khó. Một lớp các số nguyên tố p mà p - 1 có ít nhất một ước số nguyên tố lớn là lớp các số nguyên tố dạng $p = 2q + 1$, trong đó q là nguyên tố. Những số nguyên tố dạng đó được gọi là số nguyên tố Sophie Germain, có

vai trò quan trọng trong việc xây dựng một lớp khá thông dụng các hệ mật mã có khoá công khai.

Người ta cũng đã nghiên cứu phát triển nhiều thuật toán khác, cả thuật toán tất định, cả thuật toán xác suất, để tính logarit rời rạc, nhưng chưa có thuật toán nào được chứng tỏ là có độ phức tạp tính toán với thời gian đa thức.