Chương 4.

THẶNG DƯ BÌNH PHƯƠNG.

Giả sử p là một số nguyên tố lẻ, a là số nguyên tố cùng nhau với p. Vấn đề đặt ra là: *khi nào a là số chính phương modulo p?* Vấn đề này không chỉ có giá trị lí thuyết, mà như ta sẽ thấy về sau, có nhiều ứng dụng quan trọng. Để nghiên cứu vấn đề đặt ra, công cụ quan trọng là các kí hiệu Legendre và Jacobi mà ta sẽ xét trong chương này.

§1. Kí hiệu Legendre.

Định nghĩa 4.1. Giả sử m là số nguyên dương. Số a được gọi là một *thặng dư bình phương của m* nếu $(a,m)=1$ và đồng dư $x^2 \equiv a(mod\ m)$ có nghiệm. Nếu ngược lại, ta nói a là *không thặng dư bình phương* của m.

Ta sẽ chứng tỏ rằng, nếu a là một số nguyên tố lẻ, trong số các số 1, 2, ..., p-1 có đúng một nửa là thặng dư bình phương.

Bổ đề 4.1. *Giả sử p là số nguyên tố lẻ, a là số nguyên không chia hết cho p. Khi đó đồng dư sau đây không có nghiệm, hoặc có đúng hai nghiệm không đồng dư modulo p:*

$$x^2 \equiv a(mod\ p).$$

Chứng minh. Giả sử có nghiệm $x=x_0$. Khi đó, dễ chứng minh rằng $x=-x_0$ là một nghiệm không đồng dư với x_0. Ta sẽ chỉ ra rằng, nghiệm tuỳ ý khác $x=x_1$ đồng dư với x_0 hoặc $-x_0$.

Thật vậy, ta có: $x_0^2 \equiv x_1^2 (mod\ p)$, tức là $x_0^2-x_1^2=(x_0+x_1)(x_0-x_1) \equiv 0(mod\ p)$. Do đó, hoặc $p|x_0+x_1$, hoặc $p|x_0-x_1$, điều phải chứng minh.

Định lí 4.3. *Nếu p là một số nguyên tố lẻ, thì trong các số 1, 2, ..., p-1 có đúng (p-1)/2 thặng dư bình phương.*

Chứng minh. Để tìm tất cả các thặng dư modulo p trong các số 1,2,...,p-1, trước tiên ta bình phương các số đó và xét các thặng dư dương bé nhất modulo p của các kết quả nhận được. Các thặng dư dương bé nhất này là tất cả các thặng dư bình phương trong các số từ 1 đến p-1. Giả sử a là một thặng dư như vậy. Vì phương trình đồng dư $x^2 \equiv a(mod\ p)$ có đúng hai nghiệm, nên trong số $(p-1)$ bình phương đang xét, phải có hai bình phương thặng dư a: Số thặng dư bình phương đúng bằng (p-1)/2.

Để xét các thặng dư bình phương, người ta thường dùng các kí hiệu quan trọng mà ta sẽ nghiên cứu trong chương này.

Định nghĩa 4.4. Giả sử p là một số nguyên tố lẻ và a là một số nguyên không chia hết cho p. *Kí hiệu Legendre* $\left[\frac{a}{p}\right]$ được định nghĩa như sau:

$$\left[\frac{a}{p}\right] = \begin{cases} 1, \text{ nếu } a \text{ là thặng dư bình phương của } p \\ -1, \text{ nếu ngược lại.} \end{cases}$$

Ví dụ. Dễ tính được:

$$\left[\frac{1}{11}\right] = \left[\frac{3}{11}\right] = \left[\frac{4}{11}\right] = \left[\frac{5}{11}\right] = \left[\frac{9}{11}\right] = 1.$$
$$\left[\frac{2}{11}\right] = \left[\frac{6}{11}\right] = \left[\frac{7}{11}\right] = \left[\frac{8}{11}\right] = \left[\frac{10}{11}\right] = -1.$$

Tiêu chẩn sau đây thường được dùng để chứng minh các tính chất của kí hiệu Legendre.

Định lí (Tiêu chuẩn Euler). *Giả sử p là số nguyên tố lẻ, và a là số nguyên dương không chia hết cho p. Khi đó:*

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

Chứng minh. Trước tiên, giả sử rằng $\left[\frac{a}{p}\right] = 1$. Khi đó, đồng dư $x^2 \equiv a (mod\ p)$ có nghiệm $x = x_0$. Theo định lí Fermat bé, ta có:

$$a^{(p-1)/2} = (x_0^2)^{(p-1)/2} = x_0^{p-1} \equiv 1 (mod\ p)$$

Chỉ còn phải xét trường hợp $\left[\frac{a}{p}\right] = -1$. Khi đó , đồng dư $x^2 \equiv a (mod\ p)$ vô nghiệm. Với mỗi i sao cho $1 \le i \le p-1$, tồn tại duy nhất j $(1 \le j \le p-1)$ để $ij \equiv a (mod\ p)$. Rõ ràng $i \ne j$, nên ta có thể nhóm các số $1, ..., p-1$ thành $(p-1)/2$ cặp với tích từng cặp đồng dư a modulo p. Nhân các cặp này với nhau ta được:

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

Từ định lí Wilson ta có:

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

Định lí được chứng minh.

Những tính chất sau đây cho phép tính được dễ dàng kí hiệu Legendre.

Định lí 4.5. *Giả sử p là một số nguyên tố lẻ, a và b là các số nguyên không chia hết cho p. Khi đó:*

(i) Nếu $a \equiv b(\text{mod } p)$ *thì* $\left[\frac{a}{p}\right] = \left[\frac{b}{p}\right]$.

(ii) $\left[\frac{a}{p}\right]\left[\frac{b}{p}\right] = \left[\frac{ab}{p}\right]$.

(iii) $\left[\frac{a^2}{p}\right] = 1$.

Chứng minh. (i). Nếu $a \equiv b(\text{mod } p)$ thì $x^2 \equiv a(\text{mod } p)$ có nghiệm nếu và chỉ nếu $x^2 \equiv b(\text{mod } p)$ có nghiệm. Do đó $\left[\frac{a}{p}\right] = \left[\frac{b}{p}\right]$.

(ii). Bởi tiêu chuẩn Euler ta có:

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

$$\left[\frac{ab}{p}\right] \equiv (ab)^{(p-1)/2}(\text{mod } p).$$

Như vậy,

$$\left[\frac{a}{p}\right]\left[\frac{b}{p}\right] \equiv a^{(p-1)/2}b^{(p-1)/2} = (ab)^{(p-1)/2} \equiv \left[\frac{ab}{p}\right] (\text{mod } p).$$

Vì giá trị của kí hiệu Legendre chỉ có thể là ± 1 nên ta có đẳng thức cần chứng minh.

(iii) Vì $\left[\frac{a}{p}\right] = \pm 1$ nên từ phần trên ta có

$$\left[\frac{a^2}{p}\right] = \left[\frac{a}{p}\right]\left[\frac{a}{p}\right] = 1.$$

Định lí trên cho thấy rằng tích của hai *thặng dư bình phương* hoặc hai *không thặng dư bình phương* là một *thặng dư bình phương*, tích của một *thặng dư bình phương* và một *không thặng dư bình phương* là một *không thặng dư bình phương*.

Tiêu chuẩn Euler cho biết khi nào thì các số nguyên lẻ nhận -1 là thặng dư bình phương.

Định lí 4.6. *Nếu p là số nguyên tố lẻ thì*

$$\left[\frac{-1}{p}\right] = \begin{cases} 1, & khi\ \ p \equiv 1 (\mathrm{mod}\, 4) \\ -1, & khi\ \ p \equiv -1 (\mathrm{mod}\, 4) \end{cases}$$

Chứng minh. Theo tiêu chuẩn Euler ta có:

$$\left[\frac{-1}{p}\right] \equiv (-1)^{(p-1)/2} (\mathrm{mod}\ p).$$

Nếu $p \equiv 1 (mod\ 4)$ thì $p=4k+1$ với k nguyên nào đó. Như vậy,

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

tức là $\left[\frac{-1}{p}\right]=-1$.

Định lí 4.7. (Bổ đề Gauss). *Giả sử p là số nguyên tố lẻ và (a,p)=1. Nếu s là số các thặng dư dương bé nhất của các số nguyên a,2a,...((p-1)/2)a lớn hơn p/2, thì* $\left[\frac{a}{p}\right]=(-1)^s$.

Chứng minh. Trong số các thặng dư dương bé nhất của các số nguyên *a,2a,..., ((p-1)/2)a,* giả sử $u_1,u_2,...,u_s$ là các thặng dư lớn hơn p/2, và $v_1,v_2,...,v_t$ là các thặng dư nhỏ hơn *p/2*. Vì *(ja,p)=1* với mọi *j,* $1 \le j \le (p-2)/2$, nên tất cả các thặng dư dương bé nhất nói trên đều nằm trong tập hợp *1,...,p-1*.

Ta sẽ chứng tỏ rằng, $p-u_1,..., p-u_s, v_1,...,v_t$ chính là tập hợp các số *1,...(p-1)/2,* xếp theo thứ tự nào đó. Có cả thảy *(p-1)/2* số không vượt quá (p-1)/2, nên chỉ còn phải chứng minh rằng không có hai số nào đồng dư với nhau.

Rõ ràng không có hai số u_i nào, cũng như không có hai số v_j nào đồng dư với nhau modulo *p*. Thật vậy, nếu ngược lại, ta sẽ có đồng dư $ma \equiv na (mod\ p)$ với *m, n* dương nào đó không vượt quá *(p-1)/2*. Vì *(a,p)=1* nên từ đó suy ra $m \equiv n (mod\ p)$: Mâu thuẫn.

Tương tự như trên, có thể thấy rằng không có $p-u_i$ nào đó đồng dư với v_j.

Vậy ta có:

$$(p-u_1)...(p-u_s)v_1...v_t \equiv \left[\frac{p-1}{2}\right]!(mod\ p).$$

Từ đó suy ra

$$(-1)^s u_1...u_s v_1...v_t \equiv \left[\frac{p-1}{2}\right]!(mod\ p).$$

Mặt khác, vì $u_1,...u_s,v_1,...v_t$ là các thặng dư dương bé nhất của $a,2a,...,((p-1)/2)a$ nên

$$u_1...u_s v_1...v_t \equiv a^{(p-1)/2}\left[\frac{p-1}{2}\right]!(mod\ p).$$

Như vậy ta có:

$$(-1)^s\ a^{(p-1)/2}\left[\frac{p-1}{2}\right]! \equiv \left[\frac{p-1}{2}\right]!(mod\ p).$$

Vì $(p,((p-1)/2)!)=1$ nên suy ra:

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

tức là:

$$a^{(p-1)/2} \equiv (-1)^s(mod\ p)$$

Định lí suy ra từ tiêu chuẩn Euler.

Định lí 4.8. *Nếu p là một số nguyên tố lẻ thì*

$$\left[\frac{2}{p}\right]=(-1)^{(p^2-1)/8}$$

Như vậy, 2 là thặng dư bình phương của mọi số nguyên tố dạng $p \equiv \pm 1(mod\ 8)$*và là không thặng dư bình phương của mọi số nguyên tố dạng* $p \equiv \pm 3(mod\ 8)$.

Chứng minh. Áp dụng tiêu chuẩn Gauss, ta cần tính số thặng dư dương bé nhất lớn hơn $p/2$ của dãy số

$$1.2,2.2,...,((p-1)/2).2$$

Vì các số đều nhỏ hơn p nên các thặng dư dương bé nhất của mỗi số trùng với chính nó. Như vậy, ta chỉ cần tính số các số của dãy lớn hơn $p/2$. Số các số đó là $s=(p-1)/2-[p/4]$ (trong đó [ ] chỉ phần nguyên). Như vậy ta có:

$$\left[\frac{2}{p}\right]=(-1)^{(p-1)/2-[p/4]}.$$

Dễ kiểm tra đồng dư thức sau đây bằng cách phân ra các trường hợp $p \equiv 1,3,5,7(mod\ 8)$:

$$(p-1)/2-[p/4] \equiv (p^2-1)/8(mod\ 2)$$

Từ đó ta có:

$$\left[\frac{2}{p}\right] \equiv (-1)^{(p^2-1)/8}(mod\ 2).$$

Tính toán trực tiếp cho đẳng thức cần chứng minh.

§2. Luật thuận nghịch bình phương.

Định lí sau đây cho ta mối liên hệ giữa các kí hiệu Legendre $\left[\frac{p}{q}\right]$ và $\left[\frac{q}{p}\right]$. Định lí này thường được sử dụng khi tính toán với các kí hiệu Legendre.

Định lí 4.9. (Luật thuận nghịch bình phương). *Giả sử p và q là các số nguyên tố lẻ, khi đó ta có:*

$$\left[\frac{p}{q}\right]\left[\frac{q}{p}\right]=(-1)^{((p-1)/2).((q-1)/2)}.$$

Trước hết ta chứng minh bổ đề sau.

Bổ đề 4.10. *Giả sử p là một số nguyên tố lẻ, a là một số lẻ không chia hết cho p. Khi đó*

$$\left[\frac{a}{p}\right]=(-1)^{T(a,p)},$$

trong đó

$$T(a,p)=\sum_{j=1}^{(p-1)/2}[ja/p].$$

Chứng minh. Xét các thặng dư dương bé nhất của các số nguyên $a,2a,...,((p-1)/2)a$. Giả sử $u_1,...u_s,v_1,...v_t$ tương ứng là các thặng dư lớn hơn và bé hơn $p/2$. Ta có:

$$ja=p[ja/p]+\text{phần dư}$$

trong đó phần dư là một trong các số u_i hoặc v_j. Cộng từng vế $(p-1)/2$ phương trình, ta được:

$$\sum_{j=1}^{(p-1)/2}ja=\sum_{j=1}^{(p-1)/2}p[ja/p]+\sum_{j=1}^{s}u_j+\sum_{j=1}^{t}v_j$$

Như đã chứng tỏ trong chứng minh bổ đề Gauss, các số nguyên $p-u_1,..., p-u_s, v_1,...,v_t$ chính là tập hợp các số $1,...(p-1)/2$, xếp theo thứ tự nào đó.Vậy ta có:

$$\sum_{j=1}^{(p-1)/2}j=\sum_{j=1}^{s}(p-u_j)+\sum_{j=1}^{t}v_j=ps-\sum_{j=1}^{s}u_j+\sum_{j=1}^{t}v_j$$

Từ đó suy ra

$$\sum_{j=1}^{(p-1)/2}ja-\sum_{j=1}^{(p-1)/2}j=\sum_{j=1}^{(p-1)/2}p[ja/p]-ps+2\sum_{j=1}^{s}u_j$$

Từ công thức của $T(a,p)$, ta nhận được:

$$(a-1)\sum_{j=1}^{(p-1)/2} j = pT(a,p) - ps + 2\sum_{j=1}^{s} u_j \ .$$

Vì a, p lẻ nên

$$T(a,p) \equiv s (mod\ 2)$$

Bổ đề được chứng minh bằng cách áp dụng bổ đề Gauss.

Bây giờ ta chứng minh Luật thuận nghịch bình phương.

Xét các cặp số nguyên (x,y) với $1 \le x \le (p-1)/2$ và $1 \le y \le (q-1)/2$. Có tất cả $((p-1)/2)((q-1)/2)$ cặp như vậy. Ta sẽ chia các cặp đó thành hai nhóm tuỳ thuộc độ lớn của qx và py.

Trước tiên, dễ thấy rằng $qx \neq py$ đối với mọi cặp.

Để đánh số các cặp số nguyên (x,y) với $1 \le x \le (p-1)/2$, $1 \le y \le (q-1)/2$ và $qx > py$, ta chú ý rằng chúng chính là các cặp với $1 \le x \le (p-1)/2$, $1 \le y \le qx/p$. Với mỗi giá trị cố định của x, $1 \le x \le (p-1)/2$, tồn tại $[qx/p]$ số nguyên thoả mãn $1 \le y \le qx/p$. Như vậy số các cặp thoả mãn tính chất đang xét là $\sum_{j=1}^{(p-1)/2} [qj/p]$.

Tiếp theo, ta xét các cặp thoả mãn $1 \le x \le (p-1)/2$, $1 \le y \le (q-1)/2$ và $qx < py$. Lý luận tương tự như trên cho thấy, số các cặp là $\sum_{j=1}^{(q-1)/2} [pj/q]$.

Vì có tất cả là $((p-1)/2)((q-1)/2)$ cặp, ta nhận được đẳng thức sau

$$\sum_{j=1}^{(p-1)/2} [qj/p] + \sum_{j=1}^{(q-1)/2} [pj/q] = ((p-1)/2)((q-1)/2).$$

Từ định nghĩa của hàm T, ta có:

$$(-1)^{T(p,q)+T(q,p)} = (-1)^{((p-1)/2)((q-1)/2)}$$

Định lý được suy ra từ bổ đề 4.10

Nhận xét. Định lý trên đây (Luật thuận nghịch bình phương) thường được dùng để tính ký hiệu Legendre. Chẳng hạn, từ định lí có thể suy ra rằng, $\left[\frac{p}{q}\right]\left[\frac{q}{p}\right]$=-1 nếu $p \equiv q \equiv 3 (mod\ 4)$, và bằng 1 trong các trường hợp còn lại, tức là $\left[\frac{p}{q}\right] = \left[\frac{-q}{p}\right]$ nếu $p \equiv q \equiv 3 (mod\ 4)$, và $\left[\frac{p}{q}\right] = \left[\frac{q}{p}\right]$ trong các trường hợp có ít nhất một trong hai số p hoặc q đồng dư với 1 modulo 4.

Ta xét một ví dụ bằng số: tính $\left[\begin{matrix}713\\1009\end{matrix}\right]$.

$$\left[\begin{matrix}713\\1009\end{matrix}\right]=\left[\begin{matrix}23.31\\1009\end{matrix}\right]=\left[\begin{matrix}23\\1009\end{matrix}\right]\left[\begin{matrix}31\\1009\end{matrix}\right]$$

Vì $1009 \equiv 1 (mod\ 4)$ nên ta có:

$$\left[\begin{matrix}23\\1009\end{matrix}\right]=\left[\begin{matrix}1009\\23\end{matrix}\right],\left[\begin{matrix}31\\1009\end{matrix}\right]\left[\begin{matrix}1009\\31\end{matrix}\right]$$

Mặt khác,

$$\left[\begin{matrix}1009\\23\end{matrix}\right]=\left[\begin{matrix}20\\23\end{matrix}\right]=\left[\begin{matrix}2^2 5\\23\end{matrix}\right]=\left[\begin{matrix}2^2\\23\end{matrix}\right]\left[\begin{matrix}5\\23\end{matrix}\right]=\left[\begin{matrix}5\\23\end{matrix}\right]=\left[\begin{matrix}23\\5\end{matrix}\right]=\left[\begin{matrix}3\\5\end{matrix}\right]=\left[\begin{matrix}5\\3\end{matrix}\right]=\left[\begin{matrix}2\\3\end{matrix}\right]=-1$$

$$\left[\begin{matrix}1009\\31\end{matrix}\right]=\left[\begin{matrix}17\\31\end{matrix}\right]=\left[\begin{matrix}31\\17\end{matrix}\right]=\left[\begin{matrix}14\\17\end{matrix}\right]=\left[\begin{matrix}2\\17\end{matrix}\right]\left[\begin{matrix}7\\17\end{matrix}\right]=\left[\begin{matrix}7\\17\end{matrix}\right]=\left[\begin{matrix}17\\7\end{matrix}\right]=\left[\begin{matrix}3\\7\end{matrix}\right]=-\left[\begin{matrix}7\\3\end{matrix}\right]=-\left[\begin{matrix}4\\3\end{matrix}\right]$$

$$=-\left[\begin{matrix}2^2\\3\end{matrix}\right]=-1$$

Vậy, $\left[\begin{matrix}713\\1009\end{matrix}\right]=1$.

Luật thuận nghịch bình phương còn được dùng trong kiểm tra nguyên tố. Ta có định lí sau.

Định lí 4.11. (Kiểm tra Pepin). *Số Fermat F_m là số nguyên tố khi và chỉ khi*

$$3^{(F_m-1)/2} \equiv -1\ (mod\ F_m)$$

Chứng minh. Ta nhắc lại định nghĩa số Fermat: $F_m=2^{2^m}+1$.

Giả sử đồng dư phát biểu trong định lí được thoả mãn. Khi đó ta có

$$3^{F_m-1} \equiv 1\ (\text{mod}\ F_m)$$

Như vậy, nếu F_m có ước nguyên tố p thì

$$3^{F_m-1} \equiv 1\ (\text{mod}\ p)$$

Do đó, $ord_p 3$ phải là một ước của F_m-1, tức phải là một luỹ thừa của 2. Từ giả thiết suy ra $ord_p 3 \mid (F_m-1)/2=2^{2^m-1}$. Vậy ta có: $ord_p 3=F_m-1$. Từ đó suy ra $F_m-1 \le p-1$, nhưng vì p là ước của F_m, nên có nghĩa là $F_m=p$: F_m là số nguyên tố.

Ngược lại, giả sử F_m nguyên tố. Theo luật thuận nghịch bình phương, ta có:

$$\left[\frac{3}{F_m}\right] = \left[\frac{F_m}{3}\right] = \left[\frac{2}{3}\right] = -1$$

Mặt khác, theo tiêu chuẩn Euler ta có:

$$\left[\frac{3}{F_m}\right] \equiv 3^{(F_m-1)/2} \pmod{F_m}$$

Định lí đã được chứng minh.

Nhận xét. Dùng tiêu chuẩn Pepin, dễ kiểm tra được rằng F_1,F_2,F_3,F_4 là các số nguyên tố, F_5 là hợp số.

§3. Kí hiệu Jacobi.

Kí hiệu Jacobi là một mở rộng của kí hiệu Legendre, và được sử dụng để tính kí hiệu Legendre, cũng như trong nhiều vấn đề nghiên cứu các số giả nguyên tố.

Định nghĩa 4.12. Giả sử n là số nguyên dương lẻ, a nguyên tố cùng nhau với n. Nếu n có phân tích ra thừa số nguyên tố là $p_1^{t_1} p_2^{t_2} ... p_m^{t_m}$, ta định nghĩa *kí hiệu Jacobi* như sau:

$$\left[\frac{a}{n}\right] = \left[\frac{a}{p_1}\right]^{t_1}\left[\frac{a}{p_2}\right]^{t_2}\left[\frac{a}{p_m}\right]^{t_m},$$

trong đó ở vế phải là các kí hiệu Legendre.

Như vậy, trong trường hợp n là số nguyên tố thì kí hiệu Jacobi trùng với kí hiệu Legendre. Tuy nhiên cần chú ý rằng, khác với kí hiệu Legendre, khi n là hợp số, kí hiệu Jacobi không cho ta biết phương trình đồng dư $x^2 \equiv a \pmod{p}$ có nghiệm hay không. Mặc dầu vậy, kí hiệu Jacobi có nhiều tính chất tương tự với kí hiệu Legendre.

Định lí 4.13. *Giả sử n là số nguyên dương lẻ, a và b là các số nguyên tố cùng nhau với n. Khi đó:*

(i) Nếu $a \equiv b \pmod{n}$ *thì* $\left[\frac{a}{n}\right] = \left[\frac{b}{n}\right]$.

(ii) $\left[\frac{ab}{n}\right] = \left[\frac{a}{n}\right]\left[\frac{b}{n}\right]$

(iii) $\left[\frac{-1}{n}\right] = (-1)^{(n-1)/2}$

$(iv)\left[\frac{2}{n}\right]=(-1)^{(n^2-1)/8}$

Chứng minh. Hai đẳng thức đầu tiên dễ suy ra từ định nghĩa kí hiệu Jacobi và tính chất của kí hiệu Legendre.

Để chứng minh tính chất thứ 3, ta nhận xét rằng, do (p_i-1) chẵn nên

$$(1+(p_i-1))^{t1} \equiv 1+t_i(p_i-1)(mod\ 4),$$

$$(1+t_i(p_i-1))(1+t_j(p_j-1)) \equiv 1+t_i(p_i-1)+ t_j(p_j-1)(mod\ 4).$$

Từ đó suy ra:

$$n \equiv 1+t_1(p_1-1)+t_2(p_2-1)+...+ t_m(p_m-1)(mod\ 4),$$

tức là,

$$(n-1)/2 \equiv t_1(p_1-1)/2+t_2(p_2-1)/2+...+ t_m(p_m-1)/2(mod\ 2)$$

Hệ thức này cùng với định nghĩa cho ta đẳng thức (iii).

Chứng minh (iv). Ta có:

$$\left[\frac{2}{n}\right]=\left[\frac{2}{p_1}\right]^{t_1}\left[\frac{2}{p_2}\right]^{t_2}\cdots\left[\frac{2}{p_m}\right]^{t_m}=(-1)^{t_1(p_1^2-1)/8+t_2(p_2^2-1)/8+...+t_m(p_m^2-1)/8}$$

Lập luận tương tự như trong chứng minh phần trên,ta có:

$$n^2 \equiv 1+t_1(p_1^2-1)+t_2(p_2^2-1)+...+ t_m(p_m^2-1)(mod\ 64),$$

và khi đó (iv) suy ra từ định nghĩa.

Định lí 4.14. (Luật thuận nghịch bình phương đối với kí hiệu Jacobi). *Giả sử m, n là các số nguyên dương lẻ, nguyên tố cùng nhau. Khi đó:*

$$\left[\frac{n}{m}\right]\left[\frac{m}{n}\right]=(-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Chứng minh. Giả sử m, n có phân tích ra thừa số nguyên tố dạng: $m=p_1^{a_1}p_2^{a_2}...p_s^{a_s}$, $n=q_1^{b_1}q_2^{b_2}...q_r^{b_r}$. Dùng định nghĩa và luật thuận nghịch bình phương của kí hiệu Legendre, ta được:

$$\left[\frac{n}{m}\right]\left[\frac{m}{n}\right]=\prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{a_j\frac{p_j-1}{2}b_i\frac{q_i-1}{2}}=(-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}a_j\frac{p_j-1}{2}b_i\frac{q_i-1}{2}}.$$

Như trong chứng minh định lí 4.13, (iii), ta có:

$$\sum_{j=1}^{s} a_j \frac{p_j - 1}{2} \equiv \frac{m-1}{2} (\mathrm{mod}\, 2),$$

$$\sum_{i=1}^{r} b_i \frac{q_i - 1}{2} \equiv \frac{n-1}{2} (\mathrm{mod}\, 2).$$

Từ đó suy ra định lí.

§4. Thuật toán tính kí hiệu Jacobi.

Giả sử *a, b* là hai số nguyên dương nguyên tố cùng nhau, *a>b*. Đặt $R_1=a$, $R_2=b$. Dùng thuật chia Eulid và tách luỹ thừa cao nhất của 2 trong phần dư, ta được:

$$R_0 = R_1 q_1 + 2^{s_1} R_2$$

$$R_1 = R_2 q_2 + 2^{s_2} R_3$$

.....

$$R_{n-3} = R_{n-2} q_{n-2} + 2^{s_{n-2}} R_{n-1}$$

$$R_{n-2} = R_{n-1} q_{n-1} + 2^{s_{n-1}} .1$$

trong đó s_j là các số nguyên không âm, R_j là số nguyên lẻ bé hơn R_{j-1}.

Ta chú ý rằng, số các phép chia đòi hỏi trong thuật toán trên là không vượt quá số phép chia cần thiết khi dùng thuật toán Euclid để tìm ước chung lớn nhất của hai số *a* và *b*.

Đặt:

$$R(a,b) = s_1 \frac{R_1^{\,2} - 1}{8} + s_2 \frac{R_2^{\,2} - 1}{8} + \ldots + s_{n-1} \frac{R_{n-1}^{\,2} - 1}{8} + \frac{R_1 - 1}{2} . \frac{R_2 - 1}{2} + \ldots + \frac{R_{n-2} - 1}{2} . \frac{R_{n-1} - 1}{2}.$$

Ta có định lí sau.

Định lí 4.15. *Giả sử a,b là các số nguyên dương và a>b. Khi đó ta có:*

$$\left[\frac{a}{b}\right] = (-1)^{R(a,b)}$$

Chứng minh. Theo các phần *(i), (ii)*, và *(iv)* của định lí 4.13 ta có:

$$\left[\frac{a}{b}\right] = \left[\frac{R_0}{R_1}\right] = \left[\frac{2^{s_1} R_2}{R_1}\right] = \left[\frac{2}{R_1}\right]^{s_1} \left[\frac{R_2}{R_1}\right] = (-1)^{s_1 \frac{R_1^{\,2}-1}{8}} \left[\frac{R_2}{R_1}\right].$$

Dùng luật thuận nghịch bình phương của kí hiệu Jacobita được:

$$\begin{bmatrix} R_2 \\ R_1 \end{bmatrix} = (-1)^{\frac{R_1-1}{2}\frac{R_2-1}{2}} \begin{bmatrix} R_1 \\ R_2 \end{bmatrix}.$$

Như vậy,

$$\begin{bmatrix} a \\ b \end{bmatrix} = (-1)^{\frac{R_1-1}{2}\frac{R_2-1}{2}+s_1\frac{R_1^2-1}{8}} \begin{bmatrix} R_1 \\ R_2 \end{bmatrix}$$

Tiếp tục quá trình đó, ta đi đến công thức cần chứng minh.

Hệ quả 4.16. *Giả sử a và b là các số nguyên dương nguyên tố cùng nhau, a>b. Khi đó, kí hiệu Jacobi* $\begin{bmatrix} a \\ b \end{bmatrix}$ *có thể tính được với* $O((\log_2 b)^3)$ *phép tính bit.*

Chứng minh. Như ta đã nhận xét, số các phép chia trong thuật toán xác định *R(a,b)* không vượt quá số phép chia trong thuật toán Euclid để tính ước chung lớn nhất của *a* và *b*. Theo định lí Lamé, cần có $O(\log_2 b)$ phép chia. Mỗi phép chia cần không quá $O((\log_2 b)^2)$ phép tính bit. Sau mỗi phép chia, cặp số R_j, s_j tìm được bởi $O(\log_2 b)$ phép tính bit (chỉ cần là các phép dịch chuyển). Như vậy, khi biết *a, b,* chỉ cần $O((\log_2 b)^3)$ phép tính bit để xác định các số R_j, s_j. Để nâng (-1) lên luỹ thừa *R(a,b)* như trong định lí, ta chỉ cần sử dụng 3 chữ số nhị phân cuối cùng của R_j và chữ số nhị phân cuối cùng của s_j, vì giá trị luỹ thừa của (-1) chỉ phụ thuộc vào tính chẵn lẻ của số mũ. Như vậy, khi đã có R_j, s_j, ta chỉ cần $O(\log_2 b)$ để xác định $\begin{bmatrix} a \\ b \end{bmatrix}$. Hệ quả được chứng minh.

Ta có thuật toán sau đây để tính kí hiệu Jacobi dựa vào các định lí vừa chứng minh.

Thuật toán tính kí hiệu Jacobi $\begin{bmatrix} a \\ b \end{bmatrix}$ (và do đó, tính kí hiệu Legendre khi *b* là số nguyên tố).

J1. (Kiểm tra b≠0). Nếu b=0, in ra 0 nếu |a|≠1, in ra 1 nếu |a|=1 và kết thúc thuật toán.

J2. (Tách các luỹ thừa của 2 khỏi *b*). Nếu *a* và *b* đều chẵn, in ra 0 và kết thúc thuật toán. Ngược lại, đặt v←0, và khi *b* chẵn, đặt v←v+1, b←b/2. Sau đó, nếu *v* chẵn, đặt k←1, ngược lại, đặt k←$(-1)^{(a^2-1)/8}$. Cuối cùng, nếu b<0, đặt b←-b, và nếu hơn nữa, a<0, đặt k←-k.

J3. (Kết thúc?). (ở bước này, ta có *b* lẻ và b>0). Nếu a=0, in ra 0 nếu b>1, in ra *k* nếu b=1 và kết thuật toán. Ngược lại, đặt v←0 và nếu *a* chẵn, đặt v←v+1, a←a/2. Nếu *v* lẻ, đặt k← $(-1)^{(b^2-1)/8}k$.

J4. (Sử dụng luật thuận nghịch). Đặt k←$(-1)^{(a-1)(b-1)/4}$k.

Nhận xét. Ở đây, ta cần lưu ý một điều. Mặc dù trong thuật toán có xuất hiện các phép chia $(a^2-1)/8$, $(b^2-1)/8$, $(a-1)(b-1)/4$, và phép nâng (-1) lên luỹ thừa đó, ta không cần làm các phép chia cũng như nâng lên luỹ thừa, vì đòi hỏi quá nhiều phép tính bit. Vì giá trị luỹ thừa của $(-1)_2$ chỉ phụ thuộc vào tính chẵn lẻ của các đại lượng trên, nên chẳng hạn đối với $(-1)^{(a^2-1)/8}$, giá trị đó chỉ phụ thuộc a mod 8 và bằng một trong những số của dãy sau đây:

$$\{0,1,0,-1,0,-1,0,1\}.$$

Thuật toán tính căn bậc 2 modulo p.

Trong nhiều ứng dụng (chẳng hạn, xem Chương 7), ta cần phải tính căn bậc 2 modulo p, khi biết nó tồn tại. Tất nhiên, một trong các phương pháp để giải phương trình đồng dư $x^2 \equiv a(mod\ p)$, $(a,p)=1$ là kiểm tra tất cả các số từ 1 đến $p-1$. Tuy nhiên, khi làm việc với p lớn, phương pháp này không thể áp dụng được (thời gian đòi hỏi là $O(p)$).

Với những số nguyên tố dạng $p \equiv 3(mod\ 4)$, bài toán khá đơn giản. Ta có:

$$x \equiv a^{(p+1)/4}(mod\ p).$$

Thật vậy,

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

Khi $p \not\equiv 3(mod\ 4)$, ta có $p \equiv 1(mod\ 8)$ hoặc $p \equiv 5(mod\ 8)$. Trong trường hợp $p \equiv 5(mod\ 8)$, lời giải cũng có thể tìm được không khó khăn. Thật vậy, ta có:

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

do đó

$$a^{(p-1)/4} \equiv \pm 1(\text{mod p}).$$

Dễ kiểm tra được rằng, trong trường hợp đồng dư thoả mãn với dấu cộng, nghiệm phải tìm là

$$x=a^{(p+3)/8}(\text{mod p}).$$

Nếu đồng dư thoả mãn với dấu trừ, dùng định lí 4.8 ta có:

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

Từ đó nghiệm phải tìm là:

$$x=2a.(4a)^{(p-5)/8}(\text{mod p}).$$

Như vậy chỉ còn phải xét trường hợp $p \equiv 1(mod\ 8)$. Cho đến nay, mới chỉ có một thuật toán (thuật toán Shoof sử dụng đường cong elliptic) với thời gian đa thức. Tuy nhiên, trong thực tế, thuật toán đó rất khó sử dụng. Sau đây chúng ta tìm hiểu thuật toán xác suất của Tonelli và Shanks.

Thuật toán Tonelli-Shanks chính là một mở rộng tự nhiên của các trường hợp riêng đã xét trên đây.

Ta luôn luôn viết $p-1=2^e.q$, với q lẻ.

Nếu ta tìm được phần tử z và số nguyên chẵn k sao cho

$$a^q z^k \equiv 1 (\text{mod } p)$$

thì nghiệm cần tìm sẽ được cho bởi

$$x=a^{(q+1)/2} z^{k/2}.$$

Ta sẽ tìm phần tử z dưới dạng $z=n^q$.

Ta chỉ ra rằng, phần tử z như vậy thoả mãn điều kiện đặt ra khi và chỉ khi n là một không thặng dư bình phương modulo p. Ta có:

$$(a^q)^{2^e} = a^{\phi(p-1)} \equiv 1 (\text{mod } p),$$

do đó a^q thuộc vào nhóm G các phần tử cấp là một ước số của 2^e. Như vậy, để tồn tại k, chỉ cần chọn n là phần tử sinh của nhóm G (khi đó, do a là một không thặng dư bình phương nên số mũ k phải là chẵn). Số nguyên n sẽ là một phần tử sinh của G khi và chỉ khi $n, n^2, n^4,...,n^{2^e}$ ($\equiv 1 (mod\ p)$) không đồng dư với nhau modulo p. Dễ thấy rằng, điều đó xảy ra khi và chỉ khi n là một không thặng dư bình phương modulo p.

Để xây dựng thuật toán, ta cần giải quyết hai vấn đề: Tìm phần tử z, và tìm số mũ k.

Phần thứ nhất được giải quyết bằng thuật toán xác suất. Ta chọn ngẫu nhiên một số n, và tính kí hiệu Legendre $\left[\frac{n}{p}\right]$. Khi đó, nếu $\left[\frac{n}{p}\right]=-1$, ta đặt $z=n^q$. Trong trường hợp ngược lại, ta tiếp tục làm như trên với một số ngẫu nhiên khác cho đến khi tìm được một số n thích hợp. Vì số các thặng dư bình phương bằng $(p-1)/2$ nên mỗi lần chọn ngẫu nhiên một số n, xác suất để có $\left[\frac{n}{p}\right]=-1$ là 1/2.

Trong thực tế, ta có thể tìm ra một không thặng dư bình phương rất nhanh. Chẳng hạn, xác suất hai mươi lần thất bại liên tiếp nhỏ hơn 10^{-6}.

Số mũ k khó tìm hơn. Thật ra, ta không cần biết số mũ k, mà cần biết $a^{(q+1)/2} z^{k/2}$.

Thuật toán. Giả sử p là một số nguyên tố lẻ, $n \in Z$. Ta viết $p-1=2^e.q$ với q lẻ.

1. (Tìm phần tử sinh). Chọn ngẫu nhiên số n cho đến khi thoả mãn $\left[\frac{n}{p}\right]=-1$. Sau đó đặt $z \leftarrow n^q (mod\ p)$.

2. (Xuất phát). Đặt $y \leftarrow z$, $r \leftarrow e$, $x \leftarrow a^{(p-1)/2} (mod\ p)$, $b \leftarrow ax^2 (mod\ p)$, $x \leftarrow ax (mod\ p)$.

3. (Tìm số mũ). Nếu $b \equiv 1 (mod\ p)$ in ra x và kết thúc thuật toán, Trong trường hợp ngược lại, tìm số m nhỏ nhất sao cho $m \geq 1$, $b^{2^m} \equiv 1 (mod\ p)$. Nếu $m=r$, in ra thông

báo nói rằng a không phải là thặng dư bình phương modulo p.

4. (Thu hẹp số mũ). Đặt $t \leftarrow y^{2^{r-m-1}}$, $y \leftarrow t^2$, $r \leftarrow m$, $x \leftarrow xt$, $b \leftarrow by$ (mọi phép tính đều modulo p)và chuyển sang bước 3.

Chú ý rằng từ khi bắt đầu bước 3, ta luôn luôn có các đồng dư modulo p:

$$ax \equiv x^2,\ y^{2^{r-1}} \equiv -1,\ b^{2^{r-1}} \equiv 1.$$

Từ đó suy ra rằng, nếu nhóm con G_r các phần tử cấp là một ước của 2^r, thì y là phần tử sinh của nhóm G_r, $b \in G_{r-1}$, tức là b chính phương trong G_r. Vì r thực sự giảm tại mỗi bước lặp của thuật toán, nên số bước lặp nhiều nhất bằng e. Khi $r \leq 1$, ta có $b=1$, thuật toán kết thúc, và x là một căn bậc 2 của a mod p.

Có thể thấy rằng, trung bình, bước 3 và bước 4 đòi hỏi $e^2/4$ phép nhân modulo p, và nhiều nhất là e^2 phép nhân. Như vậy, thời gian chạy thuật toán là $O(\log^4 p)$.

§5. Số giả nguyên tố Euler.

Giả sử p là số nguyên tố lẻ và b là số nguyên không chia hết cho p. Khi đó theo tiêu chuẩn Euler ta có:

$$b^{(p-1)/2} \equiv \left[\frac{b}{p}\right] (\text{mod } p).$$

Như vậy, để kiểm tra một số n có phải là nguyên tố hay không, ta có thể lấy một số b nguyên tố cùng nhau với n, và kiểm tra xem đồng dư sau đây có đúng hay không:

$$b^{(n-1)/2} \equiv \left[\frac{b}{n}\right] (\text{mod } n),$$

trong đó, vế bên phải là kí hiệu Jacobi. Nếu đồng dư thức đó không đúng thì n phải là hợp số. Nếu đồng dư thức trên đây nghiệm đúng, vẫn chưa kết luận được n có phải là nguyên tố hay không, nhưng "có nhiều khả năng" n là số nguyên tố.

Định nghĩa 4.18. Số nguyên dương n được gọi là *số giả nguyên tố Euler cơ sở b* nếu nó là một hợp số và đồng dư thức sau đây nghiệm đúng:

$$b^{(n-1)/2} \equiv \left[\frac{b}{n}\right] (\text{mod } n)$$

Ta có mối liên hệ giữa số giả nguyên tố Euler cơ sở b và số giả nguyên tố cơ sở b đã xét trong chương 2.

Định lí 4.19. *Mọi số giả nguyên tố Euler cơ sở b đều là số giả nguyên tố cơ sở b.*

Chứng minh. Chỉ cần bình phương hai vế của đồng dư thức thoả mãn bởi các số giả nguyên tố Euler.

Điều ngược lại không đúng. Chẳng hạn, có thể thấy rằng số 431 là số giả nguyên tố cơ sở 2, nhưng không là số giả nguyên tố Euler cơ sở 2.

Định lí 4.20. *Mọi số giả nguyên tố mạnh cơ sở b đều là số giả nguyên tố Euler cơ sở b.*

Chứng minh. Cho n là số giả nguyên tố mạnh cơ sở b. Khi đó, nếu $n-1=2^s t$, trong đó t lẻ, thì, hoặc $b^t \equiv 1 \pmod n$, hoặc $b^{2^r t} \equiv -1 \pmod n$, với r nào đó $0 \le r \le s-1$. Giả sử $\prod_{j=1}^{m} p_j^{a_j}$ là phân tích của n thành thừa số nguyên tố. Ta xét riêng hai trường hợp.

Thứ nhất, $b^t \equiv 1 \pmod n$. Giả sử p là một ước nguyên tố của n. Khi đó $ord_p b \mid t$, và do đó $ord_p b$ là số lẻ. Mặt khác, $ord_p b$ là ước của $\phi(p)=p-1$, nên nó phải là ước của $(p-1)/2$. Vậy ta có

$$b^{(p-1)/2} \equiv 1 \pmod p$$

Theo tiêu chuẩn Euler, $\left[\frac{b}{p}\right]=1$, và do đó, $\left[\frac{b}{n}\right]=1$. Mặt khác ta có: $b^{(n-1)/2}=(b^t)^{2^s-1} \equiv 1 \pmod p$. Vậy n là số giả nguyên tố Euler cơ sở b.

Trường hợp thứ hai: $b^{2^r t} \equiv -1 \pmod n$. Nếu p là một ước nguyên tố của n thì $b^{2^r t} \equiv -1 \pmod n$.

Bình phương cả hai vế của dồng dư thức này ta được

$$b^{2^{r+1} t} \equiv 1 \pmod p.$$

Từ đó suy ra $ord_p b \mid 2^{r+1} t$, nhưng $ord_p b$ không là ước của $2^r t$. Như vậy, $ord_p b = 2^{r+1} c$, trong đó c là một số nguyên lẻ. Mặt khác, vì $ord_p b \mid (p-1)$, $2^{r+1} \mid ord_p b$, nên $2^{r+1} \mid (p-1)$.

Như vậy, ta có: $p=2^{r+1}d+1$, trong đó d là số nguyên. Vì

$$b^{(ord_p b)/2} \equiv -1 \pmod p$$

nên ta có:

$$\left[\frac{b}{p}\right] \equiv b^{(p-1)/2} = b^{(ord_p b/2)((p-1)/ord_p b)} \equiv (-1)^{(p-1)/ord_p b} = (-1)^{(p-1)/2^{r+1} c} \pmod p$$

Vì c lẻ nên từ đó suy ra $\left[\frac{b}{p}\right]=(-1)^d$.

Bây giờ giả sử n có phân tích thành thừa số nguyên tố dạng:

$$n=\prod_{j=1}^{m} p_j^{\,a_j} .$$

Theo chứng minh phần trên, các ước nguyên tố p_i có dạng $p_i=2^{r+1}d_i+1$, và ta có:

$$\left[\frac{b}{n}\right]=\prod_{i=1}^{m}\left[\frac{b}{p_i}\right]_i^a=(-1)^{\sum_{i=1}^{m} a_i d_i} .$$

Mặt khác, dễ thấy rằng,

$$n\equiv 1+2^{r+1}\sum_{i=1}^{m} a_i d_i \pmod{2^{2r+2}}.$$

Do đó

$$t2^{s-1}=(n-1)/2\equiv 2^r\sum_{i=1}^{m} a_i d_i \pmod{2^{r+1}},$$

tức là

$$t2^{s-1-r}\equiv \sum_{i=1}^{m} a_i d_i \pmod 2$$

và

$$b^{(n-1)/2}=(b^{2^r t})^{2^{s-1-r}}\equiv(-1)^{2^{s-1-r}}=(-1)^{\sum_{i=1}^{m} a_i d_i} \pmod n$$

Như vậy,

$$b^{(n-1)/2}\equiv\left[\frac{b}{n}\right]\pmod n,$$

và n là số giả nguyên tố Euler cơ sở b.

Chú ý rằng, điều ngược lại không phải luôn luôn đúng: tồn tại những số giả nguyên tố Euler cơ sở b không là giả nguyên tố mạnh cơ sở đó. Ví dụ n=1105, b=2.

Tuy nhiên, với những điều kiện bổ sung, một số giả nguyên tố Euler sẽ là giả nguyên tố mạnh cùng cơ sở. Ta có định lí sau.

Định lí 4. 21. *Số n giả nguyên tố Euler cơ sở b là số giả nguyên tố mạnh cơ sở b nếu* $n\equiv 3 \pmod 4$, *hoặc* $\left[\frac{b}{n}\right]=-1$.

Chứng minh. Trường hợp thứ nhất: $n\equiv 3 \pmod 4$. Khi đó $n-1=2.t$ và t lẻ. Vì n là số giả nguyên tố Euler cơ sở b nên

$$b^t = b^{(n-1)/2} \equiv \left[\frac{b}{n}\right] (\text{mod } n).$$

Như vậy, n là số giả nguyên tố mạnh cơ sở b.

Trong trường hợp thứ hai, ta viết $n-1=2^s t$, trong đó t lẻ, s là số nguyên dương. Vì n là số giả nguyên tố mạnh cơ sở b nên

$$b^{2^{s-1}t} = b^{(n-1)/2} \equiv \left[\frac{b}{n}\right] (\text{mod } n).$$

Theo giả thiết ta có:

$$b^{t2^{s-1}} \equiv -1 (\text{mod } n).$$

Như vậy n là số giả nguyên tố mạnh cơ sở b.

Dùng số giả nguyên tố Euler, ta có thể xây dựng thuật toán xác suất để kiểm tra một số là nguyên tố hay không. Thuật toán này được Solovay và Strassen tìm ra đầu tiên năm 1977 ([S-S]).

Ta bắt đầu bằng bổ đề sau.

Bổ đề 4.22. *Giả sử n là một số nguyên dương lẻ không chính phương. Khi đó tồn tại ít nhất một số b với 1<b<n, (b,n)=1, sao cho* $\left[\frac{b}{n}\right] = -1$.

Chứng minh. Nếu n là nguyên tố, số b tồn tại theo định lí 4.3. Khi n là hợp số không chính phương, ta viết $n=rs$, trong đó $(r,s)=1$ và $r=p^e$, với p là một số nguyên tố lẻ và e số nguyên dương lẻ. Bây giờ giả sử t là một không thặng dư bình phương của số nguyên tố p. Ta dùng định lí Trung Quốc về phần dư để tìm số nguyên b sao cho $1<b<n$, $(b,n)=1$ và

$$b \equiv t (\text{mod } r)$$

$$b \equiv 1 (\text{mod } s)$$

Khi đó ta có $\left[\frac{b}{r}\right] = \left[\frac{b}{p^e}\right] = (-1)^e = -1, \left[\frac{b}{s}\right] = 1$, tức là $\left[\frac{b}{n}\right] = -1$.

Bổ đề 4.23. *Với mỗi hợp số lẻ n, tồn tại ít nhất một số b sao cho 1<b<n, (b,n)=1 và*

$$b^{(n-1)/2} \not\equiv \left[\frac{b}{n}\right] (mod\ n). \qquad (3.1)$$

Giả sử ngược lại, với mọi số nguyên không vượt quá n và nguyên tố cùng nhau với n, ta có

$$b^{(n-1)/2} \equiv \left[\frac{b}{n}\right] (\text{mod } n).$$

Từ đó suy ra, nếu *(b,n)=1* thì

$$b^{(n-1)} \equiv 1(\text{mod } n).$$

Như vậy, *n* phải là số Carmicheal, và do đó, $n=q_1q_2...q_r$ là tích của các số nguyên tố lẻ khác nhau. Ta sẽ chỉ ra rằng

$$b^{(n-1)/2} \equiv 1(\text{mod } n).$$

đối với mọi số nguyên *b* không vượt quá *n* và nguyên tố cùng nhau với *n*.

Giả sử ngược lại, tồn tại *b* thoả mãn

$$b^{(n-1)/2} \equiv -1(\text{mod } n).$$

Dùng định lí Trung Quốc về phần dư, ta tìm được số *a, 1<a<n, (a,n)=1* sao cho

$$a \equiv b(\text{mod } q_1)$$

$$a \equiv 1(\text{mod } q_2q_3...q_r)$$

Như vậy

$$a^{(n-1)/2} \equiv b^{(n-1)/2} \equiv -1(\text{mod } q_1)$$

$$a^{(n-1)/2} \equiv 1(\text{mod } q_2q_3...q_r)$$

Do đó

$$a^{(n-1)/2} \not\equiv \pm 1(\text{mod } n),$$

trái với giả thiết phản chứng (3.1).

Như vậy, với mọi *b, 1<b<n, (b,n)=1* ta có:

$$b^{(n-1)/2} \equiv 1(\text{mod } n).$$

Từ đồng dư trên và (3.1) ta có:

$$b^{(n-1)/2} \equiv \left[\frac{b}{n}\right] \equiv 1(\text{mod } n),$$

mâu thuẫn với bổ đề 4.22. Bổ đề 4.23 được chứng minh.

Định lí trên đây được dùng làm cơ sở cho một thuật toán kiểm tra nguyên tố xác suất. Ta có định lí sau.

Định lí 4.24. *Đối với mỗi hợp số lẻ n, tồn tại không quá $\phi(n)/2$ số nguyên dương b nhỏ hơn n, nguyên tố cùng nhau với n, sao cho n là số giả nguyên tố mạnh Euler cơ sở b.*

Chứng minh. Theo bổ đề 4.23., tồn tại số *b, 1<b<n, (b,n)=1* sao cho

$$b^{(n-1)/2} \not\equiv \left[\frac{b}{n}\right] (\text{mod } n).$$

Giả sử $a_1,a_2,...,a_m$ là các số thoả mãn $1 \le a_j<n$, $(a_j,n)=1$ và

$$a_j^{(n-1)/2} \equiv \left[\frac{a_j}{n}\right] = 1 (\text{mod } n)$$

Giả sử $r_1,r_2,...,r_m$ là thặng dư dương bé nhất của các số $ba_1,ba_2,...,ba_m$. Các số r_j khác nhau và nguyên tố cùng nhau với n. Ta sẽ chứng tỏ rằng chúng không thoả mãn đồng dư thức như đối với các số a_j. Thật vậy, nếu ngược lại

$$r_j^{(n-1)/2} \equiv \left[\frac{r_j}{n}\right] = 1 (\text{mod } n)$$

thì ta có:

$$ba_j^{(n-1)/2} \equiv \left[\frac{ba_j}{n}\right] = 1 (\text{mod } n)$$

và như vậy:

$$b^{(n-1)/2} a_j^{(n-1)/2} \equiv \left[\frac{b}{n}\right]\left[\frac{a_j}{n}\right]$$

Từ đó suy ra:

$$b^{(n-1)/2} \equiv \left[\frac{b}{n}\right] (\text{mod } n),$$

mâu thuẫn với tính chất của b.

Như vậy, tập hợp các số a_j và r_j không giao nhau. Gộp cả hai tập hợp này, ta được $2m$ số khác nhau, bé hơn n và nguyên tố cùng nhau với n. Từ đó suy ra $m<\phi(n)/2$, định lí được chứng minh.

Nhận xét. Từ định lí trên, ta thấy rằng, nếu n là một hợp số lẻ, b là số chọn ngẫu nhiên trong các số $1,2,...,n-1$, thì xác suất để n là giả nguyên tố Euler có sở b sẽ bé hơn 1/2. Ta có định lí sau.

Định lí 4.25. (Thuật toán kiểm tra nguyên tố xác suất Solovay-Strassen). *Cho n là một số nguyên dương. Ta chọn ngẫu nhiên k số $b_1,b_2,...,b_k$ từ các số $1,2,...,n-1$. Đối với mỗi số nguyên b_j, xét đồng dư thức*

$$b_j^{(n-1)/2} \equiv \left[\frac{b_j}{n}\right] (\mathrm{mod}\, n)$$

-Nếu một trong các đồng dư thức đó không nghiệm đúng thì n là hợp số.

-Nếu n là nguyên tố thì mọi đồng dư thức đều nghiệm đúng.

-Nếu n là hợp số, thì xác suất để mọi đồng dư thức nghiệm đúng là bé hơn $1/2^k$.

Như vậy, nếu k đủ lớn, và n trải qua được kiểm tra xác suất trên đây, thì "hầu như chắc chắn" n là số nguyên tố.

Nhận xét. 1) Vì mọi số giả nguyên tố mạnh cơ sở *b* đều là số giả nguyên tố Euler cơ sở *b*, nên số các hợp số *n* trải qua được kiểm tra xác suất Solovay-Strassen lớn hơn số các hợp số trải qua được kiểm tra Rabin. Cả hai thuật toán kiểm tra này đều cần $O(k(log_2 n)^3)$ phép tính bit.

2) Chẳng hạn, nếu *n* là số trải qua kiểm tra xác suất Solovay-Strassen với *k=40*. Khi đó *n* là hợp số với xác suất nhỏ hơn 2^{-40} tương đương 10^{-12}, bé hơn xác suất để phần cứng máy tính mắc một sai lầm!

Bài tập và tính toán thực hành chương 4

I. Bài tập

4.1. Tìm tất cả các số tự nhiên *b* sao cho 15 và 21 là các số giả nguyên tố cơ sở b.

4.2. Chứng minh rằng tồn tại 36 cơ sở *b* (modulo 91) để 91 là số giả nguyên tố cơ sở *b*.

4.3. Giả sử *p* và *2p-1* đều là số nguyên tố. Chứng minh rằng *n=p(2p-1)* là số giả nguyên tố đối với một nửa số cơ sở *b*.

4.4. Chứng minh rằng tồn tại vô hạn số nguyên tố dạng *4k+1*.

4.5. Chứng minh rằng tồn tại vô hạn số nguyên tố có các dạng sau đây: a) *8k+3, b)8k+5, c) 8k+7*.

4.6. Chứng minh rằng nếu *p* là một số nguyên tố dạng *4k+3* và *q=2p+1* cũng là số nguyên tố, thì $q|M_p=2^p-1$.

4.7. Chứng minh rằng $23|M_{11}$, $47|M_{23}$,$503|M_{251}$.

4.8. Chứng minh rằng 1105 là số giả nguyên tố Euler cơ sở 2 và không giả nguyên tố mạnh cơ sở 2.

4.9. Chứng minh rằng 15841 là: a) số giả nguyên tố mạnh cơ sở 2; b) số giả nguyên tố Euler cơ sở 2; c) số Carmichael.

4.10. Chứng minh rằng nếu *n* là số giả nguyên tố mạnh Euler cơ sở *a* và *b* thì *n* cũng là số giả nguyên tố mạnh Euler cơ sở *ab*.

4.11. Chứng minh rằng nếu *n* là số giả nguyên tố Euler cơ sở 2, và nếu $n \equiv 5 (mod\ 8)$ thì *n* là số giả nguyên tố mạnh cơ sở 2.

4.12. Chứng minh rằng nếu *n* là số giả nguyên tố Euler cơ sở *b* thì *n* cũng là số giả nguyên tố Euler cơ sở *n-b*.

4.13. Chứng minh rằng nếu *n* là số giả nguyên tố Euler cơ sở 3 và $n \equiv 5 (mod\ 12)$ thì *n* là số giả nguyên tố mạnh cơ sở 3.

II. Thực hành trên máy tính

II. 1. Thực hành kiểm tra một số là thặng dư bình phương

Cho *a, b* là các số nguyên. để kiểm tra xem *a* có phải là thặng dư bình phương của *b* hay không ta thực hiện dòng lệnh như sau:

```
[>quadres(a, b);
```

Sau dấu (;) ấn phím "Enter". Nếu trên màn hình hiện lên số 1 thì *a* là thặng dư bình phương của *b*, nếu trên màn hình hiện lên số -1 thì không phải.

Thí dụ: 74 có phải là thặng dư bình phương của 101 hay không?

Ta thực hiện lệnh

```
[>quadres(74,101);
```

```
                                -1
```

74 không phải là thặng dư bình phương của 101

II. 2. Thực hành tính ký hiệu Legendre

Cho *a* là số nguyên, *p* là số nguyên tố. Để tính kí hiệu Legendre của *a* và *p* ta thực hiện lệnh như sau:

```
[legendre(a,p);
```

Sau dấu (;) ấn phím "Enter" trên màn hình sẽ xuất hiện kết quả.

Thí dụ: Tính $\begin{bmatrix} 9 \\ 11 \end{bmatrix}$.

Ta thực hiện lệnh

```
[legendre(9,11);
```

```
                                1
```

Chú ý: Khi thực hiện lệnh tính lí hiệu Legendre, máy tính sẽ cho kết quả là 0, 1, hoặc -1. Nếu kết quả là 0 thì *a* chia hết cho *p*. Nếu kết quả là 1 thì *a* là thặng dư bình phương của *p*. Nếu kết quả là -1 thì *a* không là thặng dư của *p*. Do đó ta cũng có thể dùng dòng lệnh trên để kiểm tra thặng dư bình phương.

II. 3. Tính kí hiệu Jacobi

Cho *b* là số nguyên dương lẻ, *a* nguyên tố cùng nhau với *b*. Để tính kí hiệu Jacobi của *a* và *b* ta thực hiện dòng lệnh như sau:

```
[jacobi(a, b);
```

Sau dấu (;) ấn phím "Enter" trên màn hình sẽ xuất hiện kết quả.

Thí dụ: Tính $\begin{bmatrix} 26 \\ 35 \end{bmatrix}$

Ta thực hiện lệnh:

```
[> jacobi(26,35);
```

```
                                -1
```

Thí dụ: Tính $\begin{bmatrix} 28 \\ 21 \end{bmatrix}$

Ta thực hiện lệnh:

```
[> jacobi(28,21);
                                    0
```

Nếu kết quả là 0 thì a và b không nguyên tố cùng nhau.

II. 4. Tìm căn bậc 2 modulo một số

Cho x, n là các số nguyên. Để tìm căn bậc 2 của x modulo n ta thực hiện dòng lệnh như sau:

```
[>msqrt(x,n);
```

Sau dấu (;) ấn phím "Enter" trên màn hình sẽ xuất hiện kết quả. Nếu căn không tồn tại trên màn hình sẽ xuất hiện chữ "FAIL".

Thí dụ: Tính căn bậc 2 của 3 modulo 11.

Ta thực hiện như sau:

```
[>msqrt(3,11);
                                    5
```

Thí dụ: Tính căn bậc 2 của 3 modulo 7.

Ta thực hiện như sau:

```
[>msqrt(3,7);
                                  FAIl
```

II. 5. Thực hành kiểm tra số giả nguyên tố Euler

Để kiểm tra số nguyên dương n cho trước có phải là số giả nguyên tố Euler cơ sở b hay không ta thực hiện theo các bước sau:

Bước 1: Kiểm tra tính nguyên tố của n, ta thực hiện bằng dònglệnh

```
[>isprime(n);
```

Sau dấu (;) ấn phím "Enter". Nếu trên màn hình xuất hiện chữ "true" thì n là số nguyên tố, khi đó ta khẳng định n không phải là số giả nguyên tố Euler cơ sở b. Nếu trên màn hình xuất hiện chữ "false" ta tiếp tục thực hiện bước 2.

Bước 2: Tính kí hiệu Jacobi $J:=\left[\frac{b}{n}\right]$ của n và b, thực hiện bằng dòng lệnh

```
[> J:= jacobi(b,n);
```

Sau dấu (;) ấn phím "Enter".

Bước 3: Kiểm tra đồng dư thức $b^{(n-1)/2} \equiv J(\text{mod } n)$, thực hiện bằng dòng lệnh

```
[>b^((n-1)/2)-J mod n;
```

Sau dấu (;) ấn phím "Enter". Nếu trên màn hình xuất hiện số 0 thì *n* là số giả nguyên tố Euler cơ sở *b*.

Thí dụ: Số 1105 có phải là số giả nguyên tố Euler cơ sở 2 hay không?

Ta thực hiện lệnh như sau:

```
[> isprime(1105);
                                  false
[> J:=J(1105,2);
                                    1
[> 2^((1105-1)/2)-J mod 1105;
                                    0
```

Vậy 1105 là số giả nguyên tố Euler cơ sở 2.