Chương 3

CÁC HÀM SỐ HỌC

Khi nghiên cứu các số nguyên, ta thường làm việc với các đại lượng như: số các ước của một số nguyên tố cho trước, tổng các ước của nó, tổng các luỹ thừa bậc k của các ước,... Ngoài những ví dụ đó còn có rất nhiều hàm số học quan trọng khác. Trong chương này, ta chỉ xét sơ qua một vài hàm quan trọng. Phần lớn của chương được giành cho hàm Euler, là một trong những hàm số học quan trọng nhất.

§1. Định nghĩa.

Định nghĩa 3.1. *Hàm số học* tức là hàm xác định trên tập hợp các số nguyên dương.

Định nghĩa 3.2. Một hàm số học f được gọi là *nhân tính* nếu với mọi n, m nguyên tố cùng nhau, ta có $f(mn)=f(m)f(n)$. Trong trường hợp đẳng thức đúng với mọi m,n (không nhất thiết nguyên tố cùng nhau), hàm f được gọi là *nhân tính mạnh*.

Những ví dụ đơn giản nhất về hàm nhân tính (mạnh) là: $f(n)=n$ và $f(n)=1$.

Dễ chứng minh tính chất sau đây: nếu f là một hàm nhân tính, n là số nguyên dương có khai triển thành thừa số nguyên tố dạng $n=p_1^{a1}p_2^{a2}...p_k^{ak}$, thì $f(n)$ được tính theo công thức

$$f(n)=f(p^{a1})f(p^{a2})..f(p^{ak}).$$

§2. Phi hàm Euler.

Trong các hàm số học, hàm Euler mà ta định nghĩa sau đây có vai trò rất quan trọng.

Định nghĩa 3.3. *Phi- hàm Euler* $\phi(n)$ là hàm số học có giá trị tại n bằng số các số không vượt quá n và nguyên tố cùng nhau với n.

Ví dụ. Từ định nghĩa ta có: $\phi(1)=1$, $\phi(2)=1$, $\phi(3)=2$, $\phi(4)=2$, $\phi(5)=4$, $\phi(6)=2$, $\phi(7)=6$, $\phi(8)=4$, $\phi(9)=6$, $\phi(10)=4$.

Từ định nghĩa trên đây ta có ngay hệ quả trực tiếp: Số p là nguyên tố khi và chỉ khi $\phi(p)=p-1$.

Nếu định lí Fermat bé cho ta công cụ nghiên cứu đồng dư modulo một số nguyên tố, thì Phi-hàm Euler được dùng để xét đồng dư modulo một hợp số. Trước khi đi vào vấn đề đó, ta cần một số định nghĩa sau.

Định nghĩa 3.4. *Hệ thặng dư thu gọn modulo n* là tập hợp ϕ(n) số nguyên sao cho mỗi phần tử của tập hợp nguyên tố cùng nhau với n , và không có hai phần tử nào đồng dư với nhau modulo n.

Nói cách khác từ hệ thặng dư đầy đủ modolo n, để lập hệ thặng dư thu gọn, ta chỉ giữ lại những giá trị nào nguyên tố cùng nhau với n.

Ví dụ. Các số 1,2,3,4,5,6 lập thành hệ thặng dư thu gọn modulo 7. Đối với modulo 8, ta có thể lấy 1,3,5,7.

Định lí 3.5. *Nếu* $r_1,r_2,...,r_{\phi(n)}$ *là một hệ thặng dư thu gọn modulo n, và a là số nguyên dương, (a,n)=1, thì tập hợp* $ar_1,ar_2,...,ar_{\phi(n)}$ *cũng là hệ thặng dư thu gọn modulo n.*

Chúng tôi dành chứng minh định lí này cho độc giả.

Định lí trên đây được dùng để chứng minh mở rộng của định lí Fermat bé.

Định lí Euler. *Nếu m là số nguyên dương và a là số nguyên tố cùng nhau với n thì* $a^{\phi(m)} \equiv 1(\text{mod } m)$.

Chứng minh. Ta lập luận hoàn toàn tương tự như trong định lí Fermat bé. Giả sử $r_1,r_2,...,r_{\phi(m)}$ modulo m, lập nên từ các số nguyên dương không vượt quá m và nguyên tố cùng nhau với m. Theo định lí 3.5, $ar_1,ar_2,...,a\,r_{\phi(m)}$ cũng là một hệ thặng dư thu gọn. Khi đó thặng dư dương bé nhất của hệ này sẽ là tập hợp $r_1,r_2,...,\, r_{\phi(m)}$ sắp xếp theo một thứ tự nào đó. Ta có:

$$ar_1ar_2...a\,r_{\phi(m)} \equiv r_1r_2...\,r_{\phi(m)} \ (mod\ m).$$

Như vậy,

$$a^{\phi(m)}\ r_1,r_2,...,r_{\phi(m)} \equiv r_1r_2...\,r_{\phi(m)} \ (mod\ m).$$

Từ đó suy ra định lí.

Định lí Euler có thể dùng để tìm nghịch đảo modulo m. Chẳng hạn nếu a và m là các số nguyên tố cùng nhau, ta có $a.a^{\phi(m)-1} \equiv 1(\text{mod } m)$, tức là $a^{\phi(m)-1}$ chính là nghịch đảo của a modulo m. Từ đó cũng suy ra nghiệm của phương trình đồng dư tuyến tính $ax \equiv b(mod\ m),$ với $(a,m)=1$ là $x \equiv a^{\phi(m)-1}b(mod\ m)$.

Định lí 3.6. *Phi hàm Euler là hàm nhân tính.*

Chứng minh. Giả sử m, n là hai số dương nguyên tố cùng nhau. Ta cần chứng tỏ rằng ϕ(mn)= ϕ(m)ϕ(n). Ta sắp xếp tất cả các số nguyên dương không vượt quá nm thành bảng sau:

1	m+1	2m+1	...	(n-1)m+1
2	m+2	2m+2	...	(n-1)m+2

... ...

r m+r 2m+r ... (n-1)m+r

... ...

m 2m 3m ... mn

Giả sử r là số nguyên không vượt quá m, và $(m,n)=d>1$. Khi đó trong hàng thứ r không có số nào nguyên tố cùng nhau với mn. Vì thế để tính $\phi(mn)$, ta chỉ cần quan tâm các số trong hàng thứ r với $(r,m)=1$. Các số trong hàng này đều nguyên tố cùng nhau với m. Mặt khác dễ thấy rằng các số trong hàng này lập thành một hệ thặng dư đầy đủ modulo n. Do đó có đúng $\phi(n)$ số trong hàng nguyên tố cùng nhau với n, tức là trong hàng có $\phi(n)$ số nguyên tố cùng nhau với mn. Cả thảy có $\phi(n)$ hàng như vậy, định lí được chứng minh.

Nhờ tính chất này ta có ngay công thức Phi-hàm Euler.

Định lí 3.7. *Giả sử $n=p_1^{a1}p_2^{a2}...p_k^{ak}$ là phân tích của n thành thừa số nguyên tố. Khi đó ta có:*

$$\phi(n)=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})...(1-\frac{1}{p_k})$$

Chứng minh. Do Phi-hàm Euler là hàm nhân tính nên ta chỉ cần chứng minh rằng, với mọi số nguyên tố p, $\phi(p^k)=p^k-p^{k-1}$.

Thật vậy, các số nguyên dương không vượt quá p^k và không nguyên tố cùng nhau với p phải có dạng sp với s nguyên dương nào đó. Có đúng p^{k-1} số như vậy. Do đó, số các số không vượt quá p^k và nguyên tố cùng nhau với p^k đúng bằng p^k-p^{k-1}. Tính chất quan trọng sau đây của Phi-hàm thường dược sử dụng về sau.

Định lí 3.8. *Giả sử n là một số nguyên dương. Khi đó*

$$\sum_{d|n}\phi(d)=n$$

trong đó tổng được lấy theo mọi ước của n.

Chứng minh. Ta phân các số nguyên từ *1* đến n thành từng nhóm C_d: $m \in C_d$ khi và chỉ khi $(m,n)=d$, tức là khi và chỉ khi $(m/d, n/d)=1$. Như vậy, số phần tử của C_d đúng bằng số các số nguyên không vượt quá n/d và nguyên tố cùng nhau với n/d, tức là bằng $\phi(n/d)$. Ta có

$$n=\sum_{d|n}\phi(n/d)$$

Khi d chạy qua mọi ước của n thì n/d cũng chạy qua mọi ước của n: định lí được chứng minh.

Nhận xét. Các tính chất của Phi-hàm Euler được sử dụng để tính đồng dư của những luỹ thừa rất lớn. Chẳng hạn, ta cần tính $a^n \bmod k$, trong đó n là một số nguyên lớn. Giả sử ta có

$$k= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} .$$

Khi đó $a^{\phi(p_i^{\alpha_i})} \equiv 1(\text{mod } p_i^{\alpha_i})$. Nếu N là bội chung nhỏ nhất của các $\phi(p_i^{\alpha_i})$ thì $a^N \equiv 1(\text{mod } k)$. Do đó, viết $n=Nq+r$ với $r<N$, ta được $a^n \equiv a^r(\text{mod } k)$.

Ta xét một ví dụ bằng số. Tính $2^{1000000} \text{ mod } 77$. Ta có: $77=11.7$, $\phi(7)=6$, $\phi(11)=10$. Bội chung nhỏ nhất của 6 và 10 là 30. Ta có $2^{30} \equiv 1(\text{mod } 77)$. Mặt khác, $1000000=30.33333+10$. Vậy

$$2^{1000000} \equiv 2^{10} \equiv 23(\text{mod } 77).$$

§3. Số hoàn hảo và số nguyên tố Mersenne.

Tiết này dành để mô tả một dạng đặc biệt của số nguyên tố, có vai trò quan trọng trong lí thuyết và ứng dụng.

Ta bắt đầu bằng một số hàm số học quan trọng.

Định nghĩa 3.9. Hàm τ(n), số các ước, có giá trị tại n bằng số các ước dương của n; hàm $\sigma(n)$, tổng các ước, có giá trị tại n bằng tổng các ước dương của n. Nói cách khác, ta có:

$$\tau(n)= \sum_{d|n} 1,$$

$$\sigma(n)= \sum_{d|n} d .$$

Ví dụ, nếu p là một số nguyên tố thì $\tau(p)=2$, $\sigma(p)=p+1$.

Định lí 3.10. *$\tau(n)$ và $\sigma(n)$ là các hàm nhân tính.*

Dễ thấy rằng, định lí trên suy ra từ bổ đề sau.

Bổ đề 3.11. *Nếu f là hàm nhân tính, thì $F(n)= \sum_{d|n} f(d)$ cũng là hàm nhân tính.*

Thật vậy, giả sử m, n là các số nguyên dương nguyên tố cùng nhau. Ta có:

$$F(mn)= \sum_{d|mn} f(d) .$$

Vì $(m,n)=1$, mỗi ước d của mn có thể viết duy nhất dưới dạng $d=d_1d_2$ trong đó d_1,d_2 tương ứng là ước của m,n, và d_1,d_2 nguyên tố cùng nhau. Do đó ta có

$$F(mn)= \sum_{d_1|m, d_2|n} f(d_1 d_2)$$

Vì f là hàm nhân tính và $(d_1,d_2)=1$ nên:

$$F(mn)=\sum f(d_1)f(d_2)=\sum_{d_1|m} f(d_1)\sum_{d_2|n} f(d_2)=F(n)F(m)$$

Định lí được chứng minh.

Sử dụng định lí trên, ta có công thức sau đây cho các hàm τ (n) và σ (n).

Định lí 3.12. *Giả sử n có phân tích sau đây ra thừa số nguyên tố* $n=p_1^{a1}p_2^{a2}...p_k^{ak}$. *Khi đó ta có:*

$$\sigma(\mathrm{n})=\prod_{\mathrm{j}=1}^{\mathrm{k}}\frac{\mathrm{p}_{\mathrm{j}}^{\mathrm{aj}+1}-1}{p_j-1}$$

$$\tau(n)=(a_1+1)(a_2+1)...(a_k+1)=\prod_{j=1}^{k}(a_j+1)$$

Chúng tôi dành chứng minh này cho độc giả.

Do các quan niệm thần bí, người cổ Hy Lạp quan tâm đến các số nguyên bằng tổng tất cả các ước dương thực sự của nó. Họ gọi các số đó là các *số hoàn hảo*.

Định nghĩa 3.13. Số nguyên dương *n* được gọi là *số hoàn hảo* nếu $\sigma(n)=2n$.

Ví dụ. Các số 6, 28 là các số hoàn hảo: $\sigma(6)=1+2+3+6=12$, $\sigma(12)=1+2+4+7+14+28=56$
Định lí sau đây được biết từ thời Hy lạp.

Định lí 3.14. *Số nguyên dương chẵn n là số hoàn hảo khi và chỉ khi* $n=2^{m-1}(2^m-1)$, *trong đó m là một số nguyên sao cho* $m\geq 2$ *và* 2^m-1 *là nguyên tố.*

Chứng minh. Trước tiên, giả sử rằng, *m* có dạng như trên. Vì σ là hàm nhân tính, ta có: $\sigma(\mathrm{n})=\sigma(2^{\mathrm{m-1}})\ \sigma(2^{\mathrm{m}}-1)$. Từ công thức của hàm σ và giả thiết 2^m-1 là nguyên tố, dễ thấy rằng $\sigma(2^{\mathrm{m-1}})=2^{\mathrm{m}}-1$, $\sigma(2^{\mathrm{m}}-1)=2^{\mathrm{m}}$, và do đó $\sigma(n)=2n$.

Ngược lại, giả sử *n* là số hoàn hảo chẵn. Viết $n=2^st$, trong đó *s,t* là các số nguyên dương, *t* lẻ, ta được:

$$\sigma(n)=\sigma(2^st)=\sigma(2^s)\ \sigma(t)=(2^{s+1}-1)\ \sigma(t)$$

Vì *n* là số hoàn hảo, $\sigma(n)=2n=2^{s+1}t$.

Như vậy, $2^{s+1}|\sigma(t)$, giả sử $\sigma(t)=2^{s+1}q$. Ta có đẳng thức

$$(2^{s+1}-1)2^{s+1}q=2^{s+1}t,$$

tức là $q|t$ và $q\neq t$. Mặt khác ta có:

$$t+q=(2^{s+1}-1)q+q=2^{s+1}q=\sigma(t)$$

Ta chứng tỏ rằng, $q=1$. Thật vậy, nếu ngược lại, *t* có ít nhất 3 ước khác nhau là *1, t, q,* do đó $\sigma(t)\geq t+q+1$, mâu thuẫn đẳng thức vừa chứng minh. Vậy $\sigma(t)=t+1$, nghĩa là *t* là số nguyên tố. Định lí được chứng minh.

Như vậy để tìm các số hoàn hảo, ta cần tìm các số nguyên tố dạng 2^m-1.

Định nghĩa 3.15. Giả sử m là một số nguyên dương, khi đó $M_m=2^m-1$ được gọi là *số Mersenne thứ m*. Nếu p là số nguyên tố, và M_p cũng nguyên tố, thì M_p được gọi là số nguyên tố Mersenne.

Ví dụ. M_2,M_3,M_5,M_7 là các số nguyên tố Mersenne, trong khi M_{11} là hợp số. Có nhiều định lí khác nhau dùng để xác định số nguyên tố Mersenne. Chẳng hạn nhờ định lí sau đây, ta có thể kiểm tra nhanh chóng dựa vào dạng của các ước số của số nguyên tố Mersenne.

Định lí 3.16. *Nếu p là một số nguyên tố lẻ, thì mọi ước của số nguyên tố Mersenne M_p đều có dạng 2kp+1, trong đó k là số nguyên dương.*

Chứng minh. Giả sử q là một số nguyên tố của M_p. Theo định lí Fermat bé, $q|(2^{q-1}-1)$. Theo hệ quả 1.9, $(2^p-1,2^{q-1}-1)=2^{(p,q-1)}-1$. Ước chung này lớn hơn 1, vì nó là một bội của q. Do đó, $(p,q-1)=p$, vì p là một số nguyên tố. Ta có $q=mp+1$, và vì q lẻ nên $m=2k$, định lí được chứng minh.

Sau đây là vài ví dụ cho thấy ứng dụng của định lí trên.

Ví dụ 1. Để xét xem $M_{13}=2^{13}-1=8191$ có phải là số nguyên tố hay không, ta cần xem các phép chia cho những số nguyên tố không vượt quá $\sqrt{8191}=90,504...$ Mặt khác, theo định lí trên, mọi ước nguyên tố đều phải có dạng $26k+1$. Như vậy chỉ cần thử với hai số 53 và 79: ta thấy M_{13} là số nguyên tố.

Ví dụ 2. Xét $M_{23}=8388607$. Ta cần xét các phép chia của nó cho các số nguyên tố dạng $46k+1$. Số đầu tiên 47 là ước của nó: M_{23} là hợp số.

Có nhiều thuật toán đặc biệt để kiểm tra nguyên tố các số Mersenne. Nhờ đó, người ta phát hiện được những số nguyên tố rất lớn. Mỗi lần có một số nguyên tố Mersenne, ta lại được một số hoàn hảo. Cho đến nay, người ta đã biết được rằng, với $p\leq 132049$, chỉ có 30 số nguyên tố Mersenne, và tính được chúng. Số nguyên tố Mersenne tìm được gần đây nhất là số M_{216091}, gồm 65050 chữ số.

Giả thuyết sau đây vẫn còn chưa được chứng minh.

Giả thuyết 3.17. *Tồn tại vô hạn số nguyên tố Mersenne*.

Người ta đã biết được rằng, trong khoảng từ 1 đến 10^{200} không có số hoàn hảo lẻ. Tuy nhiên câu hỏi sau đây vẫn chưa được trả lời.

Câu hỏi 3.18. *Tồn tại hay không các số hoàn hảo lẻ?*

§4. Căn nguyên thuỷ.

Khi xét các số phức là căn bậc n của đơn vị, ta thường chú ý những số nào không phải là căn của đơn vị với bậc thấp hơn. Những số đó gọi là căn nguyên thuỷ của đơn vị. Đối với các số nguyên, ta cũng có khái niệm hoàn toàn tương tự về "căn" và "căn nguyên thuỷ" của đơn vị.

Định nghĩa 3.19. Giả sử a và m là các số nguyên dương nguyên tố cùng nhau. Khi đó số nguyên nhỏ nhất x thoả mãn đồng dư $a^x \equiv 1 (mod\ m)$ được gọi là *bậc của a modulo m*. Ta viết $x = ord_m a$.

Ta chú ý rằng, số x như vậy tồn tại vì theo định lí Euler, $a^{\phi(m)} \equiv 1 (\mathrm{mod}\ m)$.

Định lí 3.20. *Giả sử a và n là các số nguyên tố cùng nhau, n>0. Khi đó số nguyên x là nghiệm của đồng dư $a^x \equiv 1 (mod\ m)$ khi và chỉ khi x là một bội của bậc của a modulo n.*

Chứng minh. Giả sử x thoả mãn đồng dư trên. Ta viết $x = q\ ord_n a + r$, trong đó $0 \le r < x$. Từ đó ta có $a^r \equiv 1 (mod\ m)$. Vì $ord_n a$ là số dương nhỏ nhất có tính chất đó nên $r=0$: x là một bội của bậc của a modulo n. Điều ngược lại là rõ ràng.

Hệ quả 3.21. *Nếu a và n là các số nguyên tố cùng nhau, n>0, thì $ord_n a \mid \phi(n)$.*

Hệ quả 3.22. *Nếu a và n là các số nguyên tố cùng nhau, n>0, thì $a^i \equiv a^j (mod\ n)$ khi và chỉ khi $i \equiv j (mod\ n)$.*

Chứng minh các hệ quả trên được dành cho độc giả.

Do hệ quả 3.21, nếu r và n là nguyên tố cùng nhau thì bậc của r không vượt quá $\phi(n)$. Các số có bậc đúng bằng $\phi(n)$ giữ vai trò quan trọng trong nhiều vấn đề khác nhau của số học. Ta có định nghĩa sau.

Định nghĩa 3.23. Nếu r và n là các số nguyên tố cùng nhau, $n>0$, và nếu $ord_n r = \phi(n)$ thì r được gọi là căn nguyên thuỷ modulo n.

Chú ý rằng không phải mọi số đều có căn nguyên thuỷ. Chẳng hạn, xét $n=8$. Các số nhỏ hơn 8 và nguyên tố cùng nhau với 8 là 1, 3, 5, 7, đồng thời ta có $ord_8 1 = 1$, bậc của các số còn lại bằng 2, trong khi $\phi(8)=4$. Vấn đề những số nguyên nào thì có căn nguyên thuỷ sẽ được xét về sau.

Định lí 3.24. *Nếu r, n nguyên tố cùng nhau, n>0, và nếu r là căn nguyên thuỷ modulo n, thì các số sau đây lập thành hệ thặng dư thu gọn modulo n:*

$$r^1, r^2, \ldots, r^{\phi(n)}.$$

Chứng minh. Vì $(r,n)=1$, các số trên nguyên tố cùng nhau với n. Ta chỉ cần chứng tỏ rằng, không có hai số nào đồng dư với nhau modulo n. Giả sử $r^i \equiv r^j (mod\ n)$. Theo hệ quả 3.22, $i \equiv j (mod\ \phi(n))$. Từ đó suy ra $i=j$, vì i, j không vượt quá $\phi(n)$. Định lí được chứng minh.

Định lí 3.25. *Nếu $ord_m a = t$ và u là số nguyên dương, thì $ord_m(a^u) = t / (t,u)$.*

Chứng minh. Đặt $v=(t,u)$, $t=t_1 v$, $u=u_1 v$, $s = ord_m(a^u)$. Ta có

$$(a^u)^{t_1} = (a^{u_1 v})^{t/v} = (a^t)^{u_1} \equiv 1 (mod\ m).$$

Do đó, $s \mid t_1$. Mặt khác, $(a^u)^s = a^{us} \equiv 1 (mod\ m)$ nên $t \mid su$. Như vậy, $t_1 v \mid u_1 vs$, do đó, $t_1 \mid u_1 s$. Vì $(u_1, t_1)=1$, ta có $t_1 \mid s$. Cuối cùng, vì $s \mid t_1$, $t_1 \mid s$ nên $s = t_1 = t/v = t/(t, u)$, chứng minh xong.

Hệ quả 3.26. *Giả sử r là căn nguyên thủy modulo m, trong đó m là số nguyên lớn hơn 1. Khi đó r^u là căn nguyên thủy modulo m nếu và chỉ nếu $(u, \phi(m))=1$.*

Thật vậy, $ord_m r^u = ord_m r/(u, ord_m r) = \phi(m)/(u, \phi(m))$: hệ quả được chứng minh.

Định lí 3.27. *Nếu số nguyên dương m có căn nguyên thuỷ, thì nó có tất cả $\phi(\phi(m))$ căn nguyên thuỷ không đồng dư nhau.*

Thật vậy, nếu *r* là một căn nguyên thuỷ thì $r, r^2, ..., r^{\phi(m)}$ là một hệ đầy đủ các thặng dư thu gọn modulo *m*. Số căn nguyên thuỷ modulo *m* đúng bằng số các số *u* thoả mãn $(u, \phi(m))=1$, và có đúng $\phi(\phi(m))$ số *u* như thế. Định lí được chứng minh.

§5. Sự tồn tại của căn nguyên thuỷ.

Trong tiết này, ta sẽ xác định những số nguyên có căn nguyên thuỷ. Trước tiên ta sẽ chứng minh rằng mọi số nguyên tố đều có căn nguyên thuỷ. Để làm việc đó, ta cần một vài kiến thức về đồng dư đa thức.

Giả sử $f(x)$ là đa thức với hệ số nguyên. Số *c* được gọi là *nghiệm của đa thức $f(x)$ modulo m* nếu $f(c) \equiv 0 (mod\ m)$. Dễ thấy rằng, nếu *c* là một nghiệm thì mọi số đồng dư với *c* modulo *m* cũng là nghiệm.

Đối với số nghiệm của một đa thức modulo một số nguyên, ta cũng có tính chất tương tự như số nghiệm của một đa thức.

Định lí Lagrange. *Giả sử $f(x)=a_n x^n+...+a_1 x+a_0$ là đa thức với hệ số nguyên, n>o, đồng thời $a_n \not\equiv 0 (mod\ p)$. Khi đó f(x) có nhiều nhất n nghiệm modulo p không đồng dư từng cặp.*

Chứng minh. Ta chứng minh bằng qui nạp. Khi $n=1$, định lí là rõ ràng. Giả sử định lí đã chứng minh với đa thức bậc $n-1$ có hệ số của luỹ thừa cao nhất không chia hết cho *p*, và giả sử rằng đa thức $f(x)$ có $n+1$ nghiệm modulo *p* không đồng dư từng cặp $c_0, c_1, ..., c_n$. Ta có $f(x)-f(c_0)=(x-x_0)g(x)$, trong đó $g(x)$ là đa thức bậc $n-1$ với hệ số cao nhất là a_n. Vì với mọi k, $0 \le k \le n$, $c_k - c_0 \not\equiv 0 \pmod p$, trong khi đó $f(c_k)-f(c_0)=(c_k-c_0)g(c_k) \equiv 0 (mod\ p)$, nên c_k là nghiệm của $g(x)$ modulo *p*: trái với giả thiết quy nạp. Định lí được chứng minh.

Định lí 3.28. *Giả sử p là số nguyên tố và d là một ước của p-1. Khi đó đa thức x^d-1 có đúng d nghiệm modulo p không đồng dư từng cặp.*

Chứng minh. Thật vậy, giả sử $p-1=de$. Ta có $x^{p-1}-1=(x^d-1)g(x)$. Theo định lí Fermat bé, $x^{p-1}-1$ có $p-1$ nghiệm modulo *p* không đồng dư từng cặp. Mặt khác, mỗi một nghiệm đó phải là nghiệm của x^d-1 hoặc là của $g(x)$. Theo định lí Lagrange, $g(x)$ có nhiều nhất $p-d-1$ nghiệm không đồng dư từng cặp, vì thế x^d-1 phải có ít nhất $(p-1)-(p-d-1)=d$ nghiệm. Lại theo định lí Lagrange, x^d-1 có không quá *d* nghiệm, vậy nó có đúng *d* nghiệm modulo *p* không đồng dư từng cặp. Định lí dược chứng minh.

Định lí trên đây sẽ được sử dụng trong chương 5 khi xây dựng các trường hữu hạn.

Định lí 3.29. *Giả sử p là số nguyên tố, d là ước dương của p-1. Khi đó, số các số nguyên không đồng dư bậc d modulo p là* $\phi(d)$.

Chứng minh. Giả sử *F(d)* là số các số nguyên dương bậc *d* modulo *p* và bé hơn *p*. Ta cần chứng tỏ rằng $F(d)=\phi(d)$. Vì ϕ(d)=p-1 nên $d|p-1$, từ đó ta có

$$p-1=\sum_{d|p-1} F(d)$$

Mặt khác ta có:

$$p-1=\sum_{d|p-1} \phi(d)$$

theo công thức của Phi-hàm. Như vậy định lí sẽ được chứng minh nếu ta chứng tỏ được rằng $F(d)\le\phi(d)$ nếu $d|p-1$.

Khi $F(d)=0$, điều nói trên là tầm thường. Giả sử $F(d)\neq 0$, tức là tồn tại số nguyên *a* bậc *d* modulo *p*. Khi đó, các số nguyên $a, a^2,...,a^d$ không đồng dư modulo *p*. Rõ ràng rằng, mỗi luỹ thừa của *a* là một nghiệm của $x^d-1\equiv 0(mod\ p)$, mà số nghiệm không đồng dư đúng bằng *d*, nên mỗi nghiệm modulo *p* đồng dư với một trong các luỹ thừa của *a*. Do đó, vì phần tử tuỳ ý bậc *d* là một nghiệm của phương trình $x^d-1\equiv 0(mod\ p)$ nên phải đồng dư với một trong các luỹ thừa của *a*. Mặt khác, theo định lí 3.24, luỹ thừa *k* của *a* có bậc *d* khi và chỉ khi $(k,d)=1$. Có đúng ϕ(d) số *k* như vậy, và do đó suy ra F(d))$\le\phi$(d), định lí được chứng minh.

Hệ quả 3.30. *Mọi số nguyên tố đều có căn nguyên thuỷ.*

Thật vậy, giả sử *p* là số nguyên tố. Khi đó có $\phi(p-1)$ số nguyên bậc *p-1* modulo *p* (Định lí 3.28) không đồng dư từng cặp. Theo định nghĩa, mỗi số đó là một căn nguyên thuỷ: *p* có $\phi(p-1)$ căn nguyên thuỷ.

Phần còn lại của chương được giành để tìm tất cả các số nguyên dương có căn nguyên thuỷ.

Định lí 3.31. *Nếu p là một số nguyên tố lẻ với căn nguyên thuỷ r, thì hoặc r, hoặc r+p là căn nguyên thuỷ modulo* p^2.

Chứng minh. Vì *r* là căn nguyên thuỷ modulo *p* nên ta có

$$ord_p r=\phi(d)=p-1.$$

Giả sử $n=ord_{p^2} r$. Ta có $r^n\equiv 1(mod\ p^2)$, và do đó $r^n\equiv 1(mod\ p)$. Như vậy, bậc *p-1* của *r* là một ước của *n*. Mặt khác, *n* là bậc của *r* modulo p^2 nên *n* là ước của $\phi(p^2)=p(p-1)$. Vì $n|p(p-1)$ và $p-1|n$ nên dễ dàng suy ra rằng, hoặc $n=p-1$, hoặc $n=p(p-1)$. Nếu $n=p(p-1)$ thì *r* là căn nguyên thuỷ modulo p^2, vì ord_{p^2} r=ϕ(p^2). Trong trường hợp còn lại, $n=p-1$, ta có $r^{p-1}\equiv 1(\text{mod } p^2)$. Đặt $s=r+p$. Cần phải chứng minh rằng *s* là căn nguyên thuỷ modulo p^2. Vì $s\equiv r(mod\ p)$, *s* cũng là căn nguyên thuỷ

modulo p. Như vậy, theo chứng minh trên ord_{p^2} s hoặc bằng $p-1$, hoặc bằng $p(p-1)$. Ta sẽ chứng tỏ rằng, bậc đó không thể là $p-1$. Ta có

$$s^{p-1}=(r+p)^{p-1} \equiv r^{p-1}+(p-1)pr^{p-2} (mod\ p^2) \equiv 1+(p-1)pr^{p-2} \equiv 1-pr^{p-2} (mod\ p^2)$$

Từ đó ta có thể thấy rằng, $s^{p-1} \not\equiv 1 (mod\ p^2)$. Thật vậy, nếu ngược lại thì $pr^{p-2} \equiv 0 (\text{mod } p^2)$, nên $r^{p-2} \equiv 0 (\text{mod } p)$. Điều này không thể có, vì $p \nmid r$ do r là căn nguyên thuỷ modulo p. Như vậy $ord_{p^2} s=p(p-1)=\phi(p^2)$, tức $s=r+p$ là căn nguyên thuỷ modulo p^2.

Bây giờ ta xét luỹ thừa tuỳ ý của số nguyên tố

Định lý 3.32. *Giả sử p là một số nguyên tố lẻ, khi đó p^k có căn nguyên thuỷ với mọi số nguyên dương k. Hơn nữa, nếu n là căn nguyên thuỷ modulo p^2 thì r là căn nguyên thuỷ modulo p^k với mọi số ngyên dương k.*

Chứng minh. Từ Định lí 3.31, p có căn nguyên thuỷ r sao cho đó cũng là căn nguyên thuỷ modulo p^2, và do đó

$$r^{p-1} \not\equiv 1 (mod\ p^2).$$

Ta sẽ chứng minh r cũng là căn nguyên thuỷ modulo p^k với mọi số nguyên dương k.

Bằng quy nạp có thể thấy rằng

$$r^{p^{k-1}(p-1)} \not\equiv 1 (\text{mod } p^k) \qquad (*)$$

với mọi số nguyên dương k. Giả sử

$$n=ord_{p^k} r$$

Ta có $n \mid \varphi(p^k)=p^{k-1}(p-1)$. Mặt khác

$$r^n \not\equiv 1 (mod\ p^k),$$

và $r^n \not\equiv 1 (mod\ p)$.

Do đó $p-1=\varphi(p) \mid n$ (Định lí 3.30). Vì $(p-1) \mid n$ và $n \mid p^{k-1}(p-1)$ nên $n=p^t(p-1)$, trong đó t là số nguyên dương $0 \le t \le k-1$. Nếu $n=p^t(p-1)$ với $t \le k-2$ thì

$$r^{p^{k-2}(p-1)} = (r^{p^t(p-1)})^{p^{k-2-t}} \equiv 1 (\text{mod } p^k),$$

mâu thuẫn. Vậy $ord_{p^k} r=p^{k-1}(p-1)=\varphi(p^k)$, r cũng là cũng nguyên thuỷcủa p^k.

Chứng minh (*): k=2: đúng. Giả sử (*) đúng với số nguyên dương $k \ge 2$. Khi đó

$$r^{p^{k-2}(p-1)} \not\equiv 1 (\text{mod } p^k).$$

Vì $(r,p)=1$, ta thấy $(r,p^{k-1})=1$. Do đó, từ Định lí Euler ta có

$$r^{p^{k-2}(p-1)} \equiv r^{\varphi(p^{k-1})}$$

Vậy tồn tại số nguyên d sao cho

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

trong đó $p \nmid d$, vì theo giả thiết $r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}$.

Ta lấy luỹ thừa bậc p của hai vế phương trình trên và nhận được

$$r^{p^{k-1}(p-1)} = (1 + dp^{k-1})^p = 1 + p(dp^{k-1}) + \binom{p}{2} p^2 (dp^{k-1})^2 + \ldots + (dp^{k-1})^p$$

$$\equiv 1 + dp^k \pmod{p^{k+1}}.$$

Vì $p \nmid d$ nên ta có

$$r^{p^{k-1}(p-1)} \not\equiv 1 \pmod{p^{k+1}},$$

chứng minh xong.

Ví dụ: r=3 là căn nguyên thuỷ modulo 7^k với mọi số nguyên dương k.

Định lí 3.33: *Nếu số nguyên dương n không phải là luỹ thừa của một số nguyên tố hoặc hai lần luỹ thừa một số nguyên tố, thì n không có căn nguyên thuỷ.*

Chứng minh. Giả sử n là số nguyên dương với phân tích ra thừa số nguyên tố như sau

$$n = p_1^{t_1} p_2^{t_2} \ldots p_m^{t_m}.$$

Giả sử n có căn nguyên thuỷ r, tức là $(n,r)=1$ và $ord_n r = \varphi(n)$. Vì $(r,n)=1$ nên $(r,p^t)=1$ trong đó p^t là một trong các luỹ thừa nguyên tố có mặt trong phân tích trên. Theo Định lý Euler,

$$r^{\varphi(p^t)} \equiv 1 \pmod{p^t}.$$

Giả sử U là bội chung nhỏ nhất của $\varphi(p_1^{t_1}), \varphi(p_2^{t_2}), \ldots, \varphi(p_m^{t_m})$,

$$U = [\varphi(p_1^{t_1}), \varphi(p_2^{t_2}), \ldots, \varphi(p_m^{t_m})].$$

Vì $\varphi(p_i^{t_i}) \mid U$ nên

$$r^U \equiv 1 \pmod{p_i^{t_i}}$$

Với $I=1, 2, \ldots, m$. Do đó

$$ord_n r = \varphi(n) \le U.$$

Mặt khác,

$$\varphi(n) = \varphi(p_1^{t_1} p_2^{t_2} \ldots p_m^{t_m}) = \varphi(p_1^{t_1}) \varphi(p_2^{t_2}) \ldots \varphi(p_m^{t_m}).$$

Từ đó ta có

$$\varphi(p_1^{t_1}) \varphi(p_2^{t_2}) \ldots \varphi(p_m^{t_m}) \le [\varphi(p_1^{t_1}), \varphi(p_2^{t_2}), \ldots, \varphi(p_m^{t_m})],$$

Tức là $\varphi(p_1^{t_1}), \varphi(p_2^{t_2}),\ldots, \varphi(p_m^{t_m})$ phải nguyên tố cùng nhau từng đôi một. Do $\varphi(p^t)=p^{t-1}(p-1)$ nên $\varphi(p^t)$ chẵn nếu p lẻ, hoặc nếu $p=2$ và $t\geq 2$. Vậy, các số $\varphi(p_1^{t_1}), \varphi(p_2^{t_2}),\ldots, \varphi(p_m^{t_m})$ không nguyên tố cùng nhau từng cặp, trừ trường hợp $m=1$ (và do đó n là luỹ thừa của số nguyên tố), hoặc $m=2$ và $n=2p^t$, trong đó p là số nguyên tố lẻ và t là số nguyên dương.

Định lí 3.34: *Nếu p là số nguyên tố lẻ và t là số nguyên dương, thì $2p^t$ có căn nguyên thuỷ. Cụ thể là, nếu r là căn nguyên thuỷ modulo p^t thì r, (tương ứng, $r+p^t$), là căn nguyên thuỷ modulo $2p^t$ khi r lẻ, (tương ứng, khi r chẵn).*

Chứng minh: Giả sử r là căn nguyên thuỷ modulo p^t, khi đó

$$r^{\varphi(p^t)} \equiv 1 \pmod{p^t},$$

và không có luỹ thừa nào nhỏ hơn $\varphi(p^t)$ thoả mãn đồng dư.

Do $\varphi(2p^t)= \varphi(2)\ \varphi(p^t)= \varphi(p^t)$ nên

$$r^{\varphi(2p^t)} \equiv 1 \pmod{p^t}.$$

Khi r lẻ,

$$r^{\varphi(2p^t)} \equiv 1 \pmod{2}.$$

Từ đó ta có $r^{\varphi(2p^t)} \equiv 1 \pmod{2p^t}$. Vì không có luỹ thừa bé hơn của r thoả mãn đồng dư nên r chính là căn nguyên thuỷ của $2p^t$.

Khi r chẵn, $r+p^t$ lẻ. Do đó,

$$(r+p^t)^{\varphi(2p^t)} \equiv 1 \pmod{2}.$$

Vì $r+p^t \equiv r \pmod{p^t}$ nên

$$(r+p^t)^{\varphi(2p^t)} \equiv 1 \pmod{p^t}\cdot$$

Do đó

$$(r+p^t)^{\varphi(2p^t)} \equiv 1 \pmod{2p^t},$$

và vì không có luỹ thừa bé hơn nào của $(r+p^t)$ thoả mãn đồng dư, ta suy ra $r+p^t$ là căn nguyên thuỷ modulo $2p^t$.

Định lí 3.35: *Nếu a là số nguyên lẻ, $k\geq 3$ là số nguyên thì*

$$a^{\varphi(2^k)/2} = a^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

Chứng minh. Ta chứng minh bằng quy nạp. Giả sử a là số nguyên lẻ, $a=2b+1$.Ta có $a^2=4b(b+1)+1$. Vì b hoặc $b+1$ chẵn nên $8 \mid 4b(b+1)+1$, tức là

$$a^2 \equiv 1 \pmod{8}.$$

Như vậy, định lí đúng khi $k=3$. Giả sử

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}$$

Khi đó tồn tại số nguyên d sao cho

$$a^{2^{k-2}} = 1+d.2^k.$$

Từ đó ta có:

$$a^{2^{k-1}} = 1+d.2^{k+1}+d^2.2^{2k},$$

tức là

$$a^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}.$$

Từ định lí trên ta suy ra rằng, các luỹ thừa 2^k với $k \geq 3$ không có căn nguyên thuỷ. Như vậy, trong các luỹ thừa của 2 chỉ có 2 và 4 là có căn nguyên thuỷ. Kết hợp điều này với các Định lí 3.32, 3.33, 3.34, ta có định lí sau đây

Định lí 3.36: *Số nguyên dương n có căn nguyên thuỷ khi và chỉ khi*

$$n=2, 4, p^t, 2p^t,$$

trong đó p là số nguyên tố lẻ, t là số nguyên dương.

Bài tập và tính toán thực hành chương 3

I. Bài tập

3.1. Hàm Möbius được định nghĩa như sau: $\mu(n)=(-1)^k$, nếu n không chia hết cho số chính phương nào khác 1, và k là số các ước nguyên tố của n; $\mu(1)=1$, $\mu(n)=0$ khi n có ước là số chính phương khác 1.

Chứng minh rằng, với mọi $n>1$, $\sum_{d|n}\mu(d)=0$.

3.2 (Biến đổi ngược Möbius). Cho $f(n)$ là một hàm số học. Đặt

$$F(n)=\sum_{d|n} f(d).$$

Chứng minh rằng:

1) $$f(n)=\sum_{d|n}\mu(d)\,F(n/d).$$

2) Nếu f là hàm nhân tính thì F cũng là hàm nhân tính.

3.3. Dùng biến đổi ngược Möbius và công thức $n=\sum_{d|n}\phi(n/d)$, chứng minh rằng

1) $\phi(p^k)=p^k-p^{k-1}$ với p là số nguyên tố.

2) $\phi(n)$ là hàm nhân tính.

3.4. Cho θ là hàm nhân tính và μ là hàm Möbius. Chứng minh rằng, nếu các ước nguyên tố của n là $p_1,p_2,...p_k$ thì

$$\sum_{d|n}\mu(d)\;\theta(d)=(1-\theta(p_1))(1-\theta(p_2))...(1-\theta(p_k))$$

(nếu n=1, ta xem vế phải là 1)

3.5. Hàm $\sigma_k(n)$ (tổng luỹ thừa bậc k của các ước số của n) được định nghĩa như sau:

$$\sigma_k(n)=\sum_{d|n} d^k .$$

1) Cho công thức tính $\sigma_k(p)$ với p là số nguyên tố.

2) Tính $\sigma_k(p^s)$ khi s là số nguyên dương.

3) Chứng minh rằng $\sigma_k(n)$ là hàm nhân tính.

4) Từ đó cho công thức tính $\sigma_k(n)$ khi $n= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$.

3.6. Tìm tất cả các số tự nhiên n thoả mãn

$$\sigma(n)+ \phi(n)=2n.$$

3.7. Chứng minh rằng n là một hợp số khi và chỉ khi

$$\sigma(n)>n+\sqrt{(n)}.$$

3.8. Chứng minh rằng nếu hai số nguyên có tích các ước số khác nhau thì hai số nguyên đó khác nhau.

3.9.Tính các đồng dư sau đây bằng nhiều phương pháp khác nhau (chẳng hạn bằng phương pháp bình phương liên tiếp hoặc nhờ nhận xét cuối §2):

1. $3^{1000000} \bmod 165$.
2. $5^{1234567} \bmod 221$.
3. $7^{1000000000} \bmod 541$.

3.10. Chứng minh rằng 91 là số giả nguyên tố cơ sở 3 nhưng không giả nguyên tố Euler cơ sở 3, và không là số giả nguyên tố cơ sở 2.

3.11. Cho $f(n)$ là hàm nhân tính giới nội. Chứng minh rằng tổng

$$\sum f(n)/n^s$$

hội tụ tuyệt đối trong nửa mặt phẳng $Re\ s>1$ (trong đó Re là kí hiệu phần thực của một số), và tổng trong miền hội tụ bằng tích vô hạn hội tụ sau đây

$$\prod_{p\in P}(1+f(p)p^{-s}+\dots+f(p^m)p^{-ms}+\dots),$$

(tích được lấy trên tập hợp tất cả các số nguyên tố).

3.12. Chứng minh rằng, nếu f là hàm nhân tính mạnh giới nội thì

$$\sum_{n=1}^{\infty} f(n)/n^s = \prod_{p\in P}\frac{1}{1-f(p)/p^s}.$$

3.13. Chứng minh đẳng thức sau đối với Zeta-hàm Riemann:

$$\zeta(s)=\sum_{n=1}^{\infty}1/n^s=\prod_{p\in P}\frac{1}{1-p^{-s}}.$$

3.14. Chứng minh rằng nếu $n\neq 2,4,p^{\alpha},2p^{\alpha}$, trong đó p là số nguyên tố lẻ thì

$$a^{\phi(n)/2}\equiv 1(\bmod n).$$

3.15. Chứng minh rằng nếu n chia hết cho 24 thì $\sigma(n)$ cũng chia hết cho 24.

3.17. a) Chứng minh rằng nếu p,q là các số nguyên tố lẻ khác nhau thì $n=pq$ là số giả nguyên tố cơ sở 2 khi và chỉ khi $ord_q 2 | p-1$, $ord_p 2 | q-1$.

b) Trong các số sau đây, số nào là số giả nguyên tố cơ sở 2: 871, 1378, 2047, 2813.

3.18. Chứng minh rằng nếu p,q là các số nguyên tố lẻ khác nhau thì $n=pq$ là số giả nguyên tố cơ sở 2 khi và chỉ khi $M_p M_q=(2^p-1)(2^q-1)$ là số giả nguyên tố cơ sở 2.

3.19. a) Chứng minh rằng nếu đa thức $f(x)$ bậc n, hệ số nguyên, có quá n nghiệm modulo p thì mọi hệ số của $f(x)$ đều chia hết cho p.

b) Cho p là một số nguyên tố. Chứng minh rằng mọi hệ số của đa thức

$$f(x)=(x-1)(x-2)...(x-p+1)-x^{p-1}-x+1$$

chia hết cho p.

c) Dùng câu b) để chứng minh định lí Wilson.

3.20. Tìm tất cả các số tự nhiên n sao cho: $\sigma(n)=12, 18, 24, 48, 52, 84$.

3.21. Chứng minh rằng với mọi $k>1$, phương trình $\tau(n)=k$ có vô số nghiệm.

3.22. Tìm n nhỏ nhất để $\tau(n)=1, 2, 3, 6, 14, 100$.

3.23. Tìm căn nguyên thuỷ modulo:

$$11^2, 17^2, 13^2, 19^2, 3^k, 13^k, 11^k, 17^k.$$

3.24. Chứng minh rằng nếu m có căn nguyên thuỷ thì đồng dư $x^2 \equiv 1 (mod\ m)$ chỉ có nghiệm $x=\pm 1 (mod\ m)$.

3.25. Chứng minh rằng mặc dù không tồn tại căn nguyên thuỷ 2^k, $k \geq 3$, mỗi số nguyên lẻ đồng dư với đúng một số nguyên dạng $(-1)^\alpha 5^\beta$, trong đó $\alpha=0$ hoặc 1, β là số nguyên thoả mãn $0 \leq \beta \leq 2^{k-2}-1$.

3.26. Giả sử n là một số có căn nguyên thuỷ. Chứng minh rằng tích của các số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n đồng dư (-1) modulo n (khi n là số nguyên tố, ta có định lí Wilson).

3.27. Tìm tất cả các nghiệm của đồng dư sau:

a) $x^2+x+1 \equiv 0 (mod\ 7)$

b) $x^2+5x+1 \equiv 0 (mod\ 7)$

c) $x^2+3x+1 \equiv 0 (mod\ 7)$.

II. Thực hành tính toán trên máy tính

II. 1. Tính Phi-hàm Euler

Để tính Phi-hàm Euler của một số nguyên dương n ta thực hiện dòng lệnh như sau:

```
[> phi(n);
```

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

Thí dụ: Tính Phi-hàm Euler của 65.

```
[> phi(65);
```

```
                                48
```

II. 2. Thực hành tìm các số khi biết phi-hàm Euler của nó

Để tìm các số khi biết Phi-hàm Euler k ta thực hiện dòng lệnh sau:

```
[>invphi(k);
```

Sau dấu (;) ấn phím "Enter" màn hình sẽ hiện ra các số cần tìm.

Thí dụ: Tìm các số khi biết Phi-hàm Euler của nó là 4.

Ta thực hiện như sau:

```
[> invphi(4);
```

```
                              [5, 8, 10, 12]
```

Vậy các số có Phi-hàm Euler bằng 4 là 5, 8, 10, 12.

II. 3. Thực hành kiểm tra số nguyên tố Mersenne

Cho m là một số nguyên dương, đặt $M_m:=2^m-1$. Để kiểm tra xem M_m có phải là số nguyên tố Mersenne hay không ta thực hiện dòng lệnh như sau:

```
[> mersenne(m);
```

Sau dấu (;) ấn phím "Enter". Nếu trên màn hình xuất hiện kết quả là một số thì M_m là số nguyên tố Mersenne và M_m chính bằng số đó. Nếu không trên màn hình sẽ xuất hiện chữ "false".

Thí dụ 1: M_7 có phải là số nguyên tố Mersenne hay không?

Ta thực hiện dòng lệnh như sau:

```
[> mersenne(7);
```

```
                                127
```

Vậy M_7=127 và là số nguyên tố Mersenne.

Thí dụ 2: M_{125} có phải là số nguyên tố Mersenne hay không?

```
[> mersenne(125);
```

```
                               false
```

Vậy M_{125} không phải là số nguyên tố Mersenne.

Thí dụ 3: M_{11} có phải là số nguyên tố Mersenne hay không?

```
[> mersenne(11);
```

```
                              false
```

Vậy M_{11} không phải là số nguyên tố Mersenne.

II. 4. Tính bậc của một số theo một modulo nào đó

Cho *m* là một số nguyên dương, *n* là một số nguyên. Để tính bậc của *n* modulo *m* ta thực hiện dòng lệnh như sau:

```
[>order(n,m);
```

Sau dấu (;) ấn phím "Enter". Nếu *m, n* là các số nguyên tố cùng nhau thì trên màn hình sẽ xuất hiện kết quả chính là bậc của *n* theo modulo *m*. Nếu *m, n* không nguyên tố cùng nhau thì trên màn hình sẽ xuất hiện chữ "FAIL".

Thí dụ 1: Tính bậc của 13 theo modulo 100.

```
[> order(13,100);
```

```
                                  20
```

Vậy $ord_{100}13=20$.

Thí dụ 2: Tính bậc của 5 theo modulo 8

```
[>order(5,8);
```

```
                                  2
```

Vậy $ord_8 5 = 2$.

Thí dụ 3: Tính bậc của 8 theo modulo 12.

```
[> order(8,12);
```

```
                                FAIL
```

II. 5. Tìm căn nguyên thuỷ

1. Cho *n* là một số nguyên lớn hơn 1. Để tìm căn nguyên thuỷ đầu tiên modulo *n* ta thực hiện dòng lệnh như sau:

```
[> primroot(n);
```

Sau dấu (;) ấn phím "Enter". Nếu trên màn hình hiện ra kết quả là một số thì số đó chính là căn nguyên thuỷ đầu tiên modulo *n*. Nếu màn hình hiện ra chữ "FAIL" thì *n* không có căn nguyên thuỷ.

Thí dụ 1: Tìm căn nguyên thuỷ modulo 41.

```
[> primroot(41);
```

```
                                  6
```

Vậy 6 là căn nguyên thuỷ modulo 41.

Thí dụ 2: Tìm căn nguyên thuỷ modulo 15.

```
[> primroot(15);
```

```
                              FAIL
```

Vậy 15 không có căn nguyên thuỷ.

2. Để tìm căn nguyên thuỷ modulo *n* lớn hơn *g* ta thực hiện dòng lệnh sau:

```
[> primroot(g,n);
```

Sau dấu (;) ấn phím "Enter". Nếu trên màn hình hiện ra kết quả là một số thì số đó chính là căn nguyên thuỷ lớn hơn *g* đầu tiên modulo *n*. Nếu màn hình hiện ra chữ "FAIL" thì *n* không có căn nguyên thuỷ. Chú ý, nếu *g*=0 thì hai lệnh trên là như nhau.

Thí dụ 1: Tìm căn nguyên thuỷ đầu tiên lớn hơn 7 modulo 41.

```
[> primroot(7,41);
```

```
                              11
```

Vậy 11 là căn nguyên thuỷ lớn hơn 7 đầu tiên modulo 41.

Thí dụ 2: Tìm căn nguyên thuỷ đầu tiên lớn hơn 2 modulo 8.

```
[> primroot(2,8);
```

```
                                  FAIL
```

Vậy 8 không có căn nguyên thuỷ lớn hơn 2.

II. 6. Thực hành tính hàm $\tau(n)$

Để tính giá trị của hàm $\tau(n)$ tại *n* ta thực hiện dòng lệnh như sau:

```
[> tau(n);
```

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

Thí dụ 1: Tính $\tau(-9)$.

```
[> tau(-9);
```

```
                              3
```

Thí dụ 2: Tính $\tau(100)$.

```
[> tau(100);
```

```
                              9
```

Vậy số các ước dương của 100 là 9.

II. 7. Thực hành tính hàm σ(n)

Để tính giá trị của hàm $\sigma(n)$ tại *n* ta thực hiện dòng lệnh như sau:

```
[>sigma(n);
```

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

Thí dụ: Tính $\sigma(9)$.

```
[>sigma(9);
```

13

Vậy tổng các ước dương của 9 là 13.

II. 8. Thực hành tính đồng dư thức, giải phương trình đồng dư

1. Để tính đồng dư của *a* theo modulo *n* ta thực hiện dòng lệnh như sau:

```
[> a mod n;
```

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

Thí dụ: Tính $5^{1234567} \bmod 221$

```
[> 5&^1234567 mod 221;
```

112

2. Để giải phương trình đồng dư ta thực hiện dòng lệnh như sau:

```
[>msolve (các phương trình, modulo);
```

Sau dấu (;) ấn phím "Enter", nếu phương trình đồng dư có nghiệm màn hình sẽ hiện ra kết quả.

Thí dụ: Tìm nghiệm của đồng dư sau:

$$x^2+x+1 \equiv 0 \pmod 7$$

```
[>msolve(x^2+x+1=0,7);
```

x=4, x=2

Vậy nghiệm của phương trình là x=2, x=4(mod 7).