CẤP CỦA MỘT SỐ NGUYÊN THEO MODULO n

Trần Minh Hiền
Trường THPT chuyên Quang Trung, Bình Phước

Ngày 6 tháng 8 năm 2018

Như theo định lý Euler, ta có $a^{\varphi(n)} \equiv 1(\text{mod } n)$, với $(a,n)=1$ (Ở đây $\varphi(n)$ là hàm Euler đếm số các số tự nhiên nhỏ hơn và nguyên tố cùng nhau với n , ký hiệu (a,n) là ước chung lớn nhất của a và n). Tuy nhiên thường ta có một luỹ thừa của a, nhỏ hơn $\varphi(n)$ mà đồng dư với 1 theo modulo n . Từ đó đưa đến định nghĩa sau:

Định nghĩa 1 *Cho $n>1$ và $(a,n)=1$, cấp của a theo modulo n là số nguyên dương k nhỏ nhất sao cho $a^k \equiv 1(\text{mod}n)$*

Ta xét các luỹ thừa liên tiếp của 2 theo modulo 7. Với modulo này, ta nhận được các quan hệ đồng dư sau:

$$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1, 2^2 \equiv 2, 2^5 \equiv 4, 2^6 \equiv 1, \ldots$$

Từ trên suy ra 2 có cấp 3 theo modulo 7.

Nhận xét rằng nếu hai số nguyên đồng dư với nhau theo modulo n, thì chúng có cùng cấp(theo modulo n). Thật vậy nếu $a \equiv b(\text{mod } n)$ và $a^k \equiv 1(\text{mod } n)$, lại do $a^k \equiv b^k(\text{mod } n)$ nên suy ra $b^k \equiv 1(\text{mod } n)$.

Cũng chú ý là trong định nghĩa trên chúng ta chỉ xem xét các số nguyên a sao cho $(a,n)=1$. Thật vậy, nếu $(a,n)>1$ thì ta đã biết là phương trình đồng dư $ax \equiv 1(\text{mod } n)$ vô nghiệm, do đó mối quan hệ $a^k \equiv 1(\text{mod } n)(k>1)$ không thể xảy ra vì nếu xảy ra thì ta có $x=a^{k-1}$ là nghiệm của phương trình $ax \equiv 1(\text{mod } n)$. Do vậy khi nói về cấp của số nguyên a theo modulo n , thì luôn giả thiết rằng $(a,n)=1$.

Trong ví dụ trên ta thấy $2^k \equiv 1(\text{mod } 7)$ khi và chỉ khi k là bội của 3, với 3 là cấp của 2 theo modulo 7. Định lý đầu tiên sau đây sẽ chứng tỏ trong trường hợp tổng quát hơn.

Định lý 2 *Cho số nguyên a có cấp k theo modulo n . Thì $a^h \equiv 1(\text{mod } n)$ nếu và chỉ nếu $k|h$, đặc biệt ta có $k|\varphi(n)$.*

Chứng minh
Giả sử ta có $k|h$, thì $h=k.j$, với j là số nguyên. Bởi vì $a^k \equiv 1(\text{mod } n)$ nên $(a^k)^j \equiv 1^j(\text{mod } n)$ hay $a^h \equiv 1(\text{mod } n)$.
Ngược lại, giả sử là số nguyên thoả . Theo thuật toán Euclide thì tồn tại các số q,r sao cho $h=qk+r$, với $0 \leq r < k$. Vậy $a^h = (a^q)^k.a^r$, mà cả $a^h \equiv 1(\text{mod } n)$ và $a^k \equiv 1(\text{mod } n)$. Từ đó suy ra $a^r \equiv 1(\text{mod } n)$. Bởi vì $0 \leq r < k$ và k là số nguyên dương nhỏ nhất thoả $a^k \equiv 1(\text{mod } n)$. Vậy $r=0$ nên $k|h$.

Định lý 2 cho phép ta tiến hành tính toán bậc của một số nguyên a theo modulo n , thay vì phải xem xét tất cả các luỹ thừa của a , thì các luỹ thừa chỉ cần giới hạn là các ước của $\varphi(n)$. Để giải thích điều này, chúng ta tính cấp của 2 theo modulo 13. Vì $\varphi(13)=12$, do đó cấp của 2 phải là một trong các số 1, 2, 3, 4, 6, 12. Từ:

$$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 3, 2^6 \equiv 12, 2^{12} \equiv 1(\text{mod } 13)$$

Từ đây nhận thấy rằng 2 có cấp 12 theo modulo 13. Với một ước bất kỳ d của $\varphi(n)$, không phải lúc này chúng ta cũng chọn được một số nguyên a có cấp d theo modulo n . Ví dụ là lấy $n=12$ thì $\varphi(12)=4$, và sẽ không tồn tại một số nguyên nào có cấp 4 theo modulo 12, thật vậy, vì dễ dàng thấy:

$$1^1 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1(\text{mod } 12)$$

Và do đó chỉ có thể chọn được cấp là 1 hoặc 2. Dưới đây trình bày tiếp một tính chất cơ bản liên quan đến cấp của một số nguyên.

Định lý 3 *Nếu số nguyên a có cấp k theo modulo n , thì* $a^i \equiv a^j (\text{mod } n)$ *nếu và chỉ nếu* $i \equiv j (\text{mod } k)$.

Chứng minh
Đầu tiên giả sử rằng $a^i \equiv a^j (\text{mod } n)$, với $i \geq j$. Bởi vì a nguyên tố cùng nhau với n , nên ta có $a^{i-j} \equiv 1 (\text{mod } n)$. Theo định lý 2 thì ta có $k|i-j$, suy ra $i \equiv j (\text{mod } k)$
Ngược lại, giả sử $i \equiv j (\text{mod } k)$. Thì ta có $i = j + kq$, với q là một số nguyên. Theo định nghĩa của k, $a^k \equiv 1 (\text{mod } n)$. Do đó $a^i \equiv a^{j+kq} \equiv a^j.(a^k)^q \equiv a^j (\text{mod } n)$. Từ đó ta có điều phải chứng minh.

Từ kết quả trên ta có hệ quả sau:

Hệ quả 4 *Nếu a có cấp k theo modulo n, thì các số nguyên* $a, a^2, \ldots, a^k$ *không đồng dư với nhau theo modulo n*

Chứng minh
Nếu $a^i \equiv a^j (\text{mod } n)$ với $1 \leq i \leq j \leq k$, thì theo định lý trên suy ra $i \equiv j (\text{mod } k)$. Nhưng điều này chỉ có thể xảy ra kh $i = j$

Một câu hỏi tự nhiên được đặt ra là: Có thể mô tả được hay không cấp của bất kỳ luỹ thừa nào của a theo cấp của a. Câu trả lời nhận được trong định lý sau:

Định lý 5 *Nếu số nguyên a có cấp k theo modulo n và* $h > 0$*, thì* a^h *có cấp là* $\frac{k}{(h,k)}$ *theo modulo n*

Chứng minh
Đặt $d = (h, k)$, thì khi đó ta có thể viết $h = h_1.d$ và $k = k_1.d$, với $(h_1, k_2) = 1$. Rõ ràng:

$$(a^h)^{k_1} = (a^{h_1 d})^{k/d} = (a^k)^{h_1} \equiv 1 (\text{mod } n)$$

Nếu giả sử a^h có cấp r theo modulo n, thì theo định lý 2, phải có $r|k_1$. Mặt khác, bởi vì a có cấp k theo modulo n, nên từ đồng dư:

$$a^{hr} \equiv (a^h)^r \equiv 1 (\text{mod } n)$$

suy ra $k|hr$ hay $k_1 d|h_1 dr$, suy ra $k_1|h_1 r$. Nhưng $(k_1, h_1) = 1$, do đó $k_1|r$. Vậy $k_1 = r$, ta có điều phải chứng minh.
Từ định lý trên ta rút ra một hệ quả sau:

Hệ quả 6 *Cho số nguyên a có cấp k theo modulo n. Thì* a^h *cũng có cấp k nếu và chỉ nếu* $(h, k) = 1$

Chúng ta sẽ thấy kết quả của quá trình ở trên thông qua trường hợp đặc biệt sau:

Ví dụ 1 Bảng sau đây trình bày cấp của các số nguyên dương nhỏ hơn 13 theo modulo 13:
Chúng ta quan sát rằng cấp của 2 theo modulo 13 là 12, trong khi đó cấp của 2^2 và 2^3 là 6 và 4, tương ứng; dễ dàng nhận thấy rằng: $6 = \frac{12}{(2,12)}$ và $4 = \frac{12}{(3,12)}$. Theo đúng định lý trên, các số nguyên là luỹ thừa của 2 mà cũng có cấp 12 theo modulo 13 là các luỹ thừa 2^k mà $(k, 12) = 1$; cụ thể là:

$$2^1 \equiv 2, 2^5 \equiv 6, 2^7 \equiv 11, 2^{11} \equiv 7 (\text{mod } 13)$$

Nếu một số nguyên a có khả năng có cấp lớn nhất có thể, thì ta gọi nó là là một căn nguyên thuỷ của n.

Định nghĩa 7 *Nếu* $(a, n) = 1$ *và a có cấp* $\varphi(n)$ *theo modulo n, thì a là một căn nguyên thuỷ của số nguyên n*

Hay nói một cách khác, n có a là một căn nguyên thuỷ nếu $a^{\varphi(n)} \equiv 1 (\text{mod } n)$, nhưng $a^k \equiv 1 (\text{mod } 13)$ với mọi số nguyên $k < \varphi(n)$

Dễ dàng thấy rằng 3 là một căn nguyên thuỷ của 7, do:

$$3^1 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^4 \equiv 4, 3^5 \equiv 5, 3^6 \equiv 1 (\text{mod } 7)$$

Tổng quát hơn, chúng ta có thể chứng minh căn nguyên thuỷ tồn tại với bất kỳ modulo nguyên tố nào, và đây là một kết quả quan trọng cơ bản. Mặc dù có thể có căn nguyên thuỷ của n với cả n không phải là số nguyên tố(ví dụ, 2 là một căn nguyên thuỷ của 9 vì $2^{\varphi(0)} = 2^6 = 64 \equiv 1(\text{mod } 9)$). Cũng không có lý do gì để tin tưởng là mọi số nguyên n đều sở hữu 1 căn nguyên thuỷ, vì sự tồn tại của căn nguyên thuỷ phụ thuộc vào từng trường hợp đặc biệt hơn là một quy luật chung.

Ví dụ 2 Chúng ta chứng tỏ rằng nếu $F_n = 2^{2^n} + 1, n > 1$ là số nguyên tố, thì 2 không phải là căn nguyên thuỷ của F_n(Rõ ràng 2 là căn nguyên thuỷ của $5 = F_1$). Từ sự phân tích $2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1)$, ta có:

$$2^{2^{n+1}} \equiv 1(\text{mod } F_n)$$

Từ đó suy ra cấp của 2 theo modulo F_n không vượt quá 2^{n+1}. Nhưng với giả thiết F_n là số nguyên tố thì

$$\varphi(F_n) = F_n - 1 = 2^{2^n}$$

và bằng quy nạp đơn giản dễ dàng xác nhận được $2^{2^n} > 2^{n+1}$, với $n > 1$. Do vậy, cấp của 2 theo modulo F_n nhỏ hơn $\varphi(F_n)$. Do đó 2 không thể là căn nguyên thuỷ của của F_n

Một trong những tính chất quan trọng của căn nguyên thuỷ nằm ở định lý sau:

Định lý 8 *Cho $(a, n) = 1$ và $a_1, a_2, \ldots, a_{\varphi(n)}$ là các số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n. Nếu a là một căn nguyên thuỷ của n, thì*

$$a, a^2, \ldots, a^{\varphi(n)}$$

đồng dư theo modulo với n với $a_1, a_2, \ldots, a_{\varphi(n)}$ theo một thứ tự nào đó.

Chứng minh
Vì a nguyên tố cùng nhau với n, nên các luỹ thừa của a cũng nguyên tố cùng nhau với n. Do vậy, mỗi a^k đồng dư modulo với một số a_i nào đó. Mà ta đã biết $\varphi(n)$ số trong tập $a, a^2, \ldots, a^{\varphi(n)}$ không đồng dư với nhau, do vậy các luỹ thừa này phải đồng dư(không nhất thiết theo thứ tự xuất hiện) các số nguyên $a_1, a_2, \ldots, a_{\varphi(n)}$.

Một hệ quả của những gì chúng ta vừa chứng minh ở trên, là trong trường hợp căn nguyên thuỷ tồn tại, chúng ta sẽ biết chính xác nó có bao nhiêu căn nguyên thuỷ.

Hệ quả 9 *Nếu n có một căn nguyên thuỷ, thì nó có chính xác $\varphi(\varphi(n))$ căn nguyên thuỷ.*

Chứng minh
Giả sử a là một căn nguyên thuỷ của n. Theo định lý trên, các căn nguyên thuỷ khác của n được tìm trong tập hợp $a, a^2, \ldots, a^{\varphi(n)}$. Nhưng số các luỹ thừa $a^k, 1 \leq k \leq \varphi(n)$, mà có cấp $\varphi(n)$ bằng với số các số nguyên k sao cho $(k, \varphi(n)) = 1$. Và rõ ràng có $\varphi(\varphi(n))$ số k thoả mãn. Vậy có $\varphi(\varphi(n))$ căn nguyên thuỷ.

Kết quả trên có thể giải thích qua trường hợp $a = 2$ và $n = 9$. Bởi vì $\varphi(9) = 6$, sáu luỹ thừa đầu tiên của 2 phải đồng dư theo modulo 9, theo một thứ tự nào đó với các số nguyên dương nhỏ hơn 9 và nguyên tố cùng nhau với 9. Các số nguyên dương nhỏ hơn 9 và nguyên tố cùng nhau với 9 là 1, 2, 4, 5, 7, 8, và chúng ta nhìn thấy rằng:

$$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 7, 2^5 \equiv 5, 2^6 \equiv 1(\text{mod } 9)$$

Theo hệ quả trên thì chúng ta có chính xác $\varphi(\varphi(9)) = \varphi(6) = 2$ căn nguyên thuỷ của 9, và chúng là các số 2 và 5.

Bài tập

1. Tìm các cấp của 2, 3 và 5 theo:
a. modulo 17.
b. modulo 19.
c. modulo 23.

2. Chứng minh các khẳng định dưới đây:
a. Nếu a có cấp hk theo modulo n, thì a^h có cấp k theo modulo n.

b. Nếu a có cấp $2k$ theo modulo số nguyên tố lẻ p, thì $a^k \equiv -1 (\text{mod } p)$
c. Nếu a có cấp $n-1$ theo modulo n, thì n nguyên tố.
3. Chứng minh rằng $\varphi(2^n - 1)$ là bội của n với $n > 1$.
4. Giả sử cấp của a theo modulo n là h và cấp của b theo modulo n là k. Chứng tỏ rằng cấp của ab theo modulo n chia hết hk, đặc biệt nếu $(h, k) = 1$, thì ab có cấp hk.
5. Cho biết a có cấp 3 theo modulo p, với p là số nguyên tố lẻ, chứng tỏ $a + 1$ có cấp 6 theo modulo p.
6. Xác nhận các khẳng định sau:
a. Các ước nguyên tố lẻ của $n^2 + 1$ có dạng $4k + 1$.
b. Các ước nguyên tố lẻ của $n^4 + 1$ có dạng $8k + 1$.
c. Các ước nguyên tố lẻ của $n^2 + n + 1$ khác 3 có dạng $6k + 1$.
7. Chứng minh rằng tồn tại vô hạn các số nguyên tố có dạng $4k + 1, 6k + 1$ và $8k + 1$.
8. a. Chứng minh rằng nếu p và q là các số nguyên tố lẻ và $q|a^p - 1$, thì hoặc là $q|a - 1$ hoặc là $q = 2kp + 1$ với k là số nguyên.
b. Sử dụng phân a để chứng minh rằng nếu p là số nguyên tố lẻ, thì mọi ước nguyên tố lẻ của $2^p - 1$ có dạng $2kp + 1$.
c. Tìm ước nguyên tố lẻ nhỏ nhất của số $2^{17} - 1$ và $2^{29} - 1$.
9. Chứng minh rằng tồn tại vô hạn các số nguyên tố có dạng $2kp + 1$, với p là số nguyên tố lẻ.
10. a. Chứng tỏ 2 là căn nguyên thuỷ của 19, nhưng không phải là căn nguyên thuỷ của 17.
b. Chứng tỏ rằng 15 không có căn nguyên thuỷ bằng việc tính các cấp của 2, 4, 7, 8, 11, 13, và 14 theo modulo 15.
11. Cho r là một căn nguyên thuỷ của n. Chứng minh rằng r^k là căn nguyên thuỷ của n nếu và chỉ nếu $(k, \varphi(n)) = 1$.
12. a. Tìm căn nguyên thuỷ của 10.
b. Sử dụng thông tin 3 là căn nguyên thuỷ của 17 để nhận được 8 căn nguyên thuỷ của 17.
13. a. Chứng minh rằng nếu p và $q > 3$ là các số nguyên tố lẻ và $q|R_p$, thì $q = 2kp + 1$, với k nguyên.
b. Tìm các ước nguyên tố nhỏ nhất của $R_5 = 11111$ và $R_7 = 1111111$.
14. a. Cho $p > 5$ là số nguyên tố. Nếu R_n là số nhỏ nhất sao cho $p|R_n$, chứng tỏ $n|p - 1$. Ví dụ R_8 là số nhỏ nhất chia hết cho 73, và $8|72$.
b. Tìm R_n nhỏ nhất chia hết cho 13.