ORD' của số nguyên theo modulo n

Bài toán mở đầu.

Trước hết, ta xét ví dụ sau :

Tìm $a \in \mathbb{Z}^+, a > 1$ sao cho không tồn tại n lẻ lớn hơn 1 mà $(a^n + 1) \vdots n$.

Chứng minh.

Để ý rằng, n lẻ nên $(a^n + 1) \vdots (a + 1)$, nên nếu $a + 1$ có ước nguyên tố p lẻ thì $(a^p + 1) \vdots p$ (không thỏa mãn đề bài).

Do đó ta chỉ xét những số $a + 1$ không có ước nguyên tố p lẻ hay $a = 2^k - 1$.

Ta chứng minh, mọi số có dạng $a = 2^k - 1$ thì thỏa điều kiện đề bài.

Giả sử ngược lại, tồn tại n lẻ lớn hơn 1 sao cho $(a^n + 1) \vdots n$.

Do đó $a^n \equiv -1 (\text{mod } p) \Rightarrow a^{2n} \equiv 1 (\text{mod } p)$ (*)

Gọi p là ước nguyên tố lẻ nhỏ nhất của $n \Rightarrow a^{p-1} \equiv 1 (\text{mod } p)$ (theo định lý nhỏ Fermat).

Đặt $h = \text{ord}_p(a) \Rightarrow h \mid 2n, h \mid p - 1$ nên $h = 1 \vee h = 2$. (**)

Nếu $h = 1$ thì $a \equiv 1 (\text{mod } p) \Rightarrow a^n + 1 \equiv 2 (\text{mod } p)$, mâu thuẫn.

Nếu $h = 2$ thì $a^2 \equiv 1 (\text{mod } p) \Rightarrow a \equiv -1 (\text{mod } p) \Rightarrow 2^k \equiv 0 (\text{mod } p)$, mâu thuẫn.

Vậy bài toán được chứng minh.

Nhận xét.

Đây là một lời giải rất quen thuộc, hầu như đã trở thành một mô hình trong những bài toán số học sử dụng bậc để giải quyết. Tuy nhiên lập luận ở (*) đặt ra câu hỏi : tại sao lại phải bình phương (1) để đưa về cấp rồi xử lí, sau đó lại phải loại trường hợp ở (**). Chúng ta có thể giải trực tiếp khi mà $a^n \equiv -1 (\text{mod } p)$ không ?

Tại sao chúng ta không thử đưa ra kí hiệu ord' để hệ thống những bài toán như trên thành một lời giải ngắn gọn, giản đơn, hiệu quả hơn.

Ta xây dựng định nghĩa sau:

Định nghĩa.

Cho hai số tự nhiên a,p với (a,p)=1,p>1. Tồn tại số n sao cho $a^n \equiv -1 (\text{mod } p)$.

Ta kí hiệu $\text{ord}'_p(a)$ là số nhỏ nhất thỏa mãn : $2^{\text{ord}'_p(a)} \equiv -1 (\text{mod } p)$.

Tính chất của ord' mod p.

Với mọi $(a,p)=1, p>1$ thì rõ ràng luôn tồn tại $\text{ord}_p(a)$ tuy nhiên không phải lúc nào cũng tồn tại $\text{ord}'_p(a)$. Ta sẽ đi tìm điều kiện để tồn tại $\text{ord}'_p(a)$.

Dễ thấy, nếu tồn tại một số tự nhiên n>1 thỏa điều kiện : $a^n \equiv -1 (\text{mod } p)$ (*) thì hiển nhiên, $\text{ord}'_p(a)$ tồn tại. Tuy vậy, ý tưởng $\text{ord}'_p(a)$ ra đời chính từ $\text{ord}_p(a)$, cho nên ta sẽ trình bày điều kiện tồn tại $\text{ord}'_p(a)$ theo $\text{ord}_p(a)$.

Trước hết, ta chứng minh tính chất đẹp sau :

Tính chất 1.

Cho n là số nguyên tố và $a,n \in \mathbb{Z}^+, n>1, (a,n)=1$. Nếu tồn tại $\text{ord}'_n(a)=h'$ thì $\text{ord}_n(a)=2h'$.

Chứng minh.

Giả sử $2h'$ không phải $\text{ord}_n(a)$ (*). Đặt $d=\text{ord}_p(a)$.

Gọi p là ước nguyên tố nhỏ nhất của n.

Ta có : $a^{h'} \equiv -1 (\text{mod } p) \Rightarrow a^{2h'} \equiv 1 (\text{mod } p)$.

Hay $2h' \vdots d$ nhưng để ý rằng, d lẻ nên $h' \vdots d$. Ta có

$$a^{h'-d} \cdot a^d \equiv a^{h'} \equiv -1 (\text{mod } p) \Rightarrow a^{h'-d} \equiv -1 (\text{mod } p) \text{ (vô lí).}$$

Vậy $\text{ord}_n(a)=2h'=2\text{ord}'_n(a)$.

Ta đưa đến điều kiện sau :

Tính chất 2.

Với $a,n \in \mathbb{Z}^+, n>1.(a,n)=1$. Nếu $\text{ord}_n(a) \equiv 0 (\text{mod } 2) \Rightarrow \exists \text{ord}'_n(a)$.

Chứng minh.

Đặt $h'=\dfrac{\text{ord}_n(a)}{2} \Rightarrow a^{h'} \equiv -1 (\text{mod } n)$. Mặt khác h' cũng chính là $\text{ord}'_n(a)$ vì : nếu h' không phải, tồn tại $\text{ord}'_n(a)=d \neq h'$.

Theo tính chất 1 thì $2d=\text{ord}_n(a)$ (vô lí).

Do đó, $h' = \text{ord}'_n(a)$.

Tính chất 3.

Nếu như $\text{ord}_n(a)$ có tính chất : nếu tồn tại m thỏa : $a^m \equiv 1 (\text{mod } p)$ thì $m \vdots \text{ord}_n(a)$ hay $m = k \cdot \text{ord}_n(a), k \in \mathbb{Z}^+$. Ta đặt ra câu hỏi : tính chất này có còn đúng với $\text{ord}'_n(a)$ hay không ?

Và câu trả lời là có: đặc biệt là $k = 2t+1, t \in \mathbb{Z}^+$.

Chứng minh tính chất này rất đơn giản, tư tưởng chính là biểu diễn $m = pq + r$ và thay vào đồng dư thức, ta đưa đến đpcm.

Tính chất 4.

Một câu hỏi mở rộng nữa khá thú vị cho $\text{ord}'_n(a)$ đó là : liệu có xét được tính chẵn lẻ của $\text{ord}'_n(a)$ dựa vào a, n hay không ?

Trước mắt, ta có một kết quả khá đẹp, đó là : Nếu n là một số nguyên dương có dạng $4k+3, k \in \mathbb{Z}^+$ thì nếu tồn tại $\text{ord}'_n(a)$ thì $\text{ord}'_n(a)$ lẻ.

Chứng minh.

Hoàn toàn dựa trên bài toán quen thuộc đã tìm hiểu : $x^2 + 1$ không có ước nguyên tố dạng 4k+3.

Thêm một mệnh đề nữa khá thú vị, có ứng dụng ở một mức độ nào đó, mà phát biểu hoàn toàn không liên quan đến $\text{ord}'_n(a)$, tuy nhiên lại là hệ quả từ tính chất của $\text{ord}'_n(a)$. Đó là :

Tính chất 5.

Với $(a, n) = 1, n > 1$: $a^n \equiv -1 (\text{mod } n)$ thì $a^{\left(n; \frac{p-1}{2}\right)} \equiv -1 (\text{mod } p)$ với p là một ước nguyên tố của n.

Chứng minh.

Đặt h′=$\text{ord}'_n(a)$. Dễ thấy $h' \mid n$ và $2h' \mid p-1$ nên $\left(n; \frac{p-1}{2}\right) \vdots h'$.

Theo tính chất lựa chọn p thì suy ra đpcm.

Dưới đây ta sẽ cùng xem xét một ví dụ minh họa:

Bài toán.

Tìm p,q nguyên tố thỏa mãn $q^2+1 \mid 2003^p+1$ và $p^2+1 \mid 2003^q+1$.

Lời giải.

Không mất tính tổng quát, ta xét 2 trường hợp :

i) Nếu $p=2$.

Ta có $5 \mid 2003^q+1$ nên $2003^q \equiv -1 (\mathrm{mod}\, 5)$.

Hơn nữa $2003^q \equiv (-2)^q (\mathrm{mod}\, 5)$ nên $q=2$ đúng.

Với $q>2$ thì $2003^q \equiv (-2)^q \equiv (-2).4^{\frac{q-1}{2}} \equiv (-2).(-1)^{\frac{q-1}{2}} (\mathrm{mod}\, 5)$, ta được

$$2003^q \neq -1 (\mathrm{mod}\, 5).$$

Do đó, $(p,q)=(2,2)$ là một nghiệm cần tìm.

ii) Nếu $q>p>2$.

Xét r là ước số nguyên tố lẻ nhỏ nhất của p^2+1(*).

Vì $p^2+1 \mid 2003^q+1$ nên $r \mid 2003^q+1$. Đặt $h'=\mathrm{ord}'_r(2003)$.

Ta có $2003^q \equiv -1 (\mathrm{mod}\, r)$ nêu $h' \vdots q$.

Mặt khác thì $h' \vdots (q;\frac{r-1}{2})$ nên $h' \leq \frac{r-1}{2} < r \leq \left[\sqrt{p^2+1}\right] < q$ kết hợp q nguyên tố nên $h'=1$.

Thay vào, ta được $2004 \equiv 0 (\mathrm{mod}\, r)$. Mà $2004=2^2 \cdot 3 \cdot 167$ nên suy ra $r=3$ hoặc $r=167$. Để ý, (*) tương đương r không có dạng $4k+3$ nên mâu thuẫn.

Nếu $r=2$ thì dễ thấy không thỏa.

Vậy bộ nghiệm duy nhất cần tìm là $(p,q)=(2,2)$.

Bài tập tự giải.

1. Tìm n nguyên dương thỏa mãn : $2^{n+1}+1 \vdots n+1$.

2. Tìm n nguyên dương thỏa mãn: $2^{n+1}+1 \vdots n^2$.

3. Tìm số n nguyên dương thỏa mãn: $2^n+2 \vdots n$.

4. Tìm bộ các số (p,q) nguyên tố thỏa mãn $2^p+2^q \vdots pq$.

5. Gọi F_n là số Fermat thứ n và p là ước nguyên tố của F_n. Chứng minh rằng

$$p \equiv -1 (\mathrm{mod}\, 2^{n+2}).$$

6. Tìm bộ ba các số nguyên dương (p,q,r) thỏa mãn $r \mid p^q + 1, p \mid q^r + 1, q \mid r^p + 1$.

7. Tìm bộ ba các số (a,b,c) đôi một nguyên tố cùng nhau thỏa điều kiện

$$2^a + 1 \vdots b,\ 2^b + 1 \vdots c,\ 2^c + 1 \vdots a.$$

Mở rộng vấn đề.

- Ngoài hai điều kiện về sự tồn tại của ord' với $(a,p) = 1, p > 1$ xác định đã nêu ở trên, liệu có một điều kiện nào đó rõ ràng hơn, chỉ ra tồn tại ord' dựa vào cặp (a,p) cho trước hay không ?
- Khi đã xác định được sự tồn tại của ord', từ tính chất 4 đưa đến một câu hỏi: có thể khảo sát tính chẵn lẻ của ord' hay không nếu p là số nguyên dương không có dạng $4k+3$?
- Một ý tưởng thú vị hơn: Nếu đã có thể tìm hiểu về ord và ord' tương ứng với đồng dư $1, -1$ theo một modulo nào đó, vậy khi đồng dư với số x bất kì sẽ như thế nào ? Có tồn tại một dạng tương tự ord, ord' hay không? Và tính chất có thú vị hơn không?