CẤP CỦA MỘT SỐ VÀ ỨNG DỤNG

(Lê Xuân Đại, GV THPT Chuyên Vĩnh Phúc, tỉnh Vĩnh Phúc)

Cho n là một số nguyên dương, $n>1$ và a là một số nguyên với $(a,n)=1$. Số nguyên dương h nhỏ nhất sao cho $a^h \equiv 1 (\text{mod } n)$ được gọi là cấp của a modulo n, ký hiệu $h= \text{ord}_n a$. Theo định lý Ơle ta có $a^{\varphi(n)} \equiv 1 (\text{mod } n)$ do đó số h nói trên là tồn tại . Rõ ràng là $h \le \varphi(n)$.

Đặc biệt nếu $h = \varphi(n)$ thì a được gọi là một căn nguyên thuỷ (mod n) .

Tính chất cơ bản sau đây hay được sử dụng trong bài viết

Nếu cấp của a (mod n) là h thì

(a). $a^k \equiv 1 (\text{mod } n) \Leftrightarrow k \vdots h \quad (k \in \mathbb{N})$

(b). $a^k \equiv a^\ell (\text{mod } n) \Leftrightarrow k - \ell \vdots h \quad (k; \ell \in \mathbb{N})$

Trong các bài toán có sử dụng cấp của một số ta thường kết hợp thêm với định lý Fecmat và định lý Ơle để tạo thêm các quan hệ đồng dư.

Sau đây là một số thí dụ minh hoạ.

Bài toán 1. Cho số nguyên dương n thoả mãn $3^n - 1 \vdots n$. Chứng minh rằng n chẵn.

Lời giải. Gọi p là ước số nguyên tố nhỏ nhất của n, ta cần chứng minh $p=2$.

Gọi h là cấp của 3 (mod p), ta có $\begin{cases} 3^n \equiv 1 (\text{mod } p) \\ 3^h \equiv 1 (\text{mod } p) \end{cases} \Rightarrow h \setminus n$ (kí hiệu $h \setminus n$ nếu n chia hết cho h)

Rõ ràng là $p \ne 3$. Theo định lý Fecmat thì $3^{p-1} \equiv 1 (\text{mod } p)$, suy ra $h \setminus p-1$

Nếu $h>1$ thì tồn tại q là ước nguyên tố của h. Khi đó $q \setminus n$ và $p > p-1 \ge h \ge q$, mâu thuẫn với p là ước nguyên tố nhỏ nhất của n.

Vậy $h=1$, khi đó $p=2$. Do đó n là số chẵn (đpcm).

Bài toán 2. Tìm số nguyên dương n nhỏ nhất sao cho $17^n - 1$ chia hết cho 2^{2011}.

Lời giải. Số n cần tìm chính là cấp của 17 (mod 2^{2011}). Ta có $\varphi(2^{2011}) = 2^{2010}$ nên $n \setminus \varphi(2^{2011}) = 2^{2010}$.

Do đó n có dạng $n = 2^k;\ k \in \{1;2;...;2010\}$. Ta có

$$\begin{aligned} 17^{2^k} - 1 &= (17-1)(17+1)(17^2+1)(17^{2^2}+1)...(17^{2^{k-1}}+1) \\ &= 2^4.(17+1)(17^2+1)(17^{2^2}+1)...(17^{2^{k-1}}+1) \end{aligned}$$

Có k thừa số có dạng $(17^{2^m}+1)$ chia hết cho 2 nhưng không chia hết cho 4 nên số mũ của 2 trong $17^{2^k} - 1$ bằng $4+k$, suy ra $4 + k = 2011 \Rightarrow k = 2007$.

Vậy số n cần tìm là $n = \text{ord}_{2^{2011}}(17) = 2^{2007}$.

Bài toán 3. Chứng minh rằng mọi ước nguyên tố của số $F_n = 2^{2^n} + 1$ $(n \in \mathbb{N})$ đều đồng dư với 1 theo mođun 2^{n+1}. (Số F_n được gọi là số Fecmat thứ n).

Lời giải. Gọi p là một ước nguyên tố bất kì của F_n, suy ra $2^{2^{n+1}} \equiv 1 (\text{mod } p)$.

Gọi h là cấp của 2 (mod p), ta có $2^h \equiv 1 (\text{mod } p)$ và $h \setminus 2^{n+1} \Rightarrow h = 2^k \ (k \in \mathbb{N}; 1 \le k \le n+1)$ (1)

Vì F_n lẻ nên p lẻ, theo định lý Fecmat ta được $2^{p-1} \equiv 1 (\text{mod } p) \Rightarrow h \setminus p-1$ (2)

Từ (1) và (2) giúp ta định hướng cần chứng minh rằng $h = 2^{n+1}$.

Thậy vậy, nếu $k \le n$ thì $2^{2^n} - 1 \vdots 2^h - 1 \vdots p$, nhưng $2^{2^n} + 1 \vdots p$ nên $2 \vdots p$ (vô lý).

Vậy $k = n+1$, tức là $h = 2^{n+1}$. Do đó $p \equiv 1 (\text{mod } 2^{n+1})$ (đpcm).

Nhận xét: 1. Ta có thể chứng minh một kết quả mạnh hơn là $p \equiv 1 (\text{mod } 2^{n+2})$ với $n \ge 2$ nếu sử dụng thêm tính chất của số chính phương môđun nguyên tố.

Thật vây, theo kết quả trên thì $p - 1 \vdots 2^{n+1} \Rightarrow p = 8k+1 \ (k \in \mathbb{N}^*)$.

Khi đó thì 2 là số chính phương mod p, suy ra $2^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$

Nhưng $h = 2^{n+1}$ lại là cấp của 2 (mod p) nên $\frac{p-1}{2} \vdots 2^{n+1} \Rightarrow p - 1 \vdots 2^{n+2}$.

2. Cũng từ kết quả bài toán trên ta suy ra rằng có vô hạn số nguyên tố dạng $2^n.k+1 \ (k \in \mathbb{N}^*)$ với n là một số tự nhiên cho trước (chứng minh dành cho bạn đọc).

Bài toán 4. Có bao nhiêu số nguyên dương n là bội số của 1001 và biểu diễn được dưới dạng $n = 10^j - 10^i$ với $i, j \in \mathbb{N}; \ 0 \le i < j \le 99$.

Lời giải. Ta có $n = 10^j - 10^i = 10^i (10^{j-i} - 1)$ và 1001=7.11.13 là số nguyên tố cùng nhau với 10^i.

Suy ra $10^{j-i} \vdots 1001 \Leftrightarrow 10^{j-i} \equiv 1 (\text{mod } 1001)$. Dễ thấy $\text{ord}_{1001}(10) = 6 \Rightarrow j - i \vdots 6 \Rightarrow j - i = 6m (m \in \mathbb{N}^*)$.

Như vậy số các số n bằng số các bộ $(i; j)$ thoả mãn phương trình $i + 6m = j$ (*) với $0 \le i < j \le 99; m \in \mathbb{N}^*$.

Dễ thấy là với mỗi $m \in \{1; 2; ...; 16\}$ sẽ có $100 - 6m$ giá trị của i (và j). Vậy số nghiệm của phương trình (*) là

$$\sum_{m=1}^{16} (100 - 6m) = 784.$$

Vậy có 784 số n thoả mãn đề bài.

Bài tương tự: Có bao nhiêu số nguyên dương n là bội số của 2011 và biểu diễn được dưới dạng $n = 10^j - 10^i$ với $i, j \in \mathbb{N}; \ 0 \le i < j \le 99$.

Bài toán 5. Chứng minh rằng với mỗi số n nguyên dương thì $3^n - 2^n$ không chia hết cho n.

Lời giải. Giả sử tồn tại n sao cho $3^n - 2^n$ chia hết cho n. Gọi p là ước nguyên tố nhỏ nhất của n, dễ thấy $p \ge 5$. Gọi a là một số nguyên dương sao cho $2a \equiv 1 (\text{mod } p)$ (1) (Số a như vậy luôn tồn tại)

Từ $3^n \equiv 2^n (\text{mod } p) \Rightarrow (3a)^n \equiv 1 (\text{mod } p)$. Gọi h là cấp của $3a$ (mod p), ta có $\begin{cases} h \setminus n \\ h \setminus p-1 \end{cases} \Rightarrow \begin{cases} h \setminus n \\ h < p \end{cases} \Rightarrow h = 1.$

Từ đó $3a \equiv 1 \pmod{p}$ (2).

Từ (1) và (2) suy ra $a \vdots p$, mâu thuẫn với (1). Vậy bài toán được chứng minh.

Nhận xét: Việc chọn *a* thoả mãn (1) nhằm mục đích tạo ra quan hệ đồng dư $(3a)^n \equiv 1 \pmod{p}$. Tất nhiên việc chọn được số *a* như vậy là một điều không được tự nhiên cho lắm. Ta sẽ xét thêm một bài toán nữa có sử dụng kĩ thuật này.

Bài toán 6. Tìm tất cả các số nguyên tố *p* và *q* sao cho $(5^p - 2^p)(5^q - 2^q)$ chia hết cho pq.

Lời giải. Dễ thấy ngay p và q đều khác 2 và 5, có thể giả sử $p \geq q$.

Nếu *p*=3 thì *q*=3, ta thấy $(p,q) = (3,3)$ thoả mãn.

Nếu $p \geq q > 5$ thì kết hợp với $(5^p - 2^p, p) = (5^q - 2^q, q) = 1$ ta được $\begin{cases} 5^p - 2^p \vdots q \\ 5^q - 2^q \vdots p \end{cases}$

Theo định lý Fecmat thì $5^p \equiv 5 \pmod{p}; 2^p \equiv 2 \pmod{p}$ nên $p > q$, suy ra $(p, q-1) = 1$ (*)

Gọi *a* là số tự nhiên sao cho $2a \equiv 5 \pmod{q}$ (1), ta được $a^p \equiv 1 \pmod{q}$.

Gọi *h* là cấp của *a* (mod *q*) thì $h \backslash p$. Từ (1) suy ra $(a,q) = 1 \Rightarrow a^{q-1} \equiv 1 \pmod{q} \Rightarrow h \backslash q-1 \Rightarrow (p, q-1) > 1$ (chú ý là $h \neq 1$). Điều này mâu thuẫn với (*).

Nếu $q = 3$, ta có $(5^p - 2^p)(5^3 - 2^3) \vdots 3p \Rightarrow 39(5^p - 2^p) \vdots p \Rightarrow 39 \vdots p \Rightarrow p = 3;13$

Vậy các cặp (p,q) cần tìm là $(p,q) = (3,3); (3,13); (13,3)$.

Bài toán 7. Cho hai số nguyên dương *m* và *n* (*n*>1) sao cho $1 + m^{3^n} + m^{2.3^n}$ chia hết cho *n*. Chứng minh rằng *n*=3.

Lời giải. Từ giả thiết suy ra $m^{3^{n+1}} - 1 \vdots n$. Gọi *h* là cấp của *m* (mod *n*) thì $h \backslash 3^{n+1} \Rightarrow h = 3^k (k \in \mathbb{N}; k \leq n+1)$.

Nếu $k \leq n$ thì $h \backslash 3^n \Rightarrow n \backslash m^{3^n} - 1$. Kết hợp với $n \backslash 1 + m^{3^n} + m^{2.3^n}$, suy ra *n*=3.

Nếu $h = 3^{n+1}$ thì do $h \backslash \varphi(n) \Rightarrow h < n \Rightarrow 3^{n+1} < n$, vô lí.

Nhận xét: Do *n*=3 nên dễ suy ra rằng khi đó $m \equiv 1 \pmod{3}$.

Bài toán 8 . Tìm các số nguyên tố phân biệt *p* và *q* sao cho $a^{3pq} \equiv a \pmod{3pq}$ với mọi số nguyên dương *a*.

Lời giải. Ta có thể giả sử $p > q$. Cho *a*=3 ta được

$$3^{3pq} \equiv 3 \pmod{3pq} \Rightarrow 3(3^{3pq-1} - 1) \vdots 3pq \Rightarrow p, q > 3.$$

Tiếp theo ta chọn *a* là căn nguyên thuỷ mod *p*, ta có $a^{p-1} \equiv 1 \pmod{p}$

Từ $a^{3pq} \equiv a \pmod{p} \Rightarrow a^{3pq-1} \equiv 1 \pmod{p} \Rightarrow p-1 \backslash 3pq-1 \Rightarrow p-1 \backslash 3q-1$ (1)

Tương tự ta cũng có $q-1 \backslash 3p-1$ (2)

Mà $p \geq q$ nên từ (1) dễ thấy rằng chỉ xảy ra $3q-1 \in \{p-1; 2(p-1); 3(p-1)\}$.

Bằng cách thử trực tiếp các trường hợp ta tìm ra hai bộ (*p*,*q*) là (17,11) và (11,17).

Nhận xét: Ở bước chọn *a* thứ hai ta muốn có (*a*,*p*)=1 để được $a^{p-1} \equiv 1 \pmod{p}$, nhưng ta muốn thêm rằng $p-1$ là cấp của *a* (mod *p*), như vậy *a* sẽ là căn nguyên thuỷ mod *p*. Khi đó ta có một quan hệ rất tốt là $p-1 \backslash 3pq-1$ như ở trên.

Cuối cùng là một số bài tập cho các bạn luyện tập.

Bài 1. Tìm tất cả các số nguyên dương *n* sao cho $2^n - 1 \vdots n$.

Bài 2. Tìm tất cả các số nguyên dương *n* sao cho $2^n + 1 \vdots n^2$.

Bài 3. Chứng minh rằng $n \backslash \varphi(a^n - 1)$ với mọi số nguyên dương *a* và *n*.

Bài 4. Tìm tất cả các số nguyên dương *n*, *n*<1000 sao cho *n* có dạng $n = p_1 p_2 p_3$ (p_1, p_2, p_3 là các số nguyên tố phân biệt) và $2^n + 2 \vdots n$.

Bài 5. Cho *n* nguyên dương có dạng $n = 2^k + 1$; *k*>1. Chứng minh rằng điều kiện cần và đủ để *n* nguyên tố là tồn tại số nguyên dương *a*>1 sao cho $a^{\frac{n-1}{2}} + 1 \vdots n$.