CẤP VÀ CĂN NGUYÊN THỦY

Lê Xuân Đại

(GV THPT Chuyên Vĩnh Phúc, Tỉnh Vĩnh Phúc)

MỞ ĐẦU

Đối với phân môn số học trong chương trình THPT Chuyên thì lý thuyết về cấp của một phần tử là một vấn đề cơ bản và rất quan trọng, nó có rất nhiều ứng dụng trong các bài toán số học. Việc sử dụng thành thạo các tính chất về cấp cùng sự kết hợp khéo léo thêm các định lý cơ bản của số học như định lý Euler, Fermat, Thặng dư Trung Hoa,… sẽ giúp chúng ta giải quyết được các bài toán hay và khó trong số học. Về lý thuyết thì khái niệm và các tính chất của cấp rất đơn giản nhưng biết sử dụng cấp trong các bài toán cụ thể lại là một việc gặp nhiều khó khăn.

Bài viết này trình bày các vấn đề cơ bản về cấp và căn nguyên thủy, đưa ra một số bài toán áp dụng điển hình nhất mà chủ yếu được lấy từ các bài thi Olympic về số học những năm gần đây. Với mỗi bài toán tác giả cố gắng phân tích, định hướng lời giải và đưa thêm một số bài toán tương tự. Tác giả hy vọng bài viết này sẽ là một tài liệu tham khảo bổ ích cho các thầy cô và học sinh chuyên toán. Rất mong sẽ nhận được những góp ý quý báu của các chuyên gia, các thầy cô giáo để chuyên đề được xâu sắc và hoàn thiện hơn nữa. Xin chân thành cảm ơn!

NỘI DUNG

A- Tóm tắt lý thuyết.

I. Cấp của một số

1.1. Định nghĩa . Cho $n \in \mathbb{N}^*, a \in \mathbb{Z}$, $(a,n)=1$, khi đó $a^{\varphi(n)} \equiv 1 (\bmod n)$. Do đó phương trình $a^x \equiv 1 (\bmod n)$ luôn có nghiệm nguyên. Số nguyên dương h nhỏ nhất thỏa mãn $a^h \equiv 1 (\bmod n)$ được gọi là cấp của a (mod$n$). Ký hiệu $h = ord_n(a)$, hiển nhiên $h \le \varphi(n)$.

1.2. Tính chất

Tính chất 1.2.1. Nếu a là cấp là h (mod$n$) thì mọi số thuộc lớp $\overline{a}$ đều có cấp là h (mod$n$).

Tính chất 1.2.2. Nếu cấp của a (mod n) là h thì

$$a^k \equiv 1 (\bmod n) \Leftrightarrow k \vdots h \quad (k \in \mathbb{N}) \text{ và } a^k \equiv a^\ell (\bmod n) \Leftrightarrow k - \ell \vdots h$$

Tính chất 1.2.3. Nếu a có cấp là h (mod$n$), $k \in \mathbb{N}^*$, $(k,h)=1$ thì a^k cũng có cấp là h (mod$n$).

Tổng quát hơn. Nếu a có cấp là h (mod$n$), $k \in \mathbb{N}^*$ thì a^k sẽ có cấp là $\dfrac{h}{\gcd(k,h)}$ (mod$n$).

Tính chất 1.2.4. Nếu a có cấp h_1 (mod$n$); b có cấp h_2 (mod$n$) và $(h_1,h_2)=1$. Khi đó cấp của ab (mod$n$) là $h = h_1h_2$.

Tính chất 1.2.5. Nếu a có cấp là h (mod$n$) thì hệ $A = \{1; a; a^2, ...; a^{h-1}\}$ gồm h số đôi một không đồng dư với nhau (mod$n$).

Tính chất 1.2.6. Cho các số $n_1, n_2, ..., n_k$ nguyên tố sánh đôi và $n = n_1n_2...n_k$. Giả sử a có cấp h_i (mod n_i), Khi đó cấp của a (mod$n$) là $h = lcm\{h_1, h_2, ...h_k\}$.

Nhận xét. Từ tính chất này cho phép ta đưa việc tìm cấp của a (mod$n$) quy về tìm cấp của a (mod p^α), p nguyên tố.

II. Căn nguyên thuỷ.

2.1. Định nghĩa. Cho *n* là số nguyên dương và *a* là số nguyên sao cho $(a,n)=1$. Khi đó *a* được gọi là <u>*một căn nguyên thuỷ*</u> (mod*n*) nếu cấp của *a* (mod*n*) bằng $\varphi(n)$. Ta còn nói *a* là một căn nguyên thuỷ của *n*. (*a* is called a primitive root modulo *n*).

Ví dụ. Chứng minh rằng nếu số $F_n = 2^{2^n}+1$, *n*>1, là số nguyên tố thì 2 không là căn nguyên thuỷ của F_n.

Lời giải. Ta phải xét *n*>1 vì với *n*=1 thì $F_1 = 5$ và 2 là một căn nguyên thuỷ của 5.

Ta có ngay $2^{2^{n+1}}-1=\left(2^{2^n}-1\right)\left(2^{2^n}+1\right)\Rightarrow 2^{2^{n+1}}\equiv 1 \pmod{F_n}$, do đó cấp của 2 $(\bmod F_n)$ không vượt quá 2^{n+1}. Từ F_n nguyên tố nên $\varphi(F_n)=F_n-1=2^{2^n}$ và $2^{2^n}>2^{n+1}$ ta suy ra 2 không là căn nguyên thuỷ của F_n (đpcm).

2.2. Tính chất.

Tính chất 2.2.1. Nếu *a* là căn nguyên thuỷ mod*n* thì mọi số cùng lớp với *a* theo mod*n* đều là căn nguyên thủy mod*n*.

Tính chất 2.2.2. Nếu *a* là căn nguyên thuỷ (mod*n*) thì hệ $A=\left\{a^1;a^2,...;a^{\varphi(n)}\right\}$ là hệ thặng dư thu gọn (mod*n*). Từ đó suy ra $1;a;a^2,...;a^{p-2}$ là $(p-1)$ số phân biệt và chúng là hoán vị của $1,2,3,...,p-1 \pmod p$. Đây là ***tính chất quan trọng*** và hay được ***sử dụng nhiều nhất***.

Tính chất 2.2.3. Nếu a là căn nguyên thủy của p^m thì a hoặc $a+p^m$ là căn nguyên thủy của p^{m+1}.

Tính chất 2.2.4. Mọi số nguyên tố *p* đều có căn nguyên thuỷ.

Đây có lẽ là một tính chất cơ bản và quan trọng bậc nhất của lý thuyết cấp của phần tử. Xin đưa ra hai chứng minh cho tính chất này.

Chứng minh 1. Với *p*=2 thì mệnh đề là hiển nhiên

Giả sử *p* là số nguyên tố lẻ và $\varphi(p)=p-1$. Dạng phân tích tiêu chuẩn của $\varphi(p)$ là:

$$\varphi(p)=q_1^{\alpha_1}.q_1^{\alpha_2}...q_k^{\alpha_k}\ .$$

Xét phương trình đồng dư: $x^{\frac{p-1}{q_i}} \equiv 1 \pmod{p}$ có không quá $\frac{p-1}{q_i}$ nghiệm, và $\frac{p-1}{q_i} < p-1$ cho nên với mỗi q_i phải tồn tại a_i, $(a_i, p) = 1$ sao cho $a_i^{\frac{p-1}{q_i}} \neq 1 \pmod{p}$.

Đặt $b_i = a_i^{\frac{p-1}{q_i^{\alpha_i}}}$. Ta sẽ chứng minh rằng cấp của b_i modp là $q_i^{\alpha_i}$. Thật vậy, ta có $b_i^{q_i^{\alpha_i}} = a_i^{p-1} \equiv 1 \pmod{p}$ cho nên cấp của b_i modp có dạng $q_i^{\beta_i}; 0 < \beta_i \leq \alpha_i$

Nhưng với mọi $\beta < \alpha_i$ thì $b_i^{q_i^{\beta}} = a_i^{\frac{p-1}{q_i^{\alpha_i - \beta}}} \neq 1 \pmod{p}$ cho nên ta có $\beta_i = \alpha_i$ nghĩa là $q_i^{\alpha_i}$ là cấp của b_i modp. Như vậy các số $b_1, b_2, ..., b_k$ lần lượt có cấp là $q_1^{\alpha_1}, q_2^{\alpha_2}, ..., q_k^{\alpha_k}$ theo mod*p*.

Do đó $b = b_1 b_2 ... b_k$ sẽ có cấp là $q_1^{\alpha_1}.q_1^{\alpha_2}...q_k^{\alpha_k}$ modp, tức *b* có cấp chính là $\varphi(p)$ mod*p*.

Vậy *b* là một căn nguyên thuỷ mod*p* (đpcm).

Nhận xét. Khi *p* là số nguyên tố thì *p* sẽ có đúng $\varphi(p-1)$ căn nguyên thủy.

Chứng minh 2 (**Sử dụng định lý Lagrange**).

Ta đã biết rằng với mọi $a \in \{0,1,2,...,p-1\}$ thì $ord_a(p) \mid \varphi(p) = p-1$. Ta sẽ xét tất cả các giá trị có thể của $ord_a(p)$.

Với mỗi $d \mid p-1$, gọi $f(d)$ là số các số nguyên dương trong tập $\{0,1,2,...,p-1\}$ nhận *d* làm cấp theo mod*p*. Suy ra $\sum_{d|p-1} f(d) = p-1$. Từ tính chất của hàm Euler ta có

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

Do đó $\sum_{d|p-1} f(d) = \sum_{d|p-1} \varphi(d)$. Ta sẽ chỉ ra $f(d) \leq \varphi(d)$ để từ đó dẫn đến $f(d) = \varphi(d)$ với mọi $d \mid p-1$.

Rõ ràng ta chỉ cần xét $f(d) \geq 1$, khi đó tồn tại *a* nguyên dương mà $ord_p(a) = d$.

Xét đa thức $P(x) = x^d - 1$, theo định lý Lagrange thì $P(x)$ có tối đa *d* nghiệm theo mod*p*.

Mặt khác $a^1, a^2, ..., a^d$ là *d* nghiệm phân biệt của $P(x)$ nên đó chính là tất cả các nghiệm

của $P(x)$ theo mod*p*. Vậy có tối đa *d* số $a^1, a^2, ..., a^d$ nhận *d* làm cấp.

Dễ thấy với $(k,d)>1$ thì $\left(a^k\right)^{\frac{d}{(k,d)}} \equiv 1 \pmod p$ nên a^k không nhận *d* làm cấp. Do đó, số các số còn lại nhận *d* làm cấp không vượt quá $\varphi(d)$, suy ra $f(d) \le \varphi(d)$.

Vậy $f(d) = \varphi(d)$ với mọi $d \mid p-1$. Đặc biệt ta được $f(p-1) = \varphi(p-1) \ge 1$. Như vậy tồn tại căn nguyên thủy mod*p* và không những vậy ta còn suy ra có đúng $\varphi(p-1)$ căn nguyên thủy mod*p*.

Nhận xét. Bằng phép chứng minh tương tự như trên ta cũng suy ra nếu *n* nguyên dương có căn nguyên thủy thì *n* sẽ có đúng $\varphi(\varphi(n))$ căn nguyên thủy.

Tính chất 2.2.5 (Định lý về sự tồn tại căn nguyên thuỷ).

Các số $2, 4, p^k, 2p^k$ với *p* là số nguyên tố lẻ, *k* là số nguyên dương, và chỉ các số đó có căn nguyên thuỷ. Định lý này sẽ được chứng minh chi tiết ở phần cuối của bài viết này.

B- Một số bài toán áp dụng

Bài toán 1 (Hungary-Israel Math Competition 2009). Cho số nguyên tố *p*. Tìm tất cả các số nguyên dương *k* sao cho $S_k = 1^k + 2^k + ... + (p-1)^k$ chia hết cho *p*.

Lời giải. Do *p* nguyên tố nên tồn tại *x* là căn nguyên thủy mod*p*. Khi đó

$$S_k \equiv 1 + x^k + ... + x^{(p-2)k} \pmod p \quad (*)$$

Nếu $(p-1) \mid k$ thì $S_k \equiv 1 + 1 + ... + 1 \equiv p-1 \pmod p$.

Nếu $(p-1) \nmid k$ thì từ $x^k \not\equiv 1 \pmod p$ và $x^{(p-1)k} \equiv 1 \pmod p$ ta suy ra

$$S_k \equiv \frac{x^{(p-1)k} - 1}{x^k - 1} \equiv 0 \pmod p.$$

Vậy các số *k* cần tìm là tất cả các số không chia hết cho *p*.

Nhận xét. Lời giải bài toán thật đơn giản và đẹp mắt nếu biết sử dụng sự tồn tại của căn nguyên thủy *x* (mod*p*) mà chìa khóa ở đây là tính chất (*). Ta xét tiếp một bài toán tương tự.

Bài toán 2 (**Mongolia 2015**). Cho p là số nguyên tố lẻ. Gọi $a_1, a_2, ..., a_{p-1}$ là tất cả các số nguyên dương phân biệt nhỏ hơn p. Chứng minh rằng tồn tại một hoán vị của $p-1$ số này là $b_1, b_2, ..., b_{p-1}$ sao cho $\sum_{i=1}^{p-1} a_i^{b_i}$ là bội của p.

Lời giải. Cũng tương tự bài toán 1, ta sẽ xây dựng hoán vị thỏa mãn bằng cách dùng căn nguyên thủy. Thật vậy, gọi x là một căn nguyên thủy mod$p$. Khi đó

$$\left\{x^1, x^2, x^3, ..., x^{p-1}\right\} \equiv \left\{1, 2, 3, ..., p-1\right\}.$$

Ta sẽ chỉ ra một hoán vị $\left\{k_1, k_2, ..., k_{p-1}\right\}$ của $\left\{1, 2, ..., p-1\right\}$ sao cho $\sum_{i=1}^{p-1} x^{ik_i}$ là bội của p là xong. Ta chọn các số k_i như sau: $k_i = \frac{p+1}{2} - i$ và $k_{i+\frac{p-1}{2}} = p - i$, với $i = 1, 2, ..., \frac{p-1}{2}$.

Khi đó tổng $\sum_{i=1}^{p-1} x^{ik_i}$ trở thành

$$\sum_{i=1}^{p-1} x^{ik_i} \equiv \frac{p+1}{2}\left(x^{ij} + x^{(p-i)(p-j)}\right) = \frac{p+1}{2}.x^{ij}\left(1 + x^{p^2 - p.\frac{p+1}{2}}\right)$$

$$= \frac{p+1}{2}.x^{ij}\left(1 + x^{p.\frac{p-1}{2}}\right).$$

Do x là căn nguyên thủy nên $x^{p.\frac{p-1}{2}} = x^{\frac{\varphi(p)}{2}} \equiv -1 \pmod{p}$, suy ra $1 + x^{p.\frac{p-1}{2}} \vdots p$, từ đó hoán vị vừa xây dựng thỏa mãn.

Bài toán 3 (**Iran 2013**). Cho p là số nguyên tố lẻ. Chứng minh rằng tồn tại một số tự nhiên x sao cho x và $4x$ đều là căn nguyên thủy mod$p$.

Lời giải. Để chỉ ra sự tồn tại của x thì rất tự nhiên chúng ta sẽ xây dựng nó theo một căn nguyên thủy (cố định) nào đó của p.

Gọi a là một căn nguyên thủy mod$p$. Khi đó tồn tại số nguyên dương r sao cho

$$2 \equiv a^r \pmod{p}.$$

Suy ra $4 \equiv a^{2r} \pmod{p}$. (1)

Gọi $p_1, p_2, ... p_\ell$ là các ước nguyên tố phân biệt của $p-1$. Với $1 \le k \le \ell$, đặt s_k là một số nguyên sao cho $s_k \not\equiv 0 \pmod{p_k}$ và $s_k \not\equiv -2r \pmod{p_k}$. Theo định lý phần dư trung hoa, tồn tại số tự nhiên *m* sao cho

$$m \equiv s_k \pmod{p_k}, \quad 1 \le k \le \ell.$$

Khi đó, *m* và $m+2r$ đều không chia hết cho p_k. Do đó chúng nguyên tố cùng nhau với $p-1$. Ta có

$$p-1 \nmid m, 2m, 3m, ..., (p-2)m,$$

$$p-1 \nmid m+2r, 2(m+2r), 3(m+2r), ..., (p-2)(m+2r).$$

Do *a* là căn nguyên thủy mod*p* nên ta được

$$a^m, a^{2m}, a^{3m}, ..., a^{(p-2)m} \not\equiv 1 \pmod{p},$$

$$a^{m+2r}, a^{2(m+2r)}, a^{3(m+2r)}, ..., a^{(p-2)(m+2r)} \not\equiv 1 \pmod{p}.$$

Như vậy a^m và a^{m+2r} là căn nguyên thủy mod*p*. Cùng với (1) ta suy ra số $x = a^m$ thỏa mãn yêu cầu bài toán.

Bài toán 4 (China TST 1993). Với mỗi số nguyên tố *p* lẻ, ta định nghĩa $F(p) = \sum_{k=1}^{\frac{p-1}{2}} k^{120}$ và $f(p) = \frac{1}{2} - \left\{ \frac{F(p)}{p} \right\}$. Tìm giá trị của $f(p)$.

Lời giải. Gọi *x* là căn nguyên thủy mod*p*.

Nếu $(p-1) \nmid 120$ thì $x^{120} \not\equiv 1 \pmod{p}$ và $x^{120(p-1)} \equiv 1 \pmod{p}$. Do đó

$$F(p) \equiv \frac{1}{2} \sum_{i=1}^{p-1} x^{120i} = \frac{x^{120}\left(x^{120(p-1)} - 1\right)}{2\left(x^{120} - 1\right)} \equiv 0 \pmod{p}.$$

Vậy $f(p) = \frac{1}{2}$.

Nếu $(p-1) | 120$ thì $p \in \{3, 5, 7, 11, 13, 31, 41, 61\}$ và $x^{120} \equiv 1 \pmod{p}$. Do đó

$$F(p) \equiv \frac{1}{2}\sum_{i=1}^{p-1} x^{120i} = \frac{p-1}{2} \pmod{p}.$$

Vậy $f(p) = \frac{1}{2} - \frac{p-1}{2p} = \frac{1}{2p}$.

Bài toán 5 (China TST 1993). Với mỗi số nguyên *a*, đặt $n_a = 101a - 100.2^a$. Chứng minh rằng với $0 \le a,b,c,d \le 99$ sao cho $n_a + n_b \equiv n_c + n_d \pmod{10100}$ thì $\{a,b\} \equiv \{c,d\}$.

Lời giải. Ta sẽ sử dụng bổ đề cơ bản sau: Cho *a*,*b* là các số tự nhiên. Khi đó

$$2^a \equiv 2^b \pmod{101} \Leftrightarrow a \equiv b \pmod{100}$$

Trở lại bài toán: Do $(100,101) = 1$ nên

$$n_a + n_b \equiv n_c + n_d \pmod{10100} \Leftrightarrow \begin{cases} n_a + n_b \equiv n_c + n_d \pmod{101} \\ n_a + n_b \equiv n_c + n_d \pmod{100} \end{cases}$$

Ta có $n_a \equiv a \pmod{100}$ và $n_a \equiv 2^a \pmod{101}$ nên

$$2^a + 2^b \equiv 2^c + 2^d \pmod{101} \ (1) \text{ và } a + b \equiv c + d \pmod{100} \qquad (2)$$

Chú ý là $2^{100} \equiv 1 \pmod{101}$ và (2) suy ra

$$2^a.2^b = 2^{a+b} \equiv 2^{c+d} = 2^c.2^d \pmod{101}$$

Lại có $2^b \equiv 2^c + 2^d - 2^a \pmod{101}$ nên ta được

$$2^a.\left(2^c + 2^d - 2^a\right) \equiv 2^c.2^d \pmod{101} \Leftrightarrow \left(2^a - 2^c\right).\left(2^a - 2^d\right) \pmod{101}$$

Suy ra $2^a \equiv 2^c \pmod{101}$ hoặc $2^a \equiv 2^d \pmod{101}$. Theo kết quả bài 3 suy ra

$$a \equiv c \pmod{100} \text{ hoặc } a \equiv d \pmod{100} \qquad (3)$$

Từ (2) và (3) suy ra $\{a,b\} \equiv \{c,d\}$ (đpcm).

Bài toán 6. Tìm tất cả các số có hai chữ số $n = \overline{ab}$ sao cho với mọi số nguyên *k* ta có $n \mid k^a - k^b$.

Lời giải. Dễ thấy các số $11, 22, ..., 99$ thỏa mãn đề bài. Ta xét số $n = \overline{ab}$ thỏa mãn với $a \ne b$. Gọi *p* là một ước nguyên tố của *n*. Gọi *x* là một căn nguyên thủy modp. Khi đó

$p \mid x^a - x^b$, suy ra $x^{|a-b|} \equiv 1 \pmod p$. Do $ord_p(x) = p-1$ nên $|a-b| \vdots p-1$, chú ý rằng $|a-b| \le 9$, ta suy ra $p = 2,3,5,7$.

Nếu $p = 7 \mid n$ thì $6 \mid |a-b|$, suy ra $n = 28$. Chú ý rằng $k^2 \equiv k^8 \pmod 4$ và $k^2 \equiv k^8 \pmod 7$ luôn xảy ra nên $n = 28$ thỏa mãn.

Tương tự với $p = 5$ thì $n = 15$ hoặc 40. Kiểm tra ta được $n = 15$ thỏa mãn. Với $p = 3$ thì $n = 24$ hoặc 48. Kiểm tra ta được $n = 48$ thỏa mãn. Với $p = 2$ thì $n = 16, 32, 64$. Kiểm tra không số nào thỏa mãn. Vậy tất cả các số *n* cần tìm là $n \in \{11, 22, ..., 99, 28, 15, 48\}$.

Tiếp theo là một bài toán có cấu trúc khá giống bài toán trên, tuy nhiên lại là một bài toán khó hơn hẳn.

Bài toán 7 (**Iran TST 2015**). Tìm tất cả các bộ số nguyên dương (a,b,n) thỏa mãn $a \ge b$, $\gcd(b,n) = 1$ và $n^a \mid a^n - b^n$.

Hướng giải. Để giải quyết những bài toán dạng này ta thường xuất phát bằng cách đưa thêm một biến là ước nguyên tố (thường là ước nguyên tố nhỏ nhất) để tìm ra được quan hệ giữa a,b. Tiếp sau đó là bước tìm *n* từ một quan hệ chia hết.

Dễ thấy với $a = b$ sẽ luôn thỏa mãn.

Nếu $n = 1$ thì mọi $a \ge b$ đều thỏa mãn.

Nếu $n \ge 2$, ta xét $a > b$. Gọi *p* là ước nguyên tố nhỏ nhất của *n*, ta có

$$a^n \equiv b^n \pmod p \text{ và } a^{p-1} \equiv b^{p-1} \equiv 1 \pmod p.$$

Do đó $a^{\gcd(n,p-1)} \equiv b^{\gcd(n,p-1)} \pmod p$, suy ra $a \equiv b \pmod p$. Xét *p* lẻ, khi đó

$$v_p(a^n - b^n) = v_p(a-b) + v_p(n) \text{ và } v_p(n^a) = av_p(n).$$

Từ $n^a \mid a^n - b^n$, suy ra $v_p(a-b) \ge (a-1)v_p(n) \ge a-1$, suy ra $a - b \ge p^{a-1}$, điều này mâu thuẫn vì $a - 1 < p^{a-1}$ với mọi *a* nguyên dương. Do đó $p = 2$. Khi đó

$$v_2(a^n - b^n) = v_2(a^2 - b^2) + v_p(n) - 1 \text{ và } v_2(n^a) = av_2(n) \ge a.$$

Do đó $v_2(a^2 - b^2) \ge a \Rightarrow a^2 - b^2 \ge 2^a$. Từ đó suy ra $a = 3, b = 1$.

Tiếp theo ta tìm n sao cho $v_2(n)=1$ và $n^3 \mid 3^n-1$. Cũng dùng ước nguyên tố nhỏ nhất như ở bước trên ta dễ tìm được chỉ có $n=2$ thỏa mãn.

Vậy các bộ (a,b,n) cần tìm là $(a,a,n);(a,b,1);(3,1,2)$.

Bài toán 8. Cho p là số nguyên tố lẻ. Tìm tất cả các hàm số $f:\mathbb{Z}\to\mathbb{Z}$ thỏa mãn hai điều kiện sau:

(i) Nếu $m\equiv n \pmod p$ thì $f(m)=f(n)$.

(ii) $f(mn)=f(m)f(n)$.

Lời giải. Từ (ii) suy ra $f(0)=0$ hoặc 1.

Nếu $f(0)=1$ thì cho $m=0$, ta được: $1=f(0)=f(0)f(n)=f(n)$, với mọi $n\in\mathbb{Z}$. Dễ thấy hàm $f(n)=1$ thỏa mãn.

Nếu $f(0)=0$, thì với $n\equiv 0 \pmod p$ ta được $f(n)=0$. Với $n\not\equiv 0 \pmod p$, gọi x là một căn nguyên thủy mod$p$. Khi đó $n\equiv x^k \pmod p$ với mỗi $k\in\{1,2,...,p-1\}$. Do đó $f(n)=f\left(x^k\right)=\left(f(x)\right)^k$. Theo định lý Fermat thì $x^p\equiv x \pmod p$, suy ra $\left(f(x)\right)^p=f(x)$. Do đó $f(x)=0,1$ hoặc -1.

Nếu $f(x)=0$ thì $f(n)=0,\forall n\in\mathbb{Z}$. Nếu $f(x)=1$ thì $f(n)=1,\forall n\not\equiv 0 \pmod p$.

Nếu $f(x)=-1$ thì với $n\equiv a^2 \pmod p$, $a\neq 0$ thì $f(n)=1$, ngược lại thì $f(n)=-1$.

Bài toán 9. Cho $n\in\mathbb{N}, n\geq 1: 3^n-1 \vdots n$. Chứng minh rằng n chẵn.

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

Gọi h là cấp của 3 (mod$p$), ta có $\begin{cases} 3^n\equiv 1 \pmod p \\ 3^h\equiv 1 \pmod p \end{cases} \Rightarrow h\mid n$.

Rõ ràng là $p\neq 3$. Theo định lý Fecmat thì $3^{p-1}\equiv 1 \pmod p$, suy ra $h\mid p-1$

Nếu h>1 thì tồn tại q là ước nguyên tố của h, $h\geq q$ và $q\mid n$ và $p-1\geq h$, suy ra $p\geq q$, mâu thuẫn với p là ước nguyên tố nhỏ nhất của n.

Vậy h=1, khi đó $3^1\equiv 1 \pmod p \Rightarrow p=2$. Do đó n chẵn.

Một lớp các bài toán tương tự cách suy luận về cấp như trên

Bài toán 9.1. Cho *p* nguyên tố. Chứng minh rằng mọi ước nguyên tố của $2^p - 1$ đều lớn hơn *p*.

Bài toán 9.2. Cho *p* nguyên tố, *a* nguyên; $1 < a \le p-1$. Đặt $A = \sum_{k=0}^{p-1} a^k$. Chứng minh rằng với mọi ước nguyên tố *q* của *A* ta đều thỏa mãn $p \mid q-1$.

Bài toán 9.3. Chứng minh rằng $n \mid \varphi(a^n - 1)$ với mọi số nguyên dương *a* và *n*.

Hint. Ta đi chứng minh cấp của $a \bmod (a^n - 1)$ bằng *n*.

Bài toán 10. Chứng minh rằng mọi ước nguyên tố của số Fecmat thứ *n*: $F_n = 2^{2^n} + 1$ thì đều đồng dư với 1 theo mođun 2^{n+1}.

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

Gọi *h* là cấp của 2 modp, ta có $2^h \equiv 1 (\bmod p)$ và $h \mid 2^{n+1}$.

Do F_n lẻ nên p lẻ, do đó $2^{p-1} \equiv 1 (\bmod p)$ nên $h \mid p-1$.

Ta chỉ cần chứng minh $h = 2^{n+1}$ là xong. Rõ ràng *h* có dạng $h = 2^k, k \le n+1$

Nếu $k \le n$ thì $p \mid 2^h - 1 \mid 2^{2^n} - 1$, mà $p \mid 2^{2^n} + 1 \Rightarrow p \mid 2$ (vô lý)

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

Nhận xét 1. Kết quả trên có thể tổng quát theo một trong các hướng sau

KQ1: Cho *a,b* nguyên dương và nguyên tố cùng nhau. Khi đó mọi ước lẻ của số $A = a^{2^n} + b^{2^n}, n \in \mathbb{Z}^+$ đều đồng có dạng $2^{n+1}.k + 1$.

KQ2: Cho a, n là các số nguyên dương. Khi đó mọi ước nguyên tố p của $a^{2^n} + 1$ đều bằng 2 hoặc bằng một số có dạng $2^{n+1}k + 1$.

Từ **KQ2** này ta có thể chứng minh được kết quả sau về sự tồn tại vô hạn các số nguyên tố

"Với mỗi số nguyên dương n cho trước, tồn tại vô hạn các số nguyên tố dạng $2^n.k + 1$, trong đó k là một số nguyên dương".

Thật vậy, giả sử chỉ có hữu hạn các số nguyên tố $p_1, p_2, ..., p_m$ có dạng $2^n.k + 1$.

Xét số $A=\left(2p_1p_2...p_m\right)^{2^{n-1}}+1$ thì theo **KQ2** trên ta có *A* có ước nguyên tố dạng $2^n.k+1$ và ước nguyên tố này không trùng với các số nguyên tố $p_1, p_2,..., p_m$, vô lí.

Nhận xét 2 . Ta có thể chứng minh một kết quả mạnh hơn là $p\equiv 1(\bmod 2^{n+2})$ nếu sử dụng tính chất của số chính phương mod*p*. Thật vây, theo kết quả trên thì

$$p-1\vdots 2^{n+1}\Rightarrow p=8k+1.$$

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

Nhưng $ord_p(2)=2^{n+1}$ (theo chứng minh trên) nên $2^{n+1}\mid\frac{p-1}{2}\Rightarrow p-1\vdots 2^{n+2}$. Ta có điều phải chứng minh.

Kết quả trên được coi như một bổ đề khá quan trọng để giải quyết các bài toán khó liên quan đến số Fecmat F_n. Ta xét một bài toán ứng dụng kết quả này qua bài toán sau:

Bài toán 10.1 (Đề kiểm tra của viện toán học 2016). Chứng minh rằng tồn tại vô hạn số nguyên các bộ ba số nguyên tố $\left(p,q,r\right)$ đôi một phân biệt sao cho

$$\begin{cases}2^{p-1}\equiv 1\ (\bmod q)\\ 2^{q-1}\equiv 1\ (\bmod r)\\ 2^{r-1}\equiv 1\ (\bmod p)\end{cases}$$

Ta cần sử dụng thêm các kết quả sau:

Kết quả 1. Các số F_n đôi một nguyên tố cùng nhau.

Thật vậy, điều này được suy ra ngay từ đẳng thức sau $F_n=F_0.F_1...F_{n-1}+2$.

Kết quả 2. Hoặc F_n là số nguyên tố, hoặc F_n có ít nhất hai ước nguyên tố phân biệt.

Thật vậy, ta chỉ cần chứng minh rằng nếu F_n không là số nguyên tố thì nó không phải là một lũy thừa với số mũ lớn hơn 1 của một số nguyên nào đó. Trước hết, ta chỉ ra rằng F_n không phải là số chính phương. Thật vậy, giả sử $2^{2^n}+1=a^2$ thì $2^{2^n}=\left(a-1\right)\left(a+1\right)$.

Suy ra *a* lẻ và $2^{2^n-2}=\frac{a-1}{2}.\frac{a+1}{2}$.

Từ đây ta dễ suy ra điều mâu thuẫn. Bây giờ, ta giả sử $2^{2^n}+1=a^k$ với a,k là các số nguyên lẻ và $k\geq 3$. Ta có

$$2^{2^n}=(a-1)\left(a^{k-1}+a^{k-2}+...+a+1\right)$$

Tuy nhiên $a^{k-1}+a^{k-2}+...+a+1$ là số lẻ lớn hơn 1 và do đó không thể là ước của 2^{2^n}.
Điều mâu thuẫn này cho ta điều phải chứng minh.

Quay trở lại bài toán. Ta sẽ chỉ ra cách xây dựng các bộ (p,q,r) như sau: Đầu tiên lấy n tùy ý.

* Nếu F_n nguyên tố thì ta chọn $p=F_n$, q là một ước nguyên tố bất kì của F_{n+1} và r là một ước nguyên tố bất kì của F_{n+2}.

* Nếu F_n không nguyên tố thì theo **KQ2** nó có ít nhất hai ước nguyên tố phân biệt và ta chọn p,q là hai ước như vậy và ta chọn r là một ước nguyên tố của F_{n+1}. Ta chứng minh p,q,r thỏa mãn yêu cầu bài toán. Thật vậy, nếu n nguyên tố thì $2^{p-1}-1=2^{2^{2^n}}-1=2^{2^{n+1}.m}-1=\left(F_{n+1}-1\right)^m-1\vdots F_{n+1}\vdots q$ (do $2^{2^n}=2^{n+1}.m$ với m chẵn). Do q là ước nguyên tố của F_{n+1} nên theo kết quả trên ta được $q=2^{n+2}.k+1$ với k chẵn. Từ đó suy ra $2^{q-1}-1=2^{2^{n+2}.k}-1=\left(F_{n+2}-1\right)^k-1\vdots F_{n+2}\vdots r$. Cuối cùng do r là ước nguyên tố của F_{n+2} nên $r=2^n.h+1$ với h là một số nguyên chẵn. Từ đó $2^{r-1}-1=2^{2^n.h}-1=\left(F_n-1\right)^h-1\vdots F_n\vdots p$.

Các trường hợp khác ta xét tương tự. Để ý rằng các số F_n đôi một nguyên tố cùng nhau nên xây dựng trên cho ta vô hạn các bộ (p,q,r) (đpcm).

Bài toán 11. Tìm n nguyên dương, $n<1000$ có dạng $n=p_1p_2p_3$ (p_1,p_2,p_3 nguyên tố phân biệt) thoả mãn $2^n+2\vdots n$.

Lời giải. Trước hết ta chứng minh n chẵn. Thật vậy, nếu n lẻ thì

$$n-1=2^k.m\ \ (k,m\geq 1;\ (2,m)=1).$$

Gọi p là ước nguyên tố của n thì p lẻ và ta có $2^n\equiv -2 \pmod p \Rightarrow 2^{n-1}\equiv -1 \pmod p$.

Suy ra $2^{2^k.m} \equiv -1 \pmod p \Rightarrow \left(2^m\right)^{2^{k+1}} \equiv -1 \pmod p$.

Gọi h là cấp của 2^m mod p. Cùng với định lí Fecmat $\left(2^m\right)^{p-1} \equiv 1 \pmod p$ ta được

$$\begin{cases} h \mid p-1 \\ h \mid 2^{k+1} \end{cases}.$$

Tương tự cách chứng minh bài toán 10 ta được $h = 2^{k+1}$.

Khi đó $2^{k+1} \mid p-1$. Như vậy thì $2^{k+1} \mid p_i - 1 \ \forall i = 1,2,3$. Do đó

$$n-1 = p_1 p_2 p_3 - 1 \vdots 2^{k+1} \text{ (vô lí).}$$

Vậy n chẵn. Tiếp theo ta viết n dưới dạng $n = 2pq$; p,q nguyên tố lẻ phân biệt, giả sử $p < q$. Từ $n < 1000$ suy ra $pq < 500 \Rightarrow p \le 19$.

Do n chẵn nên từ $2^n \equiv -2 \pmod p$ suy ra -2 là số chính phương mod$p$, suy ra p có dạng $8k+1$ hoặc $8k+3$, từ đó $p \in \{3;11;17;19\}$.

Thử trực tiếp các trường hợp ta được n cần tìm là $n = 2.3.11 = 66$ và $n = 2.11.43 = 946$.

Bài toán 12. 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 $a > 1$ sao cho $a^{\frac{n-1}{2}} + 1 \vdots n$.

Lời giải.

* Giả sử n nguyên tố. Gọi a là căn nguyên thủy mod n. Ta có

$$a^{n-1} \equiv 1 (\bmod n) \Rightarrow \left(a^{\frac{n-1}{2}} - 1\right)\left(a^{\frac{n-1}{2}} + 1\right) \vdots n.$$

Vì a là căn nguyên thuỷ mod n nên $a^{\frac{n-1}{2}} - 1$ không chia hết cho n, suy ra $a^{\frac{n-1}{2}} + 1 \vdots n$.

* Ngược lại, giả sử tồn tại a nguyên lớn hơn 1 sao cho $a^{\frac{n-1}{2}} + 1 \vdots n$ (1)

Gọi p là ước nguyên tố của n. Ta phải chứng minh $n = p$.

Gọi h là cấp của a mod$p$, từ (1) ta có $a^{n-1} \equiv 1 (\bmod p)$, suy ra $h \mid n-1 \Rightarrow h \mid 2^k \Rightarrow h = 2^t$

Nếu $1 \le t \le k-1$ thì $h \mid \frac{n-1}{2}$, suy ra $a^{\frac{n-1}{2}} \equiv 1 (\bmod p)$, mâu thuẫn với (1)

Vậy $t = k$ suy ra $h = 2^k$. Lại do h là cấp của a mod$p$ nên

$$h \mid p-1 \Rightarrow 2^k \mid p-1 \Rightarrow n-1 \mid p-1, \text{ tức là } n = p.$$

Do đó n là số nguyên tố. Bài toán được chứng minh hoàn toàn.

Bài tương tự. Cho n nguyên dương có dạng $n = 2^k.u + 1$; u lẻ, $u < 2^k$. Gọi p là số nguyên tố lẻ thoả mãn $p^{\frac{n-1}{2}} + 1 \vdots n$. Chứng minh rằng n là số nguyên tố.

Bài toán 13 (Canada TST 2015). Cho p nguyên tố sao cho $\frac{p-1}{2}$ cũng là số nguyên tố. Các số nguyên a, b, c không chia hết cho p. Chứng minh rằng tồn tại nhiều nhất $1 + \sqrt{2p}$ số nguyên dương n sao cho $n < p$ và $p \mid \left(a^n + b^n + c^n\right)$.

Lời giải. Ta thực hiện qua các bước sau:

1. Nếu ta có $\begin{cases} b \equiv \pm a \pmod p \\ c \equiv \pm b \pmod p \end{cases}$ thì với mỗi n nguyên dương ta có

$$a^n + b^n + c^n \equiv \pm a^n \pmod p \text{ hoặc } a^n + b^n + c^n \equiv \pm 3a^n \pmod p.$$

Khi đó không có số n nào thỏa mãn.

2. Xét $b \not\equiv \pm a \pmod p$ thì $b.a^{-1} \not\equiv \pm 1 \pmod p$. Đặt $q = \frac{p-1}{2}$ nguyên tố. Gọi h là cấp của $b.a^{-1}$ mod$p$. Ta có $h \mid (p-1) \Rightarrow h \mid 2q$.

Mà $b.a^{-1} \not\equiv \pm 1 \pmod p \Rightarrow h \ne 2 \Rightarrow h = q$ hoặc $h = 2q$.

3. Đặt tập $S = \left\{n < p; a^n + b^n + c^n \vdots p\right\}$ và đặt S_t là số cặp sắp thứ tự $(i, j) \in S \times S$ sao cho $i - j \equiv t \pmod{p-1}$.

Bổ đề. Nếu t nguyên dương, $t < 2q, t \ne q$ thì $S_t \le 2$.

Chứng minh. Xét $i, j \in S$ với $j - i \equiv t \pmod{p-1}$. Ta có

$$a^i + b^i + c^i \equiv 0 \pmod p;\ a^j + b^j + c^j \equiv 0 \pmod p.$$

Suy ra $a^i.c^{j-i}+b^i.c^{j-i}+c^j\equiv 0 \pmod p \Rightarrow a^i.c^{j-i}+b^i.c^{j-i}-a^j-b^j\equiv 0 \pmod p$

Do đó $a^i.\left(c^t-a^t\right)\equiv b^i.\left(b^t-c^t\right) \pmod p$ (*).

+ Nếu $c^t\equiv a^t \pmod p$ thì $c^t\equiv b^t \pmod p$, suy ra

$a^t\equiv b^t \pmod p \Rightarrow \left(ab^{-1}\right)^t\equiv 1 \pmod p \Rightarrow t\,\vdots\, h$, mâu thuẫn vì $t\not\vdots\, h$.

+ Nếu $c^t\not\equiv a^t \pmod p$ thì (*) được viết lại như sau

$$\left(ab^{-1}\right)^i\equiv\left(b^t-c^t\right)\left(c^t-a^t\right)^{-1} \pmod p. \qquad (1)$$

Cố định t thì vế phải của (1) không đổi, suy ra $\left(ab^{-1}\right)^i$ cố định. Từ $h=q$ hoặc $h=2q$ nên (1) có nhiều nhất hai nghiệm i, bổ đề được chứng minh.

Trở lại bài toán. Với mỗi $i\in S$ ta có không ít hơn $|S|-2$ phần tử khác với i bởi số lượng khác $q \pmod{p-1}$. Do đó theo bổ đề ta được

$$|S|\left(|S|-2\right)\le\sum_{t\ne q}S_t\le 2\left(p-2\right)\Rightarrow |S|<\sqrt{2p}+1 \text{ (đpcm).}$$

Bài toán 14 (**Romania 1996**). Tìm tất cả các số nguyên tố p,q phân biệt sao cho $a^{3pq}\equiv a \pmod{3pq}$ với mọi số nguyên a.

Lời giải. Có thể giả sử $p\ge q$. Chọn $a=3$ ta được

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

Chọn a là căn nguyên thuỷ mod$p$, ta có $a^{p-1}\equiv 1 \pmod p$ (chú ý là khi đó (a,p)=1)

Ta có $a^{3pq}\equiv a \pmod p\Rightarrow a^{3pq-1}\equiv 1 \pmod p\Rightarrow p-1\,|\,3pq-1\Rightarrow p-1\,|\,3q-1$ (1)

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

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

+ Nếu $3q-1=p-1\Rightarrow p=3q$, vô lí.

+ Nếu $3q-1=2(p-1)\Rightarrow 3q+1=2p$. Từ (2) lại có $q-1\,|\,6p-2\Rightarrow q-1\,|\,3(3q+1)-2$.

Suy ra $q-1\,|\,10\Rightarrow q=2;11$. Dễ thấy khi đó chỉ có bộ $\left(p,q\right)=\left(17,11\right)$ thoả mãn.

+ Nếu $3q-1=3(p-1)$, ta có ngay điều mâu thuẫn.

Vậy có hai bộ (p,q) cần tìm là (17,11) và (11,17).

Nhận xét. Thực chất đầu tiên ta chỉ cần chọn *a* sao cho $(a,p)=1$, khi đó ta đã có $a^{p-1}\equiv 1 \pmod p$, nhưng nếu chọn *a* là căn nguyên thuỷ mod *p* thì $p-1$ lại đóng thêm vai trò là cấp của *a* mod *p*. Khi đó ta có quan hệ rất tốt là $p-1 \mid 3pq-1$ như ở trên.

Trong bài toán trên, do số 3 đóng vai trò là một số nguyên tố, nên có thể tổng quát hoá bài toán khi thay số 3 bằng một số nguyên tố khác như sau:

Bài toán 14.1. Tìm p,q,r nguyên tố phân biệt sao cho $a^{pqr}\equiv a \pmod{pqr}$ với mọi *a* nguyên dương.

Khi đó tương tự với lời giải trên, ta đưa bài toán về việc tìm các số nguyên tố p,q,r sao cho

$$r-1 \mid pq-1;\ p-1 \mid pr-1;\ q-1 \mid pr-1 \qquad (*)$$

Và đây là bài toán giải phương trình nghiệm nguyên với các số nguyên tố thoả mãn điều kiện (*).

Bài toán 15. Chứng minh rằng với mỗi *n* nguyên dương lớn hơn 1 thì 3^n-2^n không chia hết cho *n*.

Lời giải. Giả sử rằng tồn tại *n*>1 sao cho 3^n-2^n chia hết cho *n*. Gọi *p* là ước nguyên tố nhỏ nhất của *n*, dễ thấy ngay $p\ge 5$.

Gọi *a* là một số nguyên dương sao cho $2a\equiv 1 \pmod p$ (1)

Từ $3^n\equiv 2^n \pmod p \Rightarrow (3a)^n\equiv 1 \pmod p$. Gọi *h* là cấp của 3*a* (mod*p*), ta có

$$\begin{cases} h \mid n \\ h \mid p-1 \end{cases} \Rightarrow \begin{cases} h \mid n \\ h < p \end{cases} \Rightarrow h=1. \text{ Khi đó } 3a\equiv 1 \pmod p \qquad (2)$$

Từ (1) và (2) suy ra $a\equiv 0 \pmod p$, mâu thuẫn với (1). Vậy bài toán được chứng minh.

Nhận xét. Từ quan hệ đồng dư $3^n\equiv 2^n \pmod p$ chưa cho ta dấu hiệu về cấp, việc chọn *a* thoả mãn (1) nhằm mục đích đưa về quan hệ đồng dư $(3a)^n\equiv 1 \pmod p$, lúc này đầu mối

của việc sử dụng cấp theo mod*p* mới xuất hiện. Việc chọn được các số *a* như vậy là một kĩ thuật hay, tinh tế nhưng cũng không phải là điều quá thiếu tự nhiên.

Bài toán 16. Tìm tất cả các cặp số nguyên tố (p,q) sao cho $pq \mid (5^p - 2^p)(5^q - 2^q)$.

Lời giải.

Nếu $q = 3$ thì $(5^p - 2^p) \vdots p \Rightarrow 3 \vdots p \Rightarrow p = 3$ và (3,3) là cặp số thoả mãn.

Nếu p,q đều khác 3 thì

$$\left(5^p - 2^p, p\right) = \left(5^q - 2^q, q\right) = 1 \Rightarrow \begin{cases} 5^p - 2^p \vdots q \\ 5^q - 2^q \vdots p \end{cases}$$

Có thể giả sử $p > q$, suy ra $(p, q-1) = 1$. (1)

Gọi *a* là số tự nhiên thỏa mãn $2a \equiv 5 \pmod{q}$. (2)

Ta có ngay $a^p \equiv 1 \pmod{q}$. Gọi *h* là cấp của *a* (mod*q*) thì $\begin{cases} h \mid p \\ h \mid q-1 \end{cases} \Rightarrow (p, q-1) > 1.$

(dễ thấy là *h* khác 1). Đây là điều mâu thuẫn với (1). Do đó trong hai số *p* và *q* phải có một số bằng 3.

Nếu $q \neq 3$ thì $p = 3$, khi đó $q \mid 5^3 - 2^3 \Rightarrow q = 13$.

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

Bài toán 17 (**Korea TST 2003**). Với mỗi số nguyên tố *p*, xác định đa thức

$$f_p(x) = x^{p-1} + x^{p-2} + \ldots + x + 1.$$

a) Cho *m* là một bội của *p*. Chứng minh rằng mọi ước nguyên tố của $f_p(m)$ đều nguyên tố cùng nhau với $m(m-1)$.

b) Chứng minh rằng tồn tại vô hạn các số nguyên tố dạng $np + 1$, với *n* nguyên dương.

Lời giải. a) Gọi *q* là một ước nguyên tố bất kì của $f_p(m) = m^{p-1} + m^{p-2} + \ldots + m + 1$.

Do $q \mid f_p(m)$, suy ra $(q,m) = 1$. Ta cần chứng minh $(q, m-1) = 1$. Thật vậy, giả sử $(q, m-1) > 1$ thì hiển nhiên $m \equiv 1 \pmod{q}$. Mà $q \mid (m^{p-1} + m^{p-2} + \ldots + m + 1) \Rightarrow q \mid p$. Nhưng $p \mid m \Rightarrow q \mid m$, mâu thuẫn. Vậy $(q, m-1) = 1$. Do đó $(q, m(m-1)) = 1$ (đpcm).

b) Để sử dụng được kết quả phần (a), ta lấy trước một số m cố định là bội của p. Xét q là ước nguyên tố bất kì của $f_p(m)$. Khi đó ta có

$$q \mid f_p(m) = m^{p-1} + m^{p-2} + ... + m + 1 \Rightarrow q \mid m^p - 1 \Rightarrow m^p \equiv 1 (\bmod q).$$

Gọi h là cấp của m mod$q$, thì $m^h \equiv 1 (\bmod q)$ và $h \mid p \Rightarrow h \in \{1; p\}$.

Nếu $h = 1$ thì $m \equiv 1 \pmod q$, mâu thuẫn với phần (a). Vậy $h = p$, lúc đó cùng với định lí Fermat ta thu được $p \mid q - 1$.

Như vậy, với mỗi số m_i là bội của p thì ta xác định được ít nhất một số q_i nguyên tố mà q_i có dạng $n_i p + 1$.

Như vậy việc còn lại là xây dựng một dãy $(m_i)_{i \geq 1}$ vô hạn để các số q_i đều phân biệt. Điều này không khó, ta có thể chọn $m_{i+1} = pq_1q_2...q_i$, khi đó hiển nhiên $f_p(m_{i+1})$ không thể nhận $q_1, q_2, ..., q_i$ làm ước. Từ đó ta có điều phải chứng minh.

Nhận xét. Trên đây là một cách sử dụng đa thức để chứng minh kết quả kinh điển về sự tồn tại vô hạn các số nguyên tố dạng $np + 1$, với n nguyên dương.

Kết quả tổng quát hơn. Cho a là một số nguyên dương. Khi đó tồn tại vô hạn các số nguyên tố dạng $an + 1$, với n nguyên dương.

Đây là một định lý lớn và khó với chương trình THPT, ta cần sử dụng đến căn nguyên thủy bậc n của đơn vị và không trình bày ở đây.

Bài toán 18 (**China 2009**). Tìm tất cả các số nguyên tố p, q sao cho $pq \mid 5^p + 5^q$.

Lời giải. Nếu $p = 2$, ta có $2q \mid 25 + 5^q$, từ $5^q \equiv 5 \pmod q$ ta suy ra $q \mid 30$, thử trực tiếp được $q \in \{3, 5\}$. Tương tự nếu $p = 5$ thì $q \in \{2, 3, 5, 13\}$.

Xét p, q khác 2 và 5, theo định lý Fermat ta được $p \mid 5^q + 5$, hay $p \mid 5^{q-1} + 1 \Rightarrow 5^{2(q-1)} \equiv 1 \pmod q$. Gọi h là cấp của 5 mod$p$ thì $h \mid 2(q-1)$ và $h \nmid (q-1)$.

Do đó $v_2(h) > v_2(q-1)$. Mà $5^{p-1} \equiv 1 \pmod p$ nên $h \mid p - 1$, suy ra $v_2(p-1) \geq v_2(h)$. Do đó

$$v_2(p-1) > v_2(q-1).$$

Do vai trò của p, q như nhau nên ta cũng có $v_2(q-1) > v_2(p-1)$, mâu thuẫn.

Vậy tất cả các bộ (p,q) cần tìm là (5,2), (5,3), (5,13), (5,5), (2,5), (3,5), (13,5).

Bài toán 19 (**USA TST 2003**). Tìm tất cả các cặp số nguyên tố (p,q,r) thoả mãn

$$\begin{cases} p \mid q^r + 1 \ (1) \\ q \mid r^p + 1 \ (2) \\ r \mid p^q + 1 \ (3) \end{cases}$$

Lời giải. Dễ chứng minh được p,q,r đôi một phân biệt. Giả sử p,q,r cùng lớn hơn 2.

Từ (1) suy ra $p \mid q^{2r} - 1 \Rightarrow h \mid 2r$, với h là cấp của q (modp), theo định lý Fecmat thì $h \mid p-1$. Nếu h lẻ thì $p \mid q^{2r} - 1$ nên $p \mid 2 \Rightarrow p = 2$, vô lí. Vậy h chẵn, khi đó h=2 hoặc $h = 2r$.

Nếu $h = 2r$ thì $2r \mid p-1 \Rightarrow p \equiv 1 \pmod{r} \Rightarrow 0 \equiv p^q + 1 \equiv 2 \pmod{r} \Rightarrow r = 2$ (vô lí)

Nếu $h = 2$ thì $p \mid q^2 - 1$. Không thể xảy ra $p \mid q-1$ vì $p \mid q^r + 1$ và p khác 2, do đó $p \mid q+1 \Rightarrow p \mid \frac{q+1}{2}$, suy ra $p \le \frac{q+1}{2} < q$. Tương tự ta cũng có $q < r; r < p$, vô lí.

Vậy tồn tại một số bằng 2, giả sử đó là p=2. Khi đó q lẻ.

Ta có $q \mid r^2 + 1$ và $r \mid 2^q + 1$. Từ đây ta lại suy ra $d \mid 2q$, trong đó d là cấp của 2 (mod r)

Như vậy $d \in \{2; q; 2q\}$ $(2^d \equiv 1 \pmod{r})$ (4)

Nếu $q \mid d$ thì $q \mid r-1 \Rightarrow q \mid (r^2+1) - (r^2-1) = 2 \Rightarrow q = 2$, vô lí. Vậy d=2.

Khi đó theo (4) thì $r = 3$ và $q = 5$. Vậy $(p,q,r) = (2,3,5)$ và các hoán vị.

Nhận xét. Ta rút ra một kết quả hay sau: Cho p,q,r là các số nguyên tố phân biệt sao cho $p \mid q^r + 1$ và $p > 2$. Khi đó $2r \mid p-1$ hoặc $p \mid q^2 - 1$.

Bài toán 20 (**Terkey TST 2013**). Gọi $\varphi(n)$ là số các số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n. Tìm tất cả các cặp số nguyên dương (m,n) sao cho

$$2^n + (n - \varphi(n) - 1)! = n^m + 1.$$

Lời giải. Nếu *n* có nhiều hơn một ước nguyên tố, ta gọi p,q là hai ước nguyên tố của nó trong đó *p* là ước nguyên tố nhỏ nhất. Ta có

$$n-\varphi(n)-1\geq pq-(p-1)(q-1)-1=p+q-2>p$$

Do đó $p\,|\,(n-\varphi(n)-1)!$. Cùng với giả thiết ta được $p\,|\,2^n-1$. Từ quan hệ chia hết quen thuộc này, bằng việc dùng cấp ta chỉ ra mâu thuẫn.

Xét trường hợp n có dạng $n=p^k$, với *p* nguyên tố và *k* nguyên dương.

Nếu $k\geq 3$ thì

$$n-\varphi(n)-1\geq p^3-p^2-1>p.$$

Lập luận tương tự trường hợp trên ta được điều mâu thuẫn. Vậy $k=1,2$.

Từ đó tìm ra hai bộ (m,n) cần tìm là $(m,n)=(2,2);(2,4)$.

Bài toán 21 (**Balkan 1999**). Cho *p* là số nguyên tố, *p*>2 có dạng $p=3n+2$. Xét tập

$$S=\left\{y^2-x^3-1\,|\;x,y\in\mathbb{Z};\;0\leq x,y\leq p-1\right\}.$$

Chứng minh rằng có nhiều nhất *p* phần tử trong *S* chia hết cho *p*.

Lời giải. Ta sử dụng một kết quả cơ bản sau:

Cho *p* nguyên tố và *k* là số nguyên dương sao cho $(k,p-1)=1$. Khi đó

$$x^k\equiv y^k\,(\text{mod}\,p)\Leftrightarrow x\equiv y\;(\text{mod}\,p)$$

Đặt biệt nếu $(k,p-1)=1$ thì $A=\left\{1^k;2^k;...;(p-1)^k\right\}$ là một hệ thặng dư thu gọn mod*p*.

Trở lại bài toán, do $\{1;2;...;p-1\}$ là một hệ TDTG mod*p* và *p* có dạng $p=3n+2$ nên $(3,p-1)=1$, do đó theo bổ đề thì hệ $A=\left\{1^3;2^3;...;(p-1)^3\right\}$ là một hệ TDTG modp.

Do đó với mỗi *y* với $0\leq y\leq p-1$, tồn tại đúng một phần tử *x* với $0\leq x\leq p-1$ sao cho $x^3\equiv y^2-1(\text{mod}\,p)\Rightarrow p\,|\,x^3-y^2+1$. Vậy *S* chứa nhiều nhất *p* phần tử chia hết cho *p*.

Nhận xét. Từ bài toán trên, ta có thể khái quát hoá thành bài toán sau:

Bài toán 21.1. Cho *p* là số nguyên tố, $p>2$ có dạng $p=kn+2$. Xét tập

$$S=\left\{y^j-x^k-\alpha\,|\;j,k\in\mathbb{Z};\;0\leq j,k\leq p-1\right\}.$$

Chứng minh rằng có nhiều nhất *p* phần tử trong *S* chia hết cho *p*.

Bài toán 22. Tìm tất cả các số tự nhiên *a* sao cho tồn tại *n* nguyên dương, $n > 1$ thoả mãn

$$a^n + 1 \vdots n^2$$

Lời giải. Trước hết ta chứng minh *n* thoả mãn phải là số lẻ.

Nếu n chẵn thì $n^2 \equiv 0 (\bmod 4) \Rightarrow a^n + 1 \equiv 0 (\bmod 4)$, nhưng a^n chính phương nên $a^n \equiv 0,1 (\bmod 4)$ (vô lí). Vậy *n* lẻ.

Gọi *p* là ước nguyên tố nhỏ nhất của *n*, suy ra *p* lẻ. Ta có

$$a^n \equiv -1 (\bmod p) \Rightarrow (-a)^n \equiv 1 (\bmod p).$$

Gọi *h* là cấp của $-a$ (modp) thì $(-a)^h \equiv 1 (\bmod p)$ và $\begin{cases} h \mid n \\ h \mid p-1 \end{cases}$

Do *p* là ước nguyên tố nhỏ nhất của *n* nên từ trên suy ra ngay $h = 1$.

Khi đó $-a \equiv 1 (\bmod p) \Rightarrow a + 1 \vdots p$. Nói một cách khác là $a + 1$ có ước nguyên tố lẻ.

Tiếp theo ta sẽ chứng minh các số *a* như vậy là tất cả các số cần tìm.

Thật vậy, giả sử $a + 1$ có ước nguyên tố lẻ là *p*. Ta chứng minh $a^p + 1 \vdots p^2$. Ta có

$$a^p + 1 = (a+1)\left(a^{p-1} - a^{p-2} + ... - a + 1\right).$$

Do $a \equiv -1 (\bmod p)$, *p* lẻ nên $a^{p-1} - a^{p-2} + ... - a + 1 \equiv p \equiv 0 \ (\bmod p)$. Vậy $a^p + 1 \vdots p^2$.

Vậy tất cả các số cần tìm là các số *a* mà $a + 1$ có ước lẻ hay $a \neq 2^k - 1$.

Bài toán 23 (**Bulgaria 2015**). Cho *p* là số nguyên tố lớn hơn 10^9 sao cho $4p + 1$ cũng là số nguyên tố. Chứng minh rằng trong biểu diễn thập phân của số $\dfrac{1}{4p+1}$ có chứa đủ các chữ số từ 0 đến 9.

Lời giải. Đặt $q = 4p + 1$, kí hiệu $a * b$ là số dư trong phép chia *a* cho *b*.

Ta có nhận xét rằng, nếu các chữ số cuối của $10^k * q$ có chứa đủ hết các chữ số từ 0 đến 9 thì ta sẽ suy ra điều phải chứng minh. Bây giờ ta đi chứng minh điều đó.

Gọi S là tập tất cả các số t (phân biệt theo mod$q$) sao cho tồn tại số nguyên dương x thỏa mãn $x^4 \equiv t \pmod{q}$. Do $q \equiv 1 \pmod{4}$ nên -1 là số chính phương $\bmod q$. Ta có đúng $2p$ số chính phương $\bmod q$ là $a_1, a_2, ..., a_{2p}$ và các số này được chia thành đúng p cặp dạng $(k, -k)$. Từ mỗi cặp như vậy cho ta tương ứng một số $k^2 \in S$ và hai số chọn từ hai cặp khác nhau là phân biệt. Do đó $|S| = p$.

Tiếp theo ta chứng minh với mỗi phần tử $r \in S$, đều tồn tại số nguyên dương k sao cho $10^k * q = r$ bằng việc sử dụng cấp của phần tử. Thật vậy, gọi $ord_q(10) = h$ thì $h \mid 4p$, từ đó $h \in \{p, 2p, 4p\}$.

Xét $h = p$, với mỗi $0 \le k < p$, luôn tồn tại $0 \le j \le 3$ mà $4 \mid k + jp$. Đặt $k + jp = 4r$, khi đó số $10^k * q$ cũng là số dư khi chia $(10^r)^4$ cho q. Tuy nhiên các số $10^1, 10^2, ..., 10^p$ khi chia cho q sẽ được p số dư phân biệt, do đó nó chính là p phần tử của S. Trường hợp $h = 2p$ và $h = 4p$ được xét tương tự.

Gọi u là một chữ số nào đó bất kì. Tồn tại $0 \le j \le 3$ sao cho $u + jq$ có chữ số tận cùng là 0,1,5 hoặc 6. Vì $q > 10^9$ nên $\sqrt[4]{(j+1)q - 1} - \sqrt[4]{u + jq} > 6$. Suy ra trong đoạn từ $u + jq$ đến $(j+1)q$ có ít nhất 6 lũy thừa bậc 4 của các số nguyên dương liên tiếp, 6 chữ số này luôn chưa đủ 0,1,5,6. Do đó trong đoạn trên chứa ít nhất một số có dạng x^4 và có chữ số tận cùng giống như $u + jq$. Đặt $s = x^4 * q$ thì $x^4 = s + jq$. Mà $10 \mid x^4 - (u + jq) = s - u$, suy ra s có chữ số tận cùng là u. Bài toán được chứng minh hoàn toàn.

III. Vấn đề tồn tại căn nguyên thuỷ

Định lý. Các số $2, 4, p^k, 2p^k$ với p là số nguyên tố lẻ, k là số nguyên dương, và chỉ các số đó có căn nguyên thuỷ.

Từng bước ta sẽ chứng minh định lý lớn trên qua các mệnh đề sau.

Mệnh đề 1. Tồn tại căn nguyên thủy mod$p$, với p là số nguyên tố (đã chứng minh ở phần đầu bài viết).

Mệnh đề 2. Có căn nguyên thuỷ mod 4. Thật vậy, -1 là căn nguyên thuỷ mod 4.

Mệnh đề 3. Nếu p là số nguyên tố lẻ thì có căn nguyên thuỷ mod p^{α} với mọi số nguyên dương α.

Chứng minh. Giả sử g là một căn nguyên thuỷ mod p.

Ta có thể giả sử rằng $g^{p-1} \neq 1 \pmod{p^2}$. Thật vậy, nếu không thế thì $g_1 = g + p$ cũng là một căn nguyên thuỷ và sẽ có tính chất trên vì

$$g_1^{p-1} = (g+p)^{p-1} \equiv g^{p-1} + p(p-1)g^{p-2} \pmod{p^2}.$$

Từ đó, vì $g^{p-1} \equiv 1 \pmod{p^2}$ ta được $g_1^{p-1} \equiv 1 - p.g^{p-2} \pmod{p^2}$. Nhưng $\left(g^{p-2}, p\right) = 1$, cho nên $g_1^{p-1} \neq 1 \pmod{p^2}$. Vậy ta có thể giả thiết rằng căn nguyên thuỷ g mod$p$ thoả mãn điều kiện $g^{p-1} \neq 1 \pmod{p^2}$.

Tiếp theo ta sẽ chứng minh rằng g cũng là căn nguyên thuỷ mod p^{α} với mọi $\alpha > 1$.

Vì $g^{p-1} \neq 1 \pmod{p^2}$ nên ta có $g^{p-1} = 1 + pu$ với $\left(p, u\right) = 1$.

Do đó với mọi $\beta \geq 1$, ta được

$$g^{p^{\beta}(p-1)} = 1 + p^{\beta+1}.u' \text{ với } \left(u', p\right) = 1,$$

tức là

$$g^{p^{\beta}(p-1)} \equiv 1 (\bmod\, p^{\beta+1}) \text{ và } g^{p^{\beta}(p-1)} \neq 1 (\bmod\, p^{\beta+2})$$

Từ đó ta được $g^{p^{\alpha}(p-1)} = g^{\varphi\left(p^{\alpha}\right)} \equiv 1 (\bmod\, p^{\alpha})$ và với mọi $n \mid \varphi\left(p^{\alpha}\right)$, $n < \varphi\left(p^{\alpha}\right)$ thì $g^{n} \not\equiv 1 (\bmod\, p^{\alpha})$. Vậy g là căn nguyên thuỷ mod p^{α}. (đpcm).

Mệnh đề 4. Nếu p là số nguyên tố lẻ thì có căn nguyên thuỷ mod $2p^{\alpha}$ với mọi số nguyên dương α.

Chứng minh: Ta có $\varphi\left(p^{\alpha}\right) = \varphi\left(2p^{\alpha}\right)$ và với mọi x lẻ mà thoả mãn một trong hai đồng dư thức

$$x^{k} \equiv 1 (\bmod\, p^{\alpha}) \qquad\qquad x^{k} \equiv 1 (\bmod\, 2p^{\alpha})$$

thì cũng thoả mãn đồng dư thức kia.

Bây giờ theo mệnh đề 3 thì tồn tại căn nguyên thuỷ mod p^{α}, gọi đó là g. Khi đó một trong hai số $g,\ g+p^{\alpha}$ sẽ là căn nguyên thuỷ lẻ, và với chú ý ở trên nó chính là căn nguyên thuỷ mod $2p^{\alpha}$. (đpcm).

Mệnh đề 5. Không có căn nguyên thuỷ mod 2^{α} với mọi số nguyên dương $\alpha \geq 3$.

Chứng minh. Với mọi số nguyên x lẻ ta đều có $x^2 \equiv 1(\bmod 2^3)$ cho nên, với $\alpha \geq 3$ ta được $x^{2^{\alpha-2}} = (x^2)^{2^{\alpha-3}} \equiv 1(\bmod 2^{\alpha})$

Mà $\varphi\left(2^{\alpha}\right) = 2^{\alpha-1}$, do đó không có căn nguyên thuỷ mod 2^{α} với $\alpha \geq 3$.

Mệnh đề 6. Nếu số m có từ 2 ước nguyên tố lẻ trở lên thì không có căn nguyên thuỷ mod$m$.

Chứng minh. Giả sử m có dạng $m = 2^{\alpha}.p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}$ với $\alpha \geq 0; \alpha_i \geq 1; k \geq 2$ (p_i nguyên tố lẻ). Với a nguyên và $(a,m)=1$ thì $\left(a, p_i^{\alpha_i}\right)=1$ nên $a^{p_i^{\alpha_i-1}(p_i-1)} \equiv 1 \ (\bmod\ p_i^{\alpha_i})$ với mọi $i = 1,2,...,k$. Ta luôn có $a^{2^{\alpha}} \equiv 1(\bmod 2^{\alpha})\ \ \forall \alpha \geq 0$.

Nhưng vì $k \geq 2$ cho nên 2^{α} và $a^{p_i^{\alpha_i-1}(p_i-1)}$ đều là ước của $\frac{1}{2}\varphi(m)$, từ đó ta được các đồng dư thức $a^{\frac{1}{2}\varphi(m)} \equiv 1 \ (\bmod\ p_i^{\alpha_i})$; $i = 1,2,...,k$ và $a^{\frac{1}{2}\varphi(m)} \equiv 1 \ (\bmod 2^{\alpha})$.

Do đó $a^{\frac{1}{2}\varphi(m)} \equiv 1 \ (\bmod m)$. Vậy không có căn nguyên thuỷ mod$m$ (đpcm).

Mệnh đề 7. Nếu $m = 2^{\alpha}.p^{\beta}; \alpha \geq 2, \beta \geq 1$; p là số nguyên tố lẻ thì không có căn nguyên thuỷ mod$m$.

Chứng minh. Cũng tương tự như trên, ta chứng minh được rằng với mọi a nguyên tố với m, ta đều có $a^{\frac{1}{2}\varphi(m)} \equiv 1 \ (\bmod m)$.

Định lý được chứng minh hoàn toàn.

IV. Một số bài tập vận dụng

Bài 1. (**AIME2001**). Có bao nhiêu số nguyên dương *n* là bội của 1001 có thể biểu diễn dưới dạng $10^j - 10^i;\ 0 \le i < j \le 99$.

Bài 2. Tìm tất cả các số nguyên tố *p,q* sao cho $\begin{cases} p^2+1 \mid 2003^q+1 \\ q^2+1 \mid 2003^p+1 \end{cases}$

Bài 3. Cho *a,b* nguyên dương sao cho $2a-1$ và $2b-1$ và $a+b$ đều là số nguyên tố. Chứng minh rằng a^b+b^a và a^a+b^b đều không chia hết cho $a+b$.

Bài 4. Tìm tất cả các số nguyên dương m,n với $n>1$ sao cho $n \mid 1+m^{3^n}+m^{2.3^n}$.

Bài 5. Cho a,n là các số nguyên dương lớn hơn 2 sao cho $n \mid a^{n-1}-1$ và *n* không chia hết mỗi số có dạng a^x-1, ở đó $x<n-1$ và $x \mid n-1$. Chứng minh rằng *n* là một số nguyên tố.

Bài 6 (**Brazil 2009**). Cho hai số nguyên tố p,q thỏa mãn $q=2p+1$. Chứng minh rằng tồn tại một bội của *q* có tổng các chữ số nhỏ hơn 4.

Bài 7. Cho a,b là hai số hữu tỉ phân biệt thỏa mãn tồn tại vô số số nguyên dương n mà a^n-b^n là số nguyên dương. Chứng minh rằng cả a và b đều là số nguyên.

Bài 8 (**Việt Nam TST 2010**). Với mỗi số nguyên dương *n*, xét tập $T_n=\left\{11(k+h)+10\left(n^k+n^h\right);1\le k,h\le 10\right\}$. Tìm tất cả *n* sao cho không tồn tại $a,b\in T_n$ mà $a-b$ là bội của 110.

Bài 9 (IMO Shorlist 2012). Cho *x* và *y* là hai số nguyên dương thỏa mãn điều kiện $x^{2^n}-1$ là bội của $2^n y+1$ với mọi *n* nguyên dương. Chứng minh rằng $x=1$.

Bài 10 (Argentina TST 2010). Cho *r* số nguyên $a_1,a_2,...,a_r$ thỏa mãn $a_i \ge 2$ với mọi *i* và $a_1+a_2+...+a_r=2010$. Chứng minh rằng tập hợp $T_n=\{1,2,...,2010\}$ có thể được chia thành r tập $A_1,A_2,...,A_r$ sao cho $|A_i|=a_i$ và tổng các phần tử trong mỗi tập A_i đều là bội của 2011.

Tài liệu tham khảo

[1] Hà Huy Khoái, Số học.

[2] Tài liệu từ Internet.

[3] Andreescu, T, *Number theory Structures Examples and Problems*

[4] Andreescu, T.; Feng, Z., 101 Problems in Algebra from the Training of the USA IMO Team, Australian Mathematics Trust, 2001.

[5] Andreescu, T.; Andrica, D.; Feng, Z., 104 Number Theory Problems From the Training of the USA IMO Team, Birkh¨auser, 2006 (to appear).

[6]. v15_n1 Primitive Roots Modulo Primes.