# PRIMITIVE ROOT

Nguyễn Thanh Trà K42 Trường THPT Chuyên ĐHSP HN
★thanhtra1239@yahoo.com ★

Ngày 27 tháng 11 năm 2009

# Mục lục

# 1 Một số định nghĩa và tính chất

**Định nghĩa 1.1. Cấp của một số nguyên.**
*Giả sử $a$ và $m$ là các số nguyên dương nguyên tố cùng nhau. Khi đó số nguyên dương $x$ nhỏ nhất sao cho $a^x \equiv 1 \pmod{p}$ được gọi là cấp của $a$ modulo $m$.*

Ta kí hiệu bậc của $a$ modulo $m$ bởi $ord_m a$
Như vậy, dễ dàng suy ra $ord_m a$ là ước của $\phi(m)$ với mọi $a$.

**Định nghĩa 1.2. Căn nguyên thuỷ.**
*Nếu số nguyên dương $g$ có cấp là $\phi(p) \mod p$ thì $g$ được gọi là căn nguyên thuỷ $\mod p$*

Từ định nghĩa căn nguyên thuỷ, ta có các tính chất

**Tính chất 1.** Nếu $g$ là căn nguyên thuỷ $\mod p$ thì ta có thể biểu diễn hệ thặng dư thu gọn mod $p$ dưới dạng sau:

$$\{1, g, g^2, ..., g^{\phi(p)}\}$$

**Tính chất 2.** Nếu $p$ là số nguyên tố thì $p$ có đúng $\phi(p-1)$ căn nguyên thuỷ.

**Tính chất 3.** Giả sử $p$ là một số nguyên tố lẻ, có căn nguyên thuỷ $g$. Khi đó, hoặc $g$ hoặc $g+p$ là một căn nguyên thuỷ $\mod p^2$.

**Tính chất 4.** 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 $g$ là một căn nguyên thuỷ $\mod p^2$ thì $g$ là căn nguyên thuỷ $\mod p^k$ với mọi số nguyên $k$.

**Tính chất 5.** Nếu $n = 2p^t$, $p$ là số nguyên tố lẻ, $t$ nguyên dương thì $n$ có căn nguyên thuỷ. Cụ thể là, nếu $g$ là căn nguyên thuỷ $\mod p^t$ và $r$ lẻ thì nó là căn nguyên thuỷ mod $2p^t$, còn nếu $r$ chẵn thì $r + p^t$ là căn nguyên thuỷ $\mod 2p^t$.

**Tính chất 6.** 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.

# 2 Căn nguyên thuỷ-những ứng dụng

## 2.1 Bài tập về tính chất căn nguyên thuỷ

Như ta đã biết, căn nguyên thuỷ là một khái niệm quan trọng, có nhiều ứng dụng mạnh trong giải toán. Trong mục này tôi xin giới thiệu một số bài tập về tính chất của căn nguyên thuỷ.

**Ví dụ 1.** *Cho $p = 2^n + 1$ là một số nguyên tố. Chứng minh rằng 3 là căn nguyên thuỷ* mod $p$.

*Lời giải.* Đặt $p = 2^n + 1$
Đầu tiên, ta sẽ chứng minh 3 không là bình phương mod $p$.
Thật vậy, ta chú ý rằng $p \equiv 1 \pmod 4$ và $2^n + 1 \equiv -1 \pmod 3$ (do $n$ phải là luỹ thừa của 2). Khi đó, ta có:

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = -1.$$

Như vậy, 3 không là bình phương mod 3.
Do $\phi(p) = 2^n$ nên $ord_p 3 = 2^k$ (do $ord_p 3 = 2^k | \phi(p)$). Giả sử $k < n$ ta có $3^{2^{n-1}} \equiv 1 \pmod p$.
Mà 3 không là bình phương mod 3 nên $\left(\frac{3}{p}\right) \equiv 3^{2^{n-1}} \pmod p$ suy ra $3^{2^{n-1}} \equiv -1 \pmod p$.
Do đó, $p|1 - (-1) = 2$, điều này vô lí. □

**Ví dụ 2.** *Cho $p$ là một số nguyên tố có dạng $4k + 3$ và $g$ là một căn nguyên thuỷ* mod $p$ *thoả mãn $g^2 \equiv g + 1 \pmod p$. Chứng minh rằng $g - 2$ cũng là một căn nguyên thủy* mod $p$

*Lời giải.* Để chứng minh bài toán, trước hết, ta cần một bổ đề.
**Bổ đề 1.** *Cho $p$ là một số nguyên tố và $g$ là một căn nguyên thuỷ* mod $p$. *Gọi $g'$ là số nghịch đảo của $g$* mod $p$. *Chứng minh rằng $g'$ cũng là một căn nguyên thuỷ* mod $p$.

*Lời giải của bổ đề 1.* Giả sử $g'$ không là căn nguyên thuỷ mod $p$. Khi đó, tồn tại số nguyên dương $j$ sao cho $g'^{\frac{p-1}{j}} \equiv 1 \pmod p$
Do $g'$ là nghịch đảo của $g$ mod $p$ nên $gg' \equiv 1 \pmod p \Rightarrow (gg')^{\frac{p-1}{j}} \equiv 1 \pmod p \Rightarrow g^{\frac{p-1}{j}} \equiv 1 \pmod p$
Điều này trái với giả thiết $g$ là căn nguyên thuỷ mod $p$. □

Trở lại bài toán, đầu tiên, ta sẽ chứng minh $p-1$ là một căn nguyên thuỷ $\mod p$.
Thật vậy, ta có $g^2 \equiv g+1 \pmod p \Rightarrow g(g-1) \equiv 1 \pmod p$
Theo bổ đề 1, ta có $g-1$ là căn nguyên thuỷ $\mod p$. Do đó $(g-1)^{\frac{p-1}{2}} \equiv -1 \pmod p$ hay $(g-1)^{2k+1} \equiv -1 \pmod p$
Mặt khác, từ giả thiết, ta có: $g^2 \equiv g+1 \pmod p \Rightarrow (g-1)^2 \equiv 2-g \pmod p$
Suy ra $(g-1)^{2k+3} \equiv (g-1)^2 \cdot (g-1)^{2k+1} \equiv -1 \cdot (2-g) \pmod p$
Như vậy, để chứng minh $g-2$ là căn nguyên thuỷ $\mod p$ ta chỉ cần chứng minh $(2k+3, p-1) = 1$.
Thật vậy, ta có $(2k+3, p-1) = (2k+3, 4k+2) = 1$.
Tóm lại $g-2$ là căn nguyên thuỷ $\mod p$. □

## 2.2 Một số ứng dụng của căn nguyên thuỷ

Để mở đầu cho những ứng dụng của căn nguyên thuỷ, ta hãy đến với một số ví dụ đơn giản.

**Ví dụ 3.** *Tìm các số nguyên $n > 1$ sao cho:*

$$n | a^{25} - a \text{ với mọi } a \in \mathbb{N}$$

*Lời giải.* Đặt

$$N = \prod_{p \in P}^{p-1|24} p = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$$

Ta sẽ chứng minh $n$ thoả mãn điều kiện của đề bài khi và chỉ khi $n$ là một ước số của $N$.
Theo định lí $Fermat$, ta có:

$$a^{25} - a = a(a^{24} - 1) \equiv 0 \pmod N \text{ với mọi } a \in \mathbb{Z}^+$$

Do đó, mọi ước số nguyên của $N$ đều thoả mãn đề bài.
Giả sử tồn tại một số nguyên dương $n$ không là ước số của $N$ thoả mãn điều kiện đề bài.
Nếu $n$ có một ước số nguyên $p$ không là ước của $N$, thì tồn tại một số $a$ là căn nguyên thuỷ của $p$. Khi đó, $a^{25} - a = a(a^{24} - 1) \equiv 0 \pmod p$ khi và chỉ khi $24 \equiv 0 \pmod{p-1}$. Vô lí.
Nếu $n$ có một ước số chính phương dạng $p^2$, với $a = p$, ta có:

$$p^{25} - p \equiv 0 \pmod{p^2}$$

như thế, không tồn tại $p$ thoả mãn.
Như vậy, $n$ là một ước của $N$. □

Trong bài toán trên, ta nhận thấy rằng giả thiết *với mọi* $a \in \mathbb{N}$ làm cho bài toán yếu đi. Ta hãy suy nghĩ theo một hướng khác. Ta có bài toán:

**Ví dụ 4.** *Tìm ước chung lớn nhất của các số:*

$$a^{561} - a, \text{ với } a = 2, 3, 4, ..., 561$$

*Lời giải.* Tương tự như trên, ta sẽ chứng minh rằng:

$$N = \prod_{p \in P}^{p-1|560} p = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 29 \cdot 41 \cdot 71 \cdot 281$$

là ước chúng lớn nhất của tất cả các số nói trên.
Giả sử ước chúng lớn nhất của $a^{561} - a$, với $a = 2, 3, 4, ..., 561$ là $d$. Ta xét hai trường hợp:

**Trường hợp 1.** Nếu $d$ không có ước nguyên tố lớn hơn 561.
Gọi $p$ là một ước nguyên tố bất kì của $d$, ta có $p < 561$.
Gọi $g$ là một căn nguyên thuỷ của $p$, suy ra $g < 561$ nên $g^{560} - 1 \equiv 0 \pmod{p}$. Do $g$ là căn nguyên thuỷ của $p$ nên $p - 1|560$.
Mặt khác, dễ dàng chứng minh được nếu $p - 1|560$ thì $a^{561} - a \equiv 0 \pmod{p}$ với $a = 2, 3, 4, ..., 561$.
Giả sử $n$ có một ước số dạng $p^2$ với $p$ là số nguyên tố. Khi đó $p^{561} - p \equiv 0 \pmod{p^2}$, vô lí.

**Trường hợp 2.** Nếu $d$ có một ước nguyên tố lớn hơn 561. Ta xét đa thức $f(x) = x^{560} - 1$ là một đa thức bậc 560 có 560 nghiệm $\mod p$.
Mặt khác đa thức $(x-2)(x-3)\cdots(x-561)$ cũng là một đa thức bậv 560 và có 560 nghiệm $\mod p$.
Đồng nhất hệ số của $x^{559}$, ta có:

$$\begin{aligned}
&2 + 3 + 4 + \cdots + 561 \equiv 0 \pmod{p} \\
&\Leftrightarrow \frac{561 \cdot 562}{2} - 1 \equiv 0 \pmod{p} \\
&\Leftrightarrow 561 \cdot 561 \cdot 281 \equiv 1 \pmod{p} \\
&\Leftrightarrow p|2^5 \cdot 5 \cdot 7 \cdot 563 \\
&\Rightarrow p = 563
\end{aligned}$$

Mặt khác, trong trường hợp $a = 2$, ta có $2^{561} \equiv 282 \neq 2 \pmod{563}$.
Tóm lại, từ hai trường hợp 1 và 2, ta có

$$N = \prod_{p \in P}^{p-1|560} p = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 29 \cdot 41 \cdot 71 \cdot 281$$

là ước chung lớn nhất của

$$a^{561} - a, \text{ với } a = 2, 3, 4, ..., 561$$

□

**Nhận xét.** Từ ví dụ trên, ta nhận thấy số 561 không có vai trò quan trọng trong bài toán. Ta hãy tổng quát bài toán:
**Bài toán 3.1.** *Tìm ước chung lớn nhất của các số:*

$$a^k - a, \text{ với } a = 2, 3, 4, ..., k$$

Từ một hướng nhìn nhận khác, ta có một bài toán

**Ví dụ 5** (SP TST 2008)**.** *Tìm các số nguyên tố $p, q$ thoả mãn:*

$$\alpha^{3pq} \equiv \alpha \pmod{3pq} \quad \forall \alpha \in \mathbb{Z}$$

*Lời giải.* Giả sử $p \leq q$ là các số nguyên tố thoả mãn đề bài.
Do $\alpha^{3pq} \equiv \alpha \pmod 3 \quad \forall \alpha \in \mathbb{Z}$ nên nếu chọn $a = -1$ suy ra $p, q$ đều là các số lẻ.
Do $\alpha^{3pq} \equiv \alpha \pmod{3p} \quad \forall \alpha \in \mathbb{Z}$ nên nếu chọn $\alpha$ là một căn nguyên thuỷ của $p$, ta sẽ có $3pq - 1 \equiv 0 \pmod{p-1} \Rightarrow 3q - 1 \vdots p - 1$.
Do $\alpha^{3pq} \equiv \alpha \pmod{3q} \quad \forall \alpha \in \mathbb{Z}$ nên nếu chọn $\alpha$ là một căn nguyên thuỷ của $q$, ta sẽ có $3pq - 1 \equiv 0 \pmod{q-1} \Rightarrow 3q - 1 \vdots p - 1$.
Nếu $p = q$ thì $3p - 1 \vdots p - 1$ nên suy ra $p = q = 3$. Thay vào không thoả mãn vì $4^{27} \equiv 1 \pmod{27}$.
Nếu $q \geq p + 2$ thì $\dfrac{3p-1}{q-1} < 3$ nên $3p - 1 = 2(q - 1)$ hay $2q = 3p + 1$, do đó:

$$3q - 1 = \frac{9p+1}{2} \vdots p - 1 \quad \text{và} \quad (9p + 1) - (9p - 1) = 10 \vdots p - 1$$

suy ra $p = 11, q = 17$. Thay vào, ta thấy thoả mãn điều kiện đề bài. □

**Nhận xét.** Ta thấy trong bài toán trên, số 3 cũng là một số nguyên tố. Như thế, ta hãy nghĩ cách tổng quát bài toán. Và ta có được kết quả sau.

**Ví dụ 6.** *Tìm các số nguyên tố $p, q, r$ thoả mãn:*

$$\alpha^{pqr} \equiv \alpha \pmod{pqr} \quad \forall \alpha \in \mathbb{Z}$$

*Lời giải.* Tương tự cách chứng minh bài toán trên, ta cũng có kết quả sau:

$$pq - 1 \vdots r - 1 \quad qr - 1 \vdots p - 1 \quad sp - 1 \vdots q - 1 \tag{1}$$

Như vậy bài toán đã cho được đưa trở về dạng giải phương trình nghiệm nguyên với các số nguyên tố $p, q, r$ thoả mãn điều kiện (1)

□

Ta hãy nghĩ một cách mở rộng mới cho *ví dụ 5*

**Ví dụ 7.** *Tìm các số $\beta$ sao cho tồn tại các số nguyên tố $p, q$ thoả mãn:*

$$\alpha^{3pq} \equiv \alpha\beta \pmod{3pq} \quad \forall \alpha \in \mathbb{Z}$$

*Lời giải.* Trước hết, ta chú ý tới bổ đề sau:
**Bổ đề 1.** *Cho $p$ là một số nguyên tố, $a, n$ là các số nguyên dương, $(a, n) = 1$. Khi đó phương trình $x^n \equiv a \pmod{p}$ hoặc có $(n, p-1)$ nghiệm hoặc vô nghiệm, tuỳ theo:*

$$a^{\frac{p-1}{(n,p-1)}} \equiv 1 \pmod{p}$$

*có thoả mãn hay không.*
Cách chứng minh bổ trên là khá dễ dàng, xin không nêu ra ở đây.
Trở lại bài toán, ta có:

$$\alpha^{3pq} \equiv \alpha\beta \pmod{3pq} \quad \forall \alpha \in \mathbb{Z}$$

khi và chỉ khi phương trình $x^{3pq-1} \equiv \beta \pmod{3p}$ có $p-1$ nghiệm $\mod p$ và phương trình $x^{3pq-1} \equiv \beta \pmod{3q}$ có $q-1$ nghiệm $\mod q$.
Suy ra:

$$\begin{cases} (3pq-1, p-1) = p-1 \\ (3pq-1, q-1) = q-1 \end{cases} \quad \text{và} \quad \begin{cases} \beta^{\frac{p-1}{(3pq-1,p-1)}} \equiv 1 \pmod{p} \\ \beta^{\frac{q-1}{(3pq-1,q-1)}} \equiv 1 \pmod{q} \end{cases}$$

Từ $(3pq-1, p-1) = p-1$, $(3pq-1, q-1) = q-1$, ta có $p = 11, q = 17$. Thay vào, ta được:

$$\begin{cases} \beta^1 \equiv 1 \pmod{17} \\ \beta^1 \equiv 1 \pmod{11} \end{cases}$$

Ta thấy $\beta = 1$ là số duy nhất thoả mãn.
Như vậy, các số $\beta$ thoả mãn đề bài là $\beta = 1$ □

Ta nhận thấy rằng bài toán trên còn nhiều hướng mở rộng, chẳng hạn với ba biến $p, q, r$. Tất nhiên là chúng ta vẫn giải được các bài toán theo phương pháp trên. Tuy nhiên, trong các trường hợp này tính toán tương đối phức tạp, tôi không tiện nêu ra.

Chúng ta xét thêm một số ví dụ khác.

**Ví dụ 8.** *Tìm số nguyên dương $n$ thoả mãn:*

$$2^n - 1 \vdots n$$

*Lời giải.* Bài toán trên có thể giải rất dễ dàng nhờ phương pháp cấp của số nguyên.
Gọi $p$ là ước nguyên tố nhỏ nhất của $n$. Ta có:

$$2^n - 1 \equiv 0 \pmod{n} \Rightarrow 2^n - 1 \equiv 0 \pmod{p}$$

Mặt khác do $p$ là số nguyên tố nên $2^{p-1} - 1 \equiv 0 \pmod{p}$
Suy và $2^n - 1 \equiv 0 \pmod{p}$ và $2^{p-1} - 1 \equiv 0 \pmod{p}$ suy ra $2^{(n,p-1)} - 1 \equiv 0 \pmod{p}$.
Nếu $(n, p-1) = 1$ ta có $p|1$, suy ra $n = 1$.
Nếu $(n-1, p) \neq 1$ thì $n$ sẽ chia hết cho một số nguyên tố nhỏ hơn $p$ (trái với giả thiết $p$ là ước số nguyên tố nhỏ nhất của $n$.
Như vậy, $n = 1$ thoả mãn đề bài. □

Ta hãy nghĩ mở rộng *ví dụ 9.* Ta có được ta có bài toán:

**Ví dụ 9.** *Tìm các số nguyên $n$ thoả mãn:*

$$n^2 | 2^n + 1$$

*Lời giải.* Giả sử $n > 1$ thoả mãn $n^2|2^n + 1$, khi đó $2^n + 1 \vdots n^2$ nên $n$ là một số lẻ.
Gọi $p$ là ước nguyên tố nhỏ nhất của $n$ Gọi $p$ là ước nguyên tố nhỏ nhất của $n$. Ta có:

$$2^n - 1 \equiv 0 \pmod{n} \Rightarrow 2^n - 1 \equiv 0 \pmod{p}$$

Mặt khác do $p$ là số nguyên tố nên $2^{p-1} - 1 \equiv 0 \pmod{p}$
Suy và $2^{2n} - 1 \equiv 0 \pmod{p}$ và $2^{p-1} - 1 \equiv 0 \pmod{p}$ suy ra $2^{(2n,p-1)} - 1 \equiv 0 \pmod{p}$.
Do $p$ là ước nguyên tố nhỏ nhất của $n$ nên $(2n, p-1) = 2$.
Như vậy, ta có $p|3$. Suy ra $p = 3$. Giả sử $n = 3^k d$ với $(k, d) = 1$. Vì $2^n + 1 \equiv 0 \pmod{n^2}$ nên $2^{2n} \equiv 1 \pmod{3^{2k}}$.
Do 2 là căn nguyên thuỷ của $3^k$ nên $\phi(3^{2k})|2n$ hay $2 \cdot 3^{2k-1}|2 \cdot 3^k \cdot d$. Suy ra $k \geq 2k - 1$ hay $k \leq 1$. Vậy $k = 1, n = 3d$ với $(d, 3) = 1$.
Gọi $q$ là ước nguyên tố nhỏ nhất của $d$. Khi đó do $(3, d) = 1$ nên $q \geq 5$. Đặt $k = ord_q 2 = k$.
Do $2^{2n} \equiv 1 \pmod{q}$ nên $k|2n = 6d$ và $k|q - 1$ hay $(6d, q-1)$=k. Do $(6d, q-1) = 2$ nên $k|2$, suy ra $k = 2$.
Như vậy, $2^2 = 4 \equiv 1 \pmod{q}$ suy ra $q = 3$ (vô lí).
Vậy điều giả sử là sai nên $d = 1$ và $n = 3$. Thử lại thấy $n = 3$ đúng.
Vậy số nguyên dương $n$ thoả mãn đề bài là $n = 3$.

Như ta đã thấy, việc biến hoá số chia cho ta một bài toán rất thú vị. Tiếp tục mở rộng, ta được bài toán: □

**Ví dụ 10.** *Tìm tất cả các số nguyên $n > 1$ sao cho tồn tại duy nhất số nguyên dương $a$ với $0 < a < n!$ thoả mãn:*

$$a^n + 1 \equiv 0 \pmod{n!}$$

*trong đó $n!$ là tích của các số nguyên dương từ 1 đến $n$*

*Lời giải.* Ta thấy $n = 2$ thoả mãn.
Với $n \geq 4$, $n$ là số chẵn, suy ra $a^n$ là số chính phương và $3|n!$ nhưng $3 \not| a^n + 1$. Như vậy, $n$ là số lẻ.
Đặt $n! = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ với $p_i$ là các số nguyên tố phân biệt. Theo *định lí Trung Hoa về phần dư*, phương trình $a^n + 1 \equiv 0 \pmod{n!}$ có nghiệm $a$ duy nhất nếu phương trình $a^n + 1 \equiv 0 \pmod{{p_i}^{k_i}}$ có nghiệm duy nhất với $i = 1, 2, ...r$.
Ta sẽ chứng minh rằng phương trình $a^n + 1 \equiv 0 \pmod{2^k}$ có nghiệm duy nhất.

Ta có:

$$a^n + 1 \equiv (a+1)\left(\sum_{i=0}^{n-1}(-1)^i a^i\right) \equiv 0 \pmod{p}$$

Mà $\sum_{i=0}^{n-1}(-1)^i a^i$ là số lẻ nên ta có $a + 1 \equiv 0 \pmod{2^k}$
Kí hiệu số mũ của $p$ trong phân tích thành thừa số nguyên tố của $n!$ là $v_p(n!)$. Ta xét hai trường hợp:

**Trường hợp 1.** $n \geq 3$, $n$ là một số nguyên tố. Ta có $v_p(n!) = 1$
Gọi $p \geq 3$ là một ước số nguyên tố của của $n!$, $p \neq n$ và gọi $k = v_p(n!)$
Gọi $g$ là một căn nguyên thuỷ $\mod p^k$
Suy ra $g^{\frac{\phi(p^k)}{2}} \equiv -1 \pmod{p^k}$
Do $(a, n) = 1$ nên tồn tại $x \in \{1, 2, ..., \phi(p^k)\}$ thoả mãn $a \equiv g^x \pmod{p^k}$
Như vậy $a^n \equiv -1 \pmod{p^k} \Leftrightarrow g^{nx} \equiv g^{\frac{\phi(p^k)}{2}} \pmod{p^k} \Leftrightarrow nx \equiv \dfrac{\phi(p^k)}{2} \pmod{\phi(p^k)}$
Do đó, $a$ có nghiệm duy nhất $\mod p^k$ khi và chỉ khi $x$ có nghiệm duy nhất $\mod \phi(p^k)$ Mặt khác do $gcd\left(n, \phi(p^k)\right) = gcd\left(n, p^{k-1}(p-1)\right) = 1$ nên $x$ có nghiệm duy nhất $\mod \phi(p^k)$
Suy ra $a$ có nghiệm duy nhất $\mod n!$ với $n \geq 3$ là số nguyên tố.

**Trường hợp 2.** $n$ là hợp số, $n \geq 3$.
Gọi $p$ là một ước số nguyên tố phân biệt với $n$, $p \geq 3$ ($p$ luôn tồn tại do $n$ là một hợp số lẻ).
Suy ra $k = v_p(n!) \geq 2$
Gọi $g$ là một căn nguyên thuỷ $\mod p^k$
Suy ra $g^{\frac{\phi(p^k)}{2}} \equiv -1 \pmod{p^k}$
Do $(a, n) = 1$ nên tồn tại $x \in \{1, 2, ..., \phi(p^k)\}$ thoả mãn $a \equiv g^x \pmod{p^k}$
Như vậy $a^n \equiv -1 \pmod{p^k} \Leftrightarrow g^{nx} \equiv g^{\frac{\phi(p^k)}{2}} \pmod{p^k} \Leftrightarrow nx \equiv \dfrac{\phi(p^k)}{2} \pmod{\phi(p^k)}$ hay $nx \equiv \dfrac{p^{k-1}(p-1)}{2} \pmod{p^{k-1}(p-1)}$.
Mặt khác, do $p|n$ nên $\gcd(n, \dfrac{p^{k-1}(p-1)}{2}) \neq 1$ suy ra phương trình $nx \equiv \dfrac{p^{k-1}(p-1)}{2} \pmod{p^{k-1}(p-1)}$ có nhiều hơn 1 nghiệm.

Tóm lại $n$ là số nguyên tố thoả mãn đề bài. □

Ta hãy xét các bài toán có dạng khác.

**Ví dụ 11** (Balkan 1999)**.** *Cho $p$ là một số nguyên tố có dạng $3n+2$. Đặt:*

$$S = \{y^2 - x^3 - 1 | x, y \text{ là các số nguyên, } 0 < x, y < p-1\}$$

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

*Chứng minh.* Ta có nhận xét: Nếu $p$ là một số nguyên tố. Khi đó các số $1^k, 2^k, ..., (p-1)^k$ lập thành một hệ thặng dư thu gọn $\mod p$ khi và chỉ khi $(k, p-1)=1$.
Chứng minh nhận xét trên rất đơn giản, xin dành cho bạn đọc.

Trở lại bài toán, do $1, 2, ...p-1$ là một hệ thặng dư $\mod p$ mà $(3, p) = 1$ nên $\{1^3, 2^3, ...(p-1)^3\}$ là một hệ thặng dư thu gọn $\mod p$.
Khi đó, với mỗi $0 \le y \le p-1$ tồn tại duy nhất số nguyên $x, 0 \le x \le p-1$ sao cho $x^3 \equiv y^2 - 1 \pmod p$ tức là trong tập $S$ có nhiều nhất $p$ phần tử chia hết cho $p$

□

**Nhận xét.** Từ bài toán trên, ta có thể mở rộng thành bài toán sau đây:
**Bài toán 11.1.** *Cho $p$ là một số nguyên tố có dạng $kl+2$. Đặt*

$$S = \{y^j - x^k - \alpha | j, k \text{ là các số nguyên, } 0 \le j, k \le p-1\}$$

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

Chúng ta hãy đến với một ví dụ khác.

**Ví dụ 12.** *Chứng minh rằng tồn tại một phân hoạch của tập hợp $A = \{1^3, 2^3, ..., 2000^3\}$ thành 25 tập hợp con thoả mãn tổng tất cả các phần tử trong một tập hợp con chia hết cho $2001^2$*

*Lời giải.* Gọi $a_i$ là các số nguyên dương phân biêt $1 \le a_i \le 2001$ thoả mãn $a_i + a_j \ne 2001$. Xét:

$$\begin{aligned}
&\sum_{i=1}^{n} \left(a_i^3 + (2001 - a_1)^3\right) \\
&= \sum_{i=1}^{n} \left(2001^3 - 3 \cdot 2001^2 a_i + 3 \cdot 2001 a_i^2\right) \\
&\equiv 2001 \sum_{i=1}^{n} a_i^2 \pmod{2001^2}
\end{aligned}$$

Suy ra $\sum_{i=1}^{n}(a_i^3+(2001-a_1)^3)\equiv 0 \pmod{2001^2} \Leftrightarrow \sum_{i=1}^{n} a_i^2 \equiv 0 \pmod{667}$.
Gọi $p$ là một số nguyên tố bất kì, đặt $g$ là một căn nguyên thuỷ của $p$ và lấy $k>2, k|p-1$.
Với mọi $r$, $0\le r\le \dfrac{p-1}{k}$, ta có:

$$\sum_{i=0}^{k-1}\left(g^{\frac{p-1}{k}i}+r\right)^2 \equiv g^{2r}\sum_{i=1}^{k-1} g^{\frac{2(p-1)}{k}i} \pmod{p}$$
$$\equiv g^{2r}\frac{g^{2(p-1)}-1}{g^{\frac{2(p-1}{k}}-1}\equiv 0 \pmod{p}$$

Từ $\dfrac{2(p-1)}{k}<p-1$ và $g^{\frac{2(p-1}{k}}-1\neq 0$ nên tổng bình phương của những phần tử của mỗi $\dfrac{p-1}{k}+1$ tập con của tập hợp các hệ thặng dư *modulo p*.
Do đó, ta có $\{0\}=S_{p,k,0}$ và $S_{p,k,r}=\{g^{\frac{p-1}{k}i+r}|0\le i\le p-1\}$ với mỗi $1\le r\le \dfrac{p-1}{k}$ luôn có tổng các phần tử chia hết cho p.
Với mọi $0\le i\le 23\le j\le 30$, gọi $1\le r(i,j)\le 2001$ là các số thoả mãn $r(i,j)\equiv i \pmod{23}, r(i,j)\equiv j \pmod{29}, r(i,j)\equiv 1 \pmod 3$. Như thế, ta thấy rằng các số $r(i,j)$ là duy nhất với mỗi $i,j$
Với mỗi $i,j,k,l$ thoả mãn $r(i,j)+r(k,l)\equiv 2 \pmod 3$ thì $r(i,j)+r(k,l)\neq 2001$.
Ta xét tập hợp: $X(a,b)=\{r(i,j)|i\in S_{23,11,a}\wedge j\in S_{29,4,b}\}\cap$ với $0\le a\le 2$ và $0\le b\le 7$, ta có 24 tập hợp, các tập hợp đôi một không có phần tử chung .
Mặt khác, ta có:

$$\sum_{x\in X(a,b)} x^2\equiv 29\cdot 0\equiv 0 \pmod{23}$$
$$\sum_{x\in X(a,b)} x^2\equiv 23\cdot 0\equiv 0 \pmod{29}$$
$$\sum_{x\in X(a,b)} x^2\equiv 0 \pmod{667}$$

nên:

$$\sum_{x\in X(a,b)\vee(2001-x)|x\in X(a,b)} x^3\equiv 0 \pmod{2001^2}$$

Mặt khác, ta có

$$\bigcap_{0\le a\le 2,0\le b\le 7} S(a,b)\cap S\{2008-x|x\in S(a,b)\}\subset\{1,2,3,...2000\}$$

Mà:

$$\sum_{i=1}^{2001} i^3 = \left(\sum_{i=1}^{2001} i\right)^2 = \left(\frac{2001 \cdot 2001}{2}\right)^2 \equiv 0 \pmod{p}$$

Như vậy ta có cách chia tập hợp $A = \{1^3, 2^3, ..., 2000^3\}$ thành 25 tập hợp con thoả mãn tổng tất cả các phần tử trong một tập hợp con chia hết cho $2001^2$ □

**Ví dụ 13.** *Cho $p$ là một số nguyên tố lẻ và đặt $S = \{n_1, n_2, ...n_k\}$ là một tập hợp bất kì của các số chính phương nguyên tố cùng nhau với $p$. Tìm số $k$ nhỏ nhất sao cho tồn tại một tập con $A$ của tập $S$ thoả mãn tích các phần tử của $A$ đồng dư với 1 $\mod p$*

*Lời giải.* Ta sẽ chứng minh $k = \dfrac{p-1}{2}$ là số cần tìm.

Nếu $k < \dfrac{p-1}{2}$, ta xét tập hợp $S = \{g^2, g^2, ...g^2\}$ của $k$ phần tử $g^2$. Khi đó, tích mọi phần tử của $S$ đều có dạng $g^{2a}$ với $a < \frac{p-1}{2}$. Do $g$ là căn nguyên thuỷ của $p$ nên $g^{2a}$ không đồng dư với 1 $\mod p$.

Như vậy $k \geq \dfrac{p-1}{2}$.

Xét tập hợp $S = \{n_1, n_2, ...n_k\}$ và ta viết $n_i = g^{a_i}$ với mọi $i$.

Tích các tập hợp bất kì của $S$ có dạng $g^{2A}$ với $A$ là tổng một số phần tử của tập hợp $J = \{\alpha_1, \alpha_2, ...\alpha_k\}$

Ta chứng minh rằng với mọi tập hợp có lớn hơn $\dfrac{p-1}{2}$ phần tử ta có thể chọn ra một tập con có tổng các phần tử chia hết cho $\dfrac{p-1}{2}$.

Thật vậy, xét các số:

$$\alpha_1, \alpha_1 + \alpha_2, \alpha_1 + \alpha_2 + \alpha_3, ..., \alpha_1 + \alpha_2 + \cdots + \alpha_{\frac{p-1}{2}}$$

Ta thấy có tất cả $\dfrac{p-1}{2}$ số. Nếu trong tập hợp trên có một phần tử chia hết cho $\dfrac{p-1}{2}$, ta có điều phải chứng minh.

Nếu trong tập hợp trên không có phần tử nào chia hết cho $\dfrac{p-1}{2}$, suy ra tồn tại $i, j, \quad i < j$ sao cho:

$$\alpha_1 + \alpha_2 + \cdots \alpha_i \equiv \alpha_1 + \alpha_2 + \cdots \alpha_j \pmod{p}$$

Suy ra $\alpha_i + \alpha_{i+1} + \cdots \alpha_j \equiv 0 \pmod{p}$.

Tóm lại trong tập hợp $J = \{\alpha_1, \alpha_2, ...\alpha_k\}$ luôn chọn được một số phần tử sao cho tổn các phần tử này chia hết cho $\dfrac{p-1}{2}$ Vậy số nhỏ nhất cần tìm là $k = \dfrac{p-1}{2}$ □

**Nhận xét.** Bằng phương pháp tương tự, ta có thể chứng minh được bài toán:

**Bài toán 13.1** *Cho $p$ là một số nguyên tố lẻ và đặt $S = \{n_1^m, n_2^m, ...n_k^m\}$ là một tập hợp bất kì của các số nguyên tố cùng nhau với $p$. Tìm số $k$ nhỏ nhất sao cho tồn tại một tập con $A$ của tập $S$ thoả mãn tích các phần tử của $A$ đồng dư với 1* $\mod p$

Giải tương tự như trên, ta có số $k$ nhỏ nhất cần tìm là $k\dfrac{p-1}{m}$

**Lời kết.** Căn nguyên thuỷ là một lí thuyết rất mạnh, có tính ứng dụng cao trong giải toán số học. Nhưng vì dung lượng của bài viết không nhiều nên tôi chưa thể giới thiệu hết các ứng dụng của nó. Cácvấn đề còn lại sẽ được trình bày trong thời gian sớm nhất có thể.

# 3 Một số bài tập

Để kết thúc chuyên đề, tôi xin giới thiệu một số bài tập để các bạn sử dụng căn nguyên thuỷ một cách thành thạo.

**Bài tập 1.** *Cho $n = 2^h + 1$. Chứng minh rằng $n$ là số nguyên tố nếu và chỉ nếu $3^{\frac{n-1}{2}} \equiv -1 \pmod{p}$*

**Bài tập 2.** *Cho $p$ là một số nguyên tố. Chứng minh rằng có ít nhất $\dfrac{\phi(p-1)}{2}$ số $g$ thoả mãn $0 < g < p$ và $g$ là một căn nguyên thủy của $p^k$ với mọi số tự nhiên $k$.*

**Bài tập 3.** *Giả sử rằng $4^n + 2^n + 1$ là một số nguyên tố. Chứng minh rằng $n$ là luỹ thừa của 3.*

**Bài tập 4.** *Cho $p$ là số nguyên tố với $p > \left(\dfrac{p-1}{\phi(p-1)}\right)^2 2^{2k}$, với $k$ là số các ước nguyên tố của $p-1$. $M$ là một số nguyên bất kì. Chứng minh rằng trong tập hợp $\{M+1, M+2, ..., M+2\left[\dfrac{p-1}{\phi(p-1)}2k\sqrt{p}\right] - 1\}$ tồn tại ít nhất một căn nguyên thuỷ $\mod p$*

**Bài tập 5.** *Tìm các bộ ba số nguyên tố $(p, q, r)$ thoả mãn:*

$$p|q^r + 1 \quad q|r^p + 1 \quad r|p^q + 1$$

**Bài tập 6.** *Cho $p$ là một số nguyên tố và $k \geq 2$ là một số nguyên dương. Giả sử $q$ là ước số nguyên tố nhỏ nhất của $k$. Chứng minh rằng:*

$$p^k - p^{\frac{k}{q}} \geq \phi(p^k - 1)$$