BẬC CỦA SỐ NGUYÊN - CĂN NGUYÊN THUỶ

Phạm Hy Hiếu – Toán PTNK 07-10

(chuyên đề Toán học số 9 PTNK ĐHQG TPHCM)

1. Bậc của một số nguyên:

Cho trước 2 số nguyên dương a, m thoả mãn điều kiện $\gcd(a, m) = 1$.

Từ định lý Euler ta biết rằng $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$. Vậy nên sẽ tồn tại một số nguyên dương x nhỏ nhất sao cho $a^x \equiv 1 (\mathrm{mod}\, m)$. Ta gọi số x như thế là bậc của a theo modulo m và ký hiệu là $x = \mathrm{ord}_m\, a$. Ta cũng có thể nói rằng:

$$\boxed{x = \mathrm{ord}_m\, a \Leftrightarrow \begin{cases} a^x \equiv 1 (\mathrm{mod}\, m) \\ \forall x_0 \in \mathbb{N}^*, x_0 < x \Rightarrow a^{x_0} \not\equiv 1 (\mathrm{mod}\, m) \end{cases}}$$

Ví dụ 1.1. Tìm $\mathrm{ord}_2\, 5$ và $\mathrm{ord}_{11}\, 5$.

Bằng phép thử trực tiếp ta có:

$$2^1 = 2 \equiv 2 (\mathrm{mod}\, 5);\ 2^2 = 4 \equiv 4 (\mathrm{mod}\, 5); 2^3 = 8 \equiv 3 (\mathrm{mod}\, 5); 2^4 = 16 \equiv 1 (\mathrm{mod}\, 5)$$

$$5^1 = 5 \equiv 5 (\mathrm{mod}\, 11); 5^2 = 25 \equiv 3 (\mathrm{mod}\, 11); 5^3 = 125 \equiv 4 (\mathrm{mod}\, 11);$$

$$5^4 = 625 \equiv 9 (\mathrm{mod}\, 11); 5^5 = 3125 \equiv 1 (\mathrm{mod}\, 11)$$

Vậy $\mathrm{ord}_2\, 5 = 4$ và $\mathrm{ord}_{11}\, 5 = 5$.

Sau đây ta khảo sát một số tính chất của bậc.

Định lý 1.1. Cho $a, m, \in \mathbb{N}^*$ thoả điều kiện $\gcd(a, m) = 1$. Khi đó:

$$\forall x \in \mathbb{N}^*, a^x \equiv 1 (\mathrm{mod}\, m) \Leftrightarrow \mathrm{ord}_m\, a \,|x.$$

Chứng minh:

Giả sử $a^x \equiv 1 (\mathrm{mod}\, m)$, theo thuật toán chia thì tồn tại duy nhất cặp số tự nhiên (q, r) sao cho:

$$x = q\, \mathrm{ord}_m\, a + r \text{ và } 0 \le r < \mathrm{ord}_m\, a$$

Ta sẽ chứng minh $r = 0$. Thật vậy, giả sử ngược lại, tức là $r \in \mathbb{N}^*$ và $r < \mathrm{ord}_m\, a$, ta có:

$$a^x = a^{q\, \mathrm{ord}_m\, a + r} = \left(a^{\mathrm{ord}_m\, a}\right)^q \cdot a^r \equiv a^r (\mathrm{mod}\, m) \Rightarrow a^r \equiv a^x \equiv 1 (\mathrm{mod}\, m)$$

Hơn nữa $r \in \mathbb{N}^*$ và $r < \mathrm{ord}_m\, a \Rightarrow \exists r \in \mathbb{N}^*, r < \mathrm{ord}_m\, a$ và $a^r \equiv 1 (\mathrm{mod}\, m)$, điều này trái với tính nhỏ nhất của bậc của một số nguyên a theo modulo m.

Định lý được chứng minh.

Chiều còn lại của định lý là hiển nhiên vì:

$$\mathrm{ord}_m\, a \,|x \Rightarrow \exists k \in \mathbb{N}^*, x = k\, \mathrm{ord}_m\, a \Rightarrow a^x = \left(a^{\mathrm{ord}_m\, a}\right)^k \equiv 1 (\mathrm{mod}\, m)$$

Vậy định lý được chứng minh hoàn toàn. ■

Chú ý rằng **Định lý 1.1.** cho phép ta tìm tất cả nghiệm x của phương trình đồng dư:

$$a^x \equiv 1 (\mathrm{mod}\, m)$$

Đó là tất cả các số có dạng $x_k = k\, \mathrm{ord}_m\, a$ với $k \in \mathbb{N}^*$. Như vậy, chỉ cần xác định $\mathrm{ord}_m\, a$ là ta có thể sinh ra tất cả các nghiệm của phương trình đồng dư trên. Việc này giúp cho thuật

toán xác định tập nghiệm của phương trình ấy đơn giản hơn nhiều, vì ta chỉ cần xét tối đa là $\varphi(m)$ trường hợp.

Hệ quả 1.1. Cho $a, m \in \mathbb{N}^*$ thoả điều kiện $\gcd(a,m) = 1$. Khi đó, $\text{ord}_m\, a \mid \varphi(m)$.

Chứng minh:

Theo định lý Euler ta có $a^{\varphi(m)} \equiv 1 (\text{mod}\, m)$ nên từ **định lý 1.1.** suy ra ngay $\text{ord}_m\, a \mid \varphi(m)$.

Định lý 1.2. Nếu $a, n \in \mathbb{N}^*$ và $\gcd(a,n) = 1$ thì $a^i \equiv a^j (\text{mod}\, m) \Leftrightarrow i \equiv j (\text{mod}\, \text{ord}_m\, a)$

Chứng minh:

Không mất tính tổng quát, ta có thể giả sử $i \geq j$. Thế thì:

$$a^i \equiv a^j (\text{mod}\, m) \Leftrightarrow a^j\left(a^{i-j} - 1\right) \equiv 0 (\text{mod}\, m) \Leftrightarrow a^{i-j} \equiv 1 (\text{mod}\, m)\ \left(\text{vì } \gcd(a,n) = 1 \Rightarrow \gcd\left(a^j, n\right) = 1\right)$$

Theo **định lý 1.1.** điều này tương đương với:

$$\text{ord}_m\, a \mid (i-j) \text{ hay } i \equiv j (\text{mod}\, \text{ord}_m\, a)$$

Vậy định lý được chứng minh hoàn toàn. ■

Hệ quả 1.2. Nếu $\gcd(a,m) = 1$ thì $a^1, a^2, \dots, a^{\text{ord}_m\, a}$ đôi một không đồng dư với nhau theo modulo m.

Chứng minh:

Giả sử tồn tại $i, j \in \{1,2, \dots, \text{ord}_m\, a\}$ sao cho $i \neq j$ và $a^i \equiv a^j (\text{mod}\, m)$. Theo **định lý 1.2.** thì:

$$i \equiv j (\text{mod}\, \text{ord}_m\, a)$$

Nhưng vì $i \neq j$ và $1 \leq i, j \leq \text{ord}_m\, a$ nên $\text{ord}_m\, a \nmid (i-j)$. Mâu thuẫn này cho ta đpcm. ■

Định lý 1.3. Nếu $a \equiv b (\text{mod}\, m)$ thì $\text{ord}_m\, a = \text{ord}_m\, b$.

Chứng minh:

Giả sử $a \equiv b (\text{mod}\, m)$, ta có:

$$\begin{cases} a^{\text{ord}_m\, b} \equiv b^{\text{ord}_m\, b} \equiv 1 (\text{mod}\, m) \\ b^{\text{ord}_m\, a} \equiv a^{\text{ord}_m\, b} \equiv 1 (\text{mod}\, m) \end{cases} \Rightarrow \begin{cases} \text{ord}_m\, a \mid \text{ord}_m\, b \\ \text{ord}_m\, b \mid \text{ord}_m\, a \end{cases} \Rightarrow \text{ord}_m\, a = \text{ord}_m\, b$$

Định lý được chứng minh. ■

Định lý 1.4. Cho $a, b \in \mathbb{N}^*$ thoả điều kiện $\gcd(a,m) = 1$. Khi đó, với $k \in \mathbb{N}^*$ bất kì:

$$\text{ord}_m\, a^k = \frac{\text{ord}_m\, a}{\gcd(\text{ord}_m\, a\,, k)}$$

Chứng minh:

Trước hết, đặt $\gcd(ord_m\, a\,, k) = d$ thế thì:

$$(a^k)^{\frac{\text{ord}_m\, a}{d}} = a^{\frac{k}{d}.\text{ord}_m\, a} = \left(a^{\text{ord}_m\, a}\right)^{\frac{k}{d}} \equiv 1 (\text{mod}\, m)\ \left(\text{vì } \frac{k}{d} \in \mathbb{Z}\right)$$

Bây giờ, giả sử $\text{ord}_m\, a^k = \alpha < \dfrac{\text{ord}_m\, a}{d}$, thế thì theo định lý 1.1. ta phải có:

$$\alpha \mid \frac{\text{ord}_m\, a}{\gcd(ord_m\, a\,, k)} \Rightarrow \gcd(\alpha, k) = 1$$

Mặt khác ta có $a^{k\alpha} \equiv 1 (\text{mod}\, m)$ nên cũng theo **Định lý 1.1.** thì $\text{ord}_m\, a \mid k\alpha$, mà $\gcd(\alpha, k) = 1$ nên chỉ có thể xảy ra một trong 2 khả năng sau:

1. $\text{ord}_m\, a \mid k \Rightarrow a^k \equiv 1 (\text{mod}\, m) \Rightarrow \alpha | k$, mà $\gcd(\alpha, k) = 1$ nên ta phải có $k = \alpha = 1$, điều này là vô lý vì $k \in \mathbb{N}^*$ cho trước bất kì.

2. $\text{ord}_m\, a \mid \alpha \Rightarrow \text{ord}_m\, a | \frac{\text{ord}_m\, a}{\gcd(ord_m\, a\,, k)} \Leftrightarrow \gcd(ord_m\, a\,, k) = 1, \forall k \in \mathbb{N}^*$, vô lý.

Hai mâu thuẫn trên cho ta kết luận của định lý. ■

Định lý 1.5. Cho p là một số nguyên tố và $d | p - 1$. Khi đó, số các số nguyên dương không lớn hơn $p - 1$ là có bậc theo modulo p đúng bằng d là $\varphi(d)$.

Chứng minh:

Trước tiên ta chứng minh bổ đề sau:

$$\forall n \in \mathbb{N}^*, \sum_{d|n} \varphi(d) = n$$

Thật vậy, gọi C_d là tập hợp các số m thoả điều kiện $1 \le m \le n$ sao cho $\gcd(n, m) = d$, thế thì:

$$\gcd\left(\frac{n}{d}, \frac{m}{d}\right) = 1, \forall n \in C_d$$

Theo định nghĩa của hàm Euler ta có:

$$|C_d| = \varphi\left(\frac{n}{d}\right)$$

Từ đây ta suy ra:

$$n = |\{1,2, \dots, p-1\}| = \sum_{d|n} |C_d| = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d)$$

(vì khi d "chạy" khắp tập ước của n thì $\frac{n}{d}$ cũng "chạy" hết tập ấy)

Vậy bổ đề được chứng minh hoàn toàn.

Quay lại với việc chứng minh định lý, với mọi $d \in \mathbb{N}^*$ thoả $d | p - 1$, ta ký hiệu:

$$f(d) \coloneqq \left|\left\{m \in \{1,2, \dots, p-1\} \text{ sao cho } \text{ord}_p\, m = d\right\}\right|$$

Do mỗi số nguyên m nằm trong tập hợp $\{1,2, \dots, p-1\}$ đều nguyên tố cùng nhau với p nên sẽ tồn tại $\text{ord}_p\, m$, hơn nữa $\text{ord}_p\, m \mid \varphi(p) = p - 1, \forall m \in \{1,2, \dots, p-1\}$ nên:

$$\sum_{d|p-1} f(d) = p - 1$$

Từ bổ đề ta suy ra:

$$\sum_{d|p-1} f(d) = \sum_{d|p-1} \varphi(d)$$

Để thu được kết luận của định lý, tức là $f(d) = \varphi(d), \forall d | p - 1$, ta sẽ chứng minh rằng:

$$f(d) \le \varphi(d), \forall d | p - 1$$

Thật vậy, nếu $f(d) = 0$ thì điều phải chứng minh là hiển nhiên đúng.
Nếu $f(d) > 0$ thì tồn tại số nguyên dương a sao cho $\text{ord}_p\, a = d$. Khi đó, theo **hệ quả 1.2.** thì $a^1, a^2, \dots, a^{\text{d}}$ đôi một không đồng dư với nhau theo modulo p. Mặt khác, với mỗi $k \in \mathbb{N}^*$, ta đều có $(a^k)^d \equiv 1 (\text{mod}\, p)$ nên a^k là một nghiệm của đa thức $x^d - 1$ trên $\mathbb{Z}/p\mathbb{Z}$. Đa thức này không đồng nhất với 0 nên nó có không quá d nghiệm. Hơn nữa mỗi nghiệm này phải có dạng a^k nào đó $(1 \le k \le d)$. Vậy nếu tồn tại một phần tử $m \in \{1,2, \dots, p-1\}$ sao cho $\text{ord}_p\, m = d$ thì cũng có không quá $\varphi(d)$ số như thế. Do đó, $f(d) \le \varphi(d)$ và do các lý luận trên, định lý đã được chứng minh hoàn toàn. ■

2. Căn nguyên thủy:
Nếu $(r, n) = 1$ và $\text{ord}_n\, r = \varphi(n)$ thì r được gọi là một căn nguyên thủy modulo n.
Từ các tính chất đã trình bày về bậc của số nguyên, ta dễ dàng suy ra các tính chất cơ bản của căn nguyên thủy như sau:

Định lý 2.1. Nếu r là căn nguyên thủy modulo n thì $r^k \equiv 1 \pmod m$ khi và chỉ khi $\varphi(n) | k$.

Định lý 2.2. Nếu r là căn nguyên thủy modulo n thì $r^1, r^2, \dots, r^{\varphi(n)}$ lập thành hệ thặng dư thu gọn modulo n.

Định lý 2.3. Nếu r là căn nguyên thủy modulo n thì s là căn nguyên thủy modulo n khi và chỉ khi $s \equiv r^k \pmod n \left(\left(k, \varphi(n)\right) = 1 \right)$.
Chứng minh:
Điều kiện đủ của định lý là hiển nhiên vì theo **định lý 1.3.** thì:

$$\text{ord}_n\, s = \text{ord}_n\, r^k = \frac{\text{ord}_n\, r}{(\text{ord}_n\, r\,, k)} = \frac{\varphi(n)}{\left(k, \varphi(n)\right)} = \varphi(n)$$

Với điều kiện cần, ta giả sử s là một căn nguyên thủy của modulo n, thế thì $(s, n) = 1$, hay s nằm trong hệ thặng dư thu gọn modulo n, theo **định lý 2.2.** thì tồn tại k sao cho $s \equiv r^k (\text{mod}\, n)$. Lại theo **định lý 1.3.** thì:

$$\varphi(n) = \text{ord}_n\, s = \text{ord}_n\, r^k = \frac{\text{ord}_n\, r}{(\text{ord}_n\, r\,, k)} = \frac{\varphi(n)}{\left(k, \varphi(n)\right)}$$

Suy ra $\left(k, \varphi(n)\right) = 1$. ■

Ta thấy rằng chỉ cần $(m, a) = 1$ thì đã có thể suy ra sự tồn tại của $\text{ord}_m\, a$, tuy nhiên sự tồn tại của căn nguyên thủy modulo n nào đó thì không phải là một tính chất hiển nhiên. Sau đây ta sẽ khảo sát sự tồn tại của căn nguyên thủy.

Định lý 2.4. Mọi số nguyên tố đều có căn nguyên thủy.

Đây là hệ quả trực tiếp của **định lý 1.5.** vì nếu ta gọi S là tập hợp các căn nguyên thủy của số nguyên tố p thì $|S| = \left|\{k \leq p-1 \middle| \operatorname{ord}_p k = p-1\}\right| = \varphi(p-1) \neq 0$. ■

Định lý 2.5. Mọi số nguyên dương có dạng p^2 với p là một số nguyên tố đều có căn nguyên thủy.

Chứng minh:

Gọi r là một căn nguyên thủy của p. Đặt $\operatorname{ord}_{p^2} r = k$ thì $r^k \equiv 1 (\operatorname{mod} p^2)$ nên $r^k \equiv 1 (\operatorname{mod} p)$, suy ra $\operatorname{ord}_p r = p-1 | k$, hơn nữa $k | \varphi(p^2) = p(p-1)$, vậy nên $k = p-1$ hoặc $k = p(p-1)$.

Nếu $k = p(p-1) = \varphi(p^2)$ thì theo định nghĩa, r là căn nguyên thủy của p^2.

Nếu $k = p-1$ thì $r^{p-1} \equiv 1 (\operatorname{mod} p^2)$.

Đặt $s = r + p$, ta có $s \equiv r (\operatorname{mod} p)$ nên $\operatorname{ord}_p s = \operatorname{ord}_p r = p-1$. Lý luận tương tự như trên ta cũng có $\operatorname{ord}_{p^2} s \in \{p-1; p(p-1)\}$. Mặt khác:

$$s^{p-1} = (r+p)^{p-1} = \sum_{k=0}^{p-1} \binom{p-1}{k} r^k p^{p-1-k} \equiv r^{p-1} + r^{p-2} p(p-1) \equiv 1 - r^{p-2} (\operatorname{mod} p^2)$$

Vậy nếu $\operatorname{ord}_{p^2} s = p-1$ thì $r^{p-2} \equiv 0 (\operatorname{mod} p^2)$, mâu thuẫn vì r là căn nguyên thủy của p nên $(r, p) = 1$. Do đó, $\operatorname{ord}_{p^2} s = p(p-1) = \varphi(p^2)$, tức $s = r + p$ là căn nguyên thủy của p^2.

Định lý được chứng minh. ■

Định lý 2.6. Mọi số nguyên dương có dạng p^k trong đó p là một số nguyên tố còn k nguyên dương bất kỳ đều có căn nguyên thủy.

Chứng minh:

Gọi r là một căn nguyên thủy của p^2, ta sẽ chứng minh r cũng là căn nguyên thủy của p^k, với mọi k nguyên dương. Đặt $m = \operatorname{ord}_{p^k} r$, ta có $r^m \equiv 1 (\operatorname{mod} p^k)$ nên $m | \varphi(p^k) = p^{k-1}(p-1)$. Hơn nữa $r^m \equiv 1 (\operatorname{mod} p^2)$ nên $\varphi(p^2) = p(p-1) | m$. Do đó $m = p^t(p-1)$ với $1 \leq t \leq k-1$. Để chứng minh định lý, ta chỉ cần chứng minh rằng $p^k \nmid r^{p^t(p-1)} - 1, \forall t \leq k-2$. Nhưng:

$$r^{p^t(p-1)} - 1 \Big| \left(r^{p^t(p-1)}\right)^{p^{k-2-t}} - 1$$

Nên ta chỉ cần chứng minh $p^k \nmid r^{p^{k-2}(p-1)} - 1, \forall k \in \mathbb{N}^*$.

Ta sẽ dùng quy nạp. Tại $k = 1$, điều ấy là hiển nhiên.

Giả sử $p^k \nmid r^{p^{k-2}(p-1)} - 1$, ta có $\varphi(p^{k-1}) = p^{k-2}(p-1)$ nên $p^{k-1} \parallel r^{p^{k-2}(p-1)} - 1$. Tức là:

$$r^{p^{k-2}(p-1)} = 1 + qp^{k-1} \left(q \not\equiv 0 (\operatorname{mod} p)\right)$$

Từ đó:

$$r^{p^{k-1}(p-1)} - 1 = (1 + qp^{k-1})^p - 1 = \sum_{i=0}^{p} \binom{p}{k} (qp^{k-1})^i - 1 \equiv qp^k \not\equiv 0 \ (\operatorname{mod} p^{k+1})$$

Theo nguyên lý quy nạp toán học thì định lý được chứng minh. ■

Định lý 2.7. Mọi số nguyên dương có dạng $2p^k$ trong đó p là số nguyên tố lẻ còn k là một số nguyên dương bất kỳ đều có căn nguyên thủy.

Chứng minh:

Trước hết ta có nhận xét rằng khi p là số nguyên tố lẻ thì $\varphi(p^k) = \varphi(2p^k) = p^{k-1}(p-1)$.

Gọi r là một căn nguyên thủy modulo p^k, ta có $r^{\varphi(p^k)} \equiv 1 (\mathrm{mod}\, p^k)$. Có hai khả năng. Nếu r lẻ thì ta lại có $r^{\varphi(p^k)} \equiv 1 (\mathrm{mod}\, 2)$ và do đó $r^{\varphi(p^k)} \equiv 1 (\mathrm{mod}\, 2p^k)$. Còn nếu r chẵn thì ta có $r + p^k$ lẻ nên $(r+p^k)^{\varphi(p^k)} \equiv r^{\varphi(p^k)} \equiv 1 (\mathrm{mod}\, p^k)$, hơn nữa $(r+p^k)^{\varphi(p^k)} \equiv 1 (\mathrm{mod}\, 2)$ nên suy ra $(r+p^k)^{\varphi(p^k)} \equiv 1 (\mathrm{mod}\, 2p^k)$. Hơn nữa, nếu có số nguyên dương $m < \varphi(p^k)$ sao cho $r^m \equiv 1 (\mathrm{mod}\, 2p^k)$ hoặc $(r+p^k)^m \equiv 1 (\mathrm{mod}\, 2p^k)$ thì ta đều suy ra $r^m \equiv 1 (\mathrm{mod}\, p^k)$, điều này trái với giả thiết rằng r là căn nguyên thủy modulo p^k. Do vậy, tồn tại r' để $\mathrm{ord}_{2p^k} r' = \varphi(2p^k)$, tức r' là căn nguyên thủ modulo $2p^k$. Định lý được chứng minh. ■

Định lý 2.8. Nếu số nguyên dương n không có các dạng $2; 4; p^k; 2p^k$ trong đó p là số nguyên tố lẻ, k nguyên dương nào đó thì n không có căn nguyên thủy.

Chứng minh:

Xét phân tích tiêu chuẩn $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, thế thì:

$$\varphi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \dots p_s^{\alpha_s - 1} (p_1 - 1)(p_2 - 1) \dots (p_s - 1)$$

Giả sử tồn tại căn nguyên thủy r của n. Ta có:

$$r^{\varphi\left(p_i^{\alpha_i}\right)} \equiv 1 \left(\mathrm{mod}\, p_i^{\alpha_i}\right)$$

Đặt $\Phi = \left[\varphi\left(p_1^{\alpha_1}\right), \varphi\left(p_2^{\alpha_2}\right), \dots, \varphi\left(p_s^{\alpha_s}\right)\right]$, ta có $\varphi\left(p_i^{\alpha_i}\right) | \Phi, \forall i$ nên $r^{\Phi} \equiv 1 (\mathrm{mod}\, n)$. Nhưng r là căn nguyên thủy modulo n nên $\mathrm{ord}_n r = \varphi(n) = \varphi\left(p_1^{\alpha_1}\right)\varphi\left(p_2^{\alpha_2}\right) \dots \varphi\left(p_s^{\alpha_s}\right) | \Phi$. Tức là:

$$\varphi\left(p_1^{\alpha_1}\right)\varphi\left(p_2^{\alpha_2}\right) \dots \varphi\left(p_s^{\alpha_s}\right) \left| \left[\varphi\left(p_1^{\alpha_1}\right), \varphi\left(p_2^{\alpha_2}\right), \dots, \varphi\left(p_s^{\alpha_s}\right)\right]\right.$$

Suy ra $\left(\varphi\left(p_i^{\alpha_i}\right), \varphi\left(p_i^{\alpha_j}\right)\right) = 1$ với mọi i, j. Nhưng điều này là không thể, vì n không có dạng $2; 4; p^k; 2p^k$, hơn nữa $p_i - 1 \vdots 2, \forall i$. Mâu thuẫn trên cho ta kết luận của định lý. ■

Như vậy, các định lý **2.5**, **2.6**, **2.7**, **2.8** cho chúng ta phát biểu mệnh đề mang tính tổng hợp về sự tồn tại căn nguyên thủy.

Định lý 2.9. Một số nguyên dương có căn nguyên thủy khi và chỉ khi có bằng 2; 4 hoặc nó có dạng p^k hay $2p^k$ với $k \in \mathbb{N}^*$ còn p là một số nguyên tố lẻ nào đó.

3. Ứng dụng của bậc và căn nguyên thủy:

3.1. Một số bài toán về bậc của số nguyên:

Ví dụ 3.1.1. Xét số Fermat $F_m = 2^{2^m} + 1$ $(m \geq 2)$. Chứng minh rằng nếu p là ước nguyên tố của F_m thì $p \equiv 1 (\mathrm{mod}\, 2^{m+1})$.

Lời giải:

Đặt $k = \text{ord}_p\, 2$. Ta có: $p|F_m$ nên $2^{2^m} \equiv -1 (\text{mod}\, p)$, suy ra rằng $2^{2^{m+1}} \equiv 1 (\text{mod}\, p)$. Theo tính chất của bậc thì $k|2^{m+1}$, tuy nhiên $k \nmid 2^m$, vì nếu không thì $-1 \equiv 2^{2^m} \equiv 1 (\text{mod}\, p)$, suy ra $2|p$, tức là $p = 2$, vô lý do F_m là số lẻ với $m \geq 2$. Vậy $k = 2^{m+1}$. Nhưng vì $k = \text{ord}_p\, 2$ nên $k|p-1$, tức là $p \equiv 1 (\text{mod}\, 2^{m+1})$. Bài toán được chứng minh. ■

Ví dụ 3.1.2. Cho $n, k \in \mathbb{N}^*$, k lẻ. Giả sử $p = 2^n \cdot k + 1$ là một số nguyên tố lẻ và tồn tại một số nguyên dương m sao cho $p|F_m = 2^{2^m} + 1$. Chứng minh rằng $k^{2^{n-1}} \equiv 1 (\text{mod}\, p)$.

Lời giải:

Đặt $h = \text{ord}_p\, 2$. Ta có $p|F_m$ nên $2^{2^m} \equiv -1 (\text{mod}\, p)$, suy ra $2^{2^{m+1}} \equiv 1 (\text{mod}\, p)$. Theo tính chất của bậc thì $2^{m+1} \vdots h$. Nhưng nếu $h|2^m$ thì $2^{2^m} \equiv 1 (\text{mod}\, p)$, vô lý. Cho nên $h|2^{m+1}$ và $h \nmid 2^m$. Từ đó $h = 2^{m+1}$. Suy ra $p - 1 = 2^n k \vdots 2^{m+1}$. Vì k lẻ nên $n \geq m + 1$. Ta có:

$$2^{2^{n-1}} - 1 = \left(2^{2^{n-2}} + 1\right)\left(2^{2^{n-3}} + 1\right) \cdots \left(2^{2^m} + 1\right)\left(2^{2^m} - 1\right) \vdots F_m$$

Do p là ước nguyên tố của F_m nên $2^{2^{n-1}} \equiv 1 (\text{mod}\, p)$. Nhân hai vế cho $k^{2^{n-1}}$ ta có:

$$k^{2^{n-1}} \equiv (2k)^{2^{n-1}} \equiv (-1)^{2^{n-1}} \equiv 1 (\text{mod}\, p)$$

Bài toán được chứng minh. ■

Ví dụ 3.1.3. Tồn tại hay không các số nguyên dương phân biệt $a_1, a_2, \ldots, a_n$ thỏa mãn:

$$a_1|2^{a_2} - 1; a_2|2^{a_3} - 1; \ldots; a_{n-1}|2^{a_n} - 1; a_n|2^{a_1} - 1$$

Lời giải:

Trước hết ta có nhận xét sau:

Gọi p là ước nguyên tố nhỏ nhất của n, q là ước nguyên tố nhỏ nhất của $2^n - 1$. Thế thì $q > p$.

Thật vậy, đặt $k = \text{ord}_2\, q$, ta có $2^n \equiv 1 (\text{mod}\, q)$ nên $k|n$, nhưng vì p là ước nguyên tố nhỏ nhất của n nên $k \geq p$. Hơn nữa, $k|q-1$ nên $q \geq k + 1 \geq p + 1 > p$.

Vào bài toán. Gọi p_i, q_i tương ứng là ước nguyên tố nhỏ nhất của $a_i, 2^{a_i} - 1$, với mọi $i = 1,2, \ldots, n$. Ta có $p_i|a_i$ và $a_i|2^{a_{i+1}} - 1$ nên $p_i|2^{a_{i+1}} - 1$, nhưng q_{i+1} là ước nguyên tố nhỏ nhất của $2^{a_{i+1}} - 1$ nên $p_i \geq q_{i+1}$. Mặt khác theo nhận xét trên thì $q_{i+1} > p_{i+1}$ nên $p_i > p_{i+1}$, với mọi $i = 1,2, \ldots, n$, ở đây i được sử dụng theo nghĩa modulo n, tức là ta coi $a_{n+1} \equiv a_1, p_{n+1} \equiv p_1$ và $q_{n+1} \equiv q_1$. Từ đó suy ra $p_1 > p_2 > \cdots > p_n > p_1$ (vô lý).

Vậy bài toán có câu trả lời phủ định. ■

Ví dụ 3.1.4. (VMO 2004)

Với mỗi số tự nhiên n, ta kí hiệu $S(n)$ là tổng các chữ số trong biểu diễn thập phân của n. Tìm:

$$\min_{n:2003} S(n)$$

Lời giải:

Dễ dàng nhận thấy $\text{ord}_{2003}\, 10 = 1001$.

Hiển nhiên 10^k không là bội của 2003 với mọi k.

Giả sử tồn tại $k \in \mathbb{N}^*$ thỏa mãn $10^k + 1 \equiv 0 (\text{mod } 2003)$, thế thì $10^{2k} \equiv 1 (\text{mod } 2003)$, do đó $2k \vdots 1001$, tức là $k \vdots 1001$, suy ra $10^k \equiv 1 (\text{mod } 2003)$, vô lý. Vậy nên không tồn tại n sao cho $n \vdots 2003$ và $S(n) = 2$.
Mặt khác, ta sẽ chứng minh rằng tồn tại $n \vdots 2003$ sao cho $S(n) = 3$.
Gọi a_i, b_i tương ứng là số dư trong phép chia 10^i và $-10^i - 1$ cho 2003 ($i = 1,2, \dots, 1001$). Rõ ràng là $a_i, b_i \notin \{0,2002\}$ nên a_i, b_i chỉ có thể nhận các giá trị $1,2, \dots, 2001$. Vậy theo nguyên lý Dirichlet thì tồn tại hai số nào đó trong 2002 số a_i, b_i bằng nhau. Hơn nữa, $\text{ord}_{2003} 10 = 1001$ nên $a_i \neq a_j$ và $b_i \neq b_j$ với mọi $i \neq j$, vậy tồn tại i, j sao cho $a_i = b_j$, hay $10^i + 10^j + 1 \vdots 2003$. Chú ý rằng $S\left(10^i + 10^j + 1\right) = 3$ nên giá trị nhỏ nhất cần tìm là 3. ■

Câu hỏi phụ: Thử xác định xem số n nhỏ nhất sao cho $n \vdots 2003$ và $S(n) = 3$ là số nào?

Ví dụ 3.1.5. Cho $a \in \mathbb{N}^*$ và p là một ước nguyên tố của a. Chứng minh rằng số $a^{p^k} - 1$ có ước nguyên tố lớn hơn $kp^k \log_a p$.
Lời giải:
Xét số M xác định bởi:

$$M = a^{p^{k-1}(p-1)} + a^{p^{k-1}(p-2)} + \cdots + a^{p^{k-1}} + 1 = \frac{a^{p^k} - 1}{a^{p^{k-1}} - 1}$$

Rõ ràng $M | a^{p^k} - 1$. Ta sẽ chứng minh M có ước nguyên tố $q > kp^k \log_a p$. Thật vậy, giả sử q là một ước nguyên tố của M. Đặt $h = \text{ord}_q a$. Ta có $a^{p^k} \equiv 1 (\text{mod } q)$ nên $h | p^k$, nhưng nếu $h \leq p^{k-1}$ thì $h | p^{k-1}$, do đó $a^{p^{k-1} \cdot m} \equiv 1 (\text{mod } q)$ với mọi m nguyên dương, dẫn đến $M \equiv p (\text{mod } q)$ (vô lý do $q | M$ nên $q \nmid a$, tức là $(q, p) = 1$). Vậy nên $h = p^k$ và theo tính chất của bậc của số nguyên thì $p^k | q - 1$. Như vậy, mọi ước nguyên tố của M đều có dạng $p^k \cdot k_i + 1$ với $k_i \in \mathbb{N}^*$ nào đó.
Giả sử kết luận của bài toán là sai, tức là mọi ước nguyên tố của M đều không lớn hơn $kp^k \log_a p$. Xét phân tích tiêu chuẩn của M như sau:

$$M = \prod_{i=1}^{s} q_i^{a_i} = \prod_{i=1}^{s} (p^k \cdot k_i + 1)^{a_i}$$

Ta có $q_i = p^k \cdot k_i + 1 < kp^k \log_a p$ nên $1 \leq k_i \leq k \log_a p$ với mọi $i = 1,2, \dots, s$. Suy ra:

$$a^{p^k} > M = \prod_{i=1}^{s} (p^k \cdot k_i + 1)^{a_i} > (p^k + 1)^{\sum_{i=1}^{s} a_i}$$

Logarithm hai vế ta được:

$$p^k > \log_a (p^k + 1) \sum_{i=1}^{s} a_i > k \log_a p \cdot \sum_{i=1}^{s} a_i \geq \sum_{i=1}^{s} a_i k_i$$

Mặt khác theo định lý nhị thức thì:

$$(p^k \cdot k_i + 1)^{a_i} = \sum_{t=0}^{a_i} \binom{a_i}{t} (p^k \cdot k_i)^t \equiv p^k \cdot a_i k_i + 1 (\mathrm{mod}\, p^{2k})$$

Suy ra:

$$M = \prod_{i=1}^{s} (p^k \cdot k_i + 1)^{a_i} \equiv \prod_{i=1}^{s} (p^k \cdot a_i k_i + 1) \equiv p^k \sum_{i=1}^{s} a_i k_i + 1 (\mathrm{mod}\, p^{2k})$$

Nhưng $p|a$ nên $M = a^{p^{k-1}(p-1)} + a^{p^{k-1}(p-2)} + \cdots + a^{p^{k-1}} + 1 \equiv 1 (\mathrm{mod}\, p)$ nên ta có:

$$1 \equiv p^k \sum_{i=1}^{s} a_i k_i + 1 (\mathrm{mod}\, p^{2k})$$

Hay:

$$p^k \sum_{i=1}^{s} a_i k_i \equiv 0 (\mathrm{mod}\, p^{2k})$$

Song điều này là vô lý vì ta có $\sum_{i=1}^{s} a_i k_i < p^k$.

Mâu thuẫn ấy cho ta kết luận của bài toán.

■

3.2. Một số bài toán về căn nguyên thủy:

Ví dụ 3.2.1. Cho n là một số nguyên dương có căn nguyên thủy. Chứng minh rằng:

$$\prod_{(a,n)=1} a \equiv -1 (\mathrm{mod}\, n)$$

Lời giải:

Do r là căn nguyên thủy modulo n nên $r, r^2, \dots, r^{\varphi(n)}$ lập thành hệ thặng dư đầy đủ modulo n. Ta có:

$$\prod_{(a,n)=1} a = \prod_{k=1}^{\varphi(n)} r^k \equiv r^{\sum_{k=1}^{\varphi(n)} k} \equiv r^{\frac{\varphi(n)(\varphi(n)+1)}{2}} = \left(r^{\varphi(n)+1}\right)^{\frac{\varphi(n)}{2}} \equiv r^{\frac{\varphi(n)}{2}}$$

Phương trình đồng dư $x^2 \equiv 1 (\mathrm{mod}\, n)$ chỉ có đúng hai nghiệm modulo n là 1 và -1, trong đó $r^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$ và vì r là căn nguyên thủy modulo n nên $r^{\frac{\varphi(n)}{2}} \not\equiv 1 (\mathrm{mod}\, n)$.

Vậy $r^{\frac{\varphi(n)}{2}} \equiv -1 (\mathrm{mod}\, n)$. ■

Ví dụ 3.2.2. Cho p là một số nguyên tố lẻ. Chứng minh rằng r là căn nguyên thủy modulo p khi và chỉ khi $r^{\frac{p-1}{q}} \not\equiv 1 (\mathrm{mod}\, p)$, với mọi ước nguyên tố q của $p-1$.

Lời giải:

Nếu r là căn nguyên thủy modulo p thì $\mathrm{ord}_p\, r = p-1$ nên kết luận của ta là hiển nhiên.

Ngược lại, giả sử $r^{\frac{p-1}{q}} \not\equiv 1 (\mathrm{mod}\, p)$, với mọi ước nguyên tố q của $p-1$. Ta đặt $k \coloneqq \mathrm{ord}_p\, r$, thế thì $k|p-1$, nhưng vì $r^{\frac{p-1}{q}} \not\equiv 1 (\mathrm{mod}\, p)$ nên $k \nmid \frac{p-1}{q}$ với mọi ước nguyên tố q của p. Vì thế phải có $k = p-1$. Vậy $\mathrm{ord}_p\, r = p-1$. ■

Ví dụ 3.2.3. Tìm các số nguyên tố p, q thỏa mãn điều kiện: $a^{3pq} \equiv a (\text{mod } 3pq), \forall a \in \mathbb{N}^*$.

Lời giải:

Ta có $a^{3pq} \equiv (a^p)^{3q} \equiv a^{3q} (\text{mod } p)$ nên $a^{3q} \equiv a (\text{mod } p)$, với mọi $a \in \mathbb{N}^*$.

Xét $a = r$ là một căn nguyên thủy modulo p, ta có $r^{3q-1} \equiv 1 (\text{mod } p)$ nên $3q - 1 \vdots \text{ord}_p\, r$ hay $3q - 1 \vdots p - 1$. Tương tự thì $3p - 1 \vdots q - 1$.

Không mất tính tổng quát ta có thể giả sử $p \geq q$. Vì $3q - 1 \vdots p - 1$ nên:

$$p - 1 \leq 3q - 1 \leq 3p - 1$$

Vậy $\dfrac{3q-1}{p-1} \in \{1,2,3,4\}$. Xét các trường hợp:

1. $\dfrac{3q-1}{p-1} = 1$. Ta có: $3q - 1 = p - 1$, từ đó $p = 3q$ (vô lý).

2. $\dfrac{3q-1}{p-1} = 2$. Ta có: $3q = 2p - 1$ hay $q = \dfrac{2p-1}{3}$.

Ta lại có $3q - 1 \vdots p - 1$ nên:

$$3p - 1 \vdots \frac{2p-1}{3} - 1 \Leftrightarrow 9p - 3 \vdots 2p - 4$$

Suy ra $9p - 3 \vdots p - 2$. Mặt khác $9p - 3 = 9(p - 2) + 15$ nên $15 \vdots p - 2$. Do đó $p - 2 \in \{1,3,5,15\}$, suy ra $p \in \{3,5,7,17\}$.

Hơn nữa $q = \dfrac{2p-1}{3} \in \mathbb{N}^*$ nên ta có $p \equiv 2 (\text{mod } 3)$. Vậy $(p, q) \in \{(5,3), (17,11)\}$.

3. $\dfrac{3q-1}{p-1} = 3$ thì $3q - 1 = 3(p - 1) \vdots 3$(vô lý).

4. $\dfrac{3q-1}{p-1} = 1$, ta có $4(p - 1) = 3q - 1 \leq 3p - 1$ nên $p \leq 3$.

Suy ra $p \in \{2; 3\}$, dẫn đến $p = q = 3$.

Vậy ta có các kết quả $(p, q) \in \{(3,3); (5,3); (17; 11)\}$.

Tuy nhiên không phải cả ba kết quả trên đều chấp nhận được. Thật vậy, xét $a = 3$, ta có $3^{27} - 3 = 3(3^{26} - 1) \not\equiv 0 (\text{mod } 27)$ và $3^{45} - 3 = 3(3^{44} - 1) \not\equiv 0 (\text{mod } 45)$, do đó các kết quả $(p, q) = (5,3)$ và $(p, q) = (3,3)$ bị loại.

Với $(p, q) = (17,11)$, ta có $3 \cdot 11 \cdot 17 = 561$, đây là một số Carmichael. Có thể dễ dàng kiểm tra rằng $a^{560} \equiv 1 (\text{mod } 561)$ với mọi $a \in \mathbb{N}^*$.

Vậy $(p, q) \in \{(17,11), (11,17)\}$. ■

Ví dụ 3.2.4. Chứng minh rằng với mọi số nguyên dương n đều tồn tại vô hạn các số nguyên tố p sao cho căn nguyên thủy nhỏ nhất modulo p lớn hơn n.

Lời giải:

Ta có nhận xét rằng nếu a là một thặng dư bình phương modulo p thì a không phải là căn nguyên thủy modulo p. Thật vậy, vì $a \equiv x^2 (\text{mod } p)$ nên $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 (\text{mod } p)$. Từ đó $\text{ord}_p\, a < p - 1$.

Ta sẽ chứng minh rằng với mọi $n \in \mathbb{N}^*$ thì tồn tại vô hạn số nguyên tố p sao cho $1,2,\dots,n$ đều là thặng dư bình phương modulo p.

Thật vậy, giả sử $p_1, p_2, \dots, p_s$ là tất cả các số nguyên tố lẻ không lớn hơn n. Theo định lý Trung Hoa thì tồn tại số nguyên dương k sao cho:

$$\begin{cases} k \equiv 1 (\text{mod } 8) \\ k \equiv 1 (\text{mod } p_i) \forall i = 1,2,\dots,s \end{cases}$$

Xét dãy số $\{q_n\}_{n=0}^{\infty}$ xác định bởi $q_n = k + n \cdot 8p_1p_2 \cdots p_s$. Theo định lý Dirictlet, trong dãy chứa vô hạn số nguyên tố q. Mặt khác với mỗi số nguyên tố q trong dãy ta đều có:

$$\left(\frac{p_i}{q}\right)\left(\frac{q}{p_i}\right) = (-1)^{\frac{q-1}{2}.\frac{p_i-1}{2}} = 1 \Rightarrow \left(\frac{p_i}{q}\right) = \left(\frac{q}{p_i}\right) = \left(\frac{1}{p_i}\right) = 1$$

Vậy tất cả p_i đều là thặng dư bình phương modulo q. Hơn nữa mọi số nguyên dương không lớn hơn n đều có dạng $p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ trong đó $\alpha_i \geq 0$ nên chúng đều là thặng dư bình phương modulo q.

Cuối cùng, vì q là số nguyên tố nên nó phải có căn nguyên thủy, nhưng $1,2,\dots,n$ đều không phải là căn nguyên thủy modulo q nên căn nguyên thủy nhỏ nhất của nó lớn hơn n. ■

4. Bài tập áp dụng:

Bài toán 1.

Chứng minh rằng $n \nmid 3^n + 1$ với mọi số nguyên dương n.

Bài toán 2.

Gọi p là ước nguyên tố nhỏ nhất của n và q là ước nguyên tố nhỏ nhất của $2^n + 1$. Giả sử rằng $q < p$. Hãy tìm q.

Bài toán 3.

Cho $F_n = 2^{2^n}$ là số Fermat thứ n. Chứng minh rằng điều kiện cần và đủ để F_n là một số nguyên tố là $3^{\frac{F_n-1}{2}} \equiv -1 (\text{mod } F_n)$.

Bài toán 4. (China TST 2004)

Chứng minh rằng với mọi số nguyên dương n, số Fermat F_n có ước nguyên tố lớn hơn $2^{n+2}(n+1)$.

Bài toán 5.

Chứng minh rằng tồn tại vô hạn các cặp số nguyên tố (p, q) thỏa mãn điều kiện:

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

Bài toán 6.

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

Bài toán 7.
Cho p là một số nguyên tố lẻ. Chứng minh rằng tích các căn nguyên thủy của p đồng dư với 1 theo modulo p.

Bài toán 8.
Dùng nghĩa $\mu(n)$ là hàm Mobius.
Giả sử p là một số nguyên tố lẻ và $r_1, r_2, \cdots, r_{\varphi(p-1)}$ là các căn nguyên thủy của p. Chứng minh rằng:

$$\sum_{k=1}^{\varphi(p-1)} r_k \equiv \mu(p-1) \pmod{p}$$

Bài toán 9.
Chứng minh rằng với mọi số nguyên tố lẻ p, tồn tại r sao cho r là căn nguyên thủy modulo p^n, với mọi $n \in \mathbb{N}^*$.

5. Tài liệu tham khảo:

1. *Chuyên đề bồi dưỡng HSG toán trung học phổ thông: SỐ HỌC* (GS. TSKH Hà Huy Khoái).
2. *Một số vấn đề Số Học chọn lọc* (Nguyễn Văn Mậu (chủ biên), Trần Nam Dũng, Đặng Hùng Thắng, Đặng Huy Ruận).
3. *Mathematical Olympiad in China – Problems and Solutions* (Xiong Bin, Lee Peng Yee).
4. *Problem in Elementery Number Theory (PEN)* (Hojoo Lee).
5. Các trang diễn đàn Toán học: http://www.mathlinks.ro/ , http://www.mathscope.org/ , http://www.diendantoanhoc.net/.