TRƯỜNG THPT CHUYÊN THÁI NGUYÊN

TRƯƠNG THANH TÙNG

CẤP CỦA PHẦN TỬ - CĂN NGUYÊN THỦY

Thái Nguyên - Năm 2013

1 Kiến thức cơ bản

1.1 Đồng dư thức

Trong vành số nguyên $\mathbb{Z}$, cho n là một số tự nhiên, $n \neq 0$, a, b là những số nguyên.

Định nghĩa 1.1. *Ta nói rằng a đồng dư với b theo modulo n nếu trong phép chia a và b cho n ta được cùng một số dư.*

Khi a đồng dư với b theo modulo n, ta ký hiệu: $a \equiv b \,(\mathrm{mod}\, n)$, và gọi đó là một *đồng dư thức.*

Định lý 1.1. *Các điều kiện sau là tương đương.*

a) $a \equiv b \,(\mathrm{mod}\, n)$

b) $n \,|(a - b)$

c) Có một số nguyên t sao cho $a = b + nt$

1.2 Các tính chất của đồng dư thức

1. Quan hệ đồng dư là một quan hệ tương đương trong $\mathbb{Z}$.

2. Ta có thể cộng hoặc trừ từng vế nhiều đồng dư thức theo cùng một modulo n với nhau, cụ thể là nếu ta có

$$a_i \equiv b_i \,(\mathrm{mod}\, n)\,,\ i = 1, 2, ..., k$$

thì ta cũng có

$$\sum_{i=1}^{k} \varepsilon_i a_i \equiv \sum_{i=1}^{k} \varepsilon_i b_i \ \ (\mathrm{mod}\, n) \ \text{ với } \varepsilon_i = \pm 1.$$

3. Ta có thể nhân từng về với nhiều đồng dư thức theo cùng một modulo n với nhau, cụ thể là nếu ta có

$$a_i \equiv b_i \,(\mathrm{mod}\, n)\,,\ i = 1, 2, ..., k$$

thì ta cũng có

$$\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \ (\mathrm{mod}\, n)$$

4. Ta có thể chia hai vế của đồng dư thức cho một ước chung nguyên tố với modulo, cụ thể là nếu $c \,|a$, $c \,|b$ và $(c, n) = 1$ thì từ đồng dư thức

$$a \equiv b \,(\,\mathrm{mod}\ n)$$

ta cũng có

$$\frac{a}{c} \equiv \frac{b}{c} (\bmod\ n).$$

5. Ta có thể nhân hai vế của một đồng dư thức và modulo với cùng một số nguyên dương, chia chia hai vế và modulo cho cùng một số nguyên dương là ước chung của chúng, cụ thể là nếu

$$a \equiv b (\bmod\ n)$$

thì với mọi số nguyên dương c, ta cũng có

$$ac \equiv bc (\bmod\ nc)$$

và với mọi số d nguyên dương, $d|(a, b, n)$, ta cũng có

$$\frac{a}{d} \equiv \frac{b}{d} \left(\bmod \frac{n}{d}\right)$$

6. Nếu hai số đồng dư với nhau theo nhiều modulo thì chúng cũng đồng dư với nhau theo modulo là bội chung nhỏ nhất của các modulo đã cho, cụ thể là nếu

$$a \equiv b (\bmod\ n_i),\ i = 1, 2, ..., k$$

và $n = [n_1, n_2, ..., n_k]$ thì ta cũng có

$$a \equiv b (\bmod\ \ n)$$

Định nghĩa 1.2. *(Hàm số Euler)*

Cho n là số tự nhiên khác 0. Ta gọi $\varphi(n)$ là số các số nguyên dương không vượt quá n và nguyên tố với n.

Các tính chất của hàm $\varphi(n)$

1. Hàm số $\varphi(n)$ có tính chất nhân, tức là: $\varphi(n_1).\varphi(n_1) = \varphi(n_1.n_2)$ với $(n_1, n_2) = 1$
2. Nếu p nguyên tố thì $\varphi(p) = p - 1$ và $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ $(\alpha > 1)$
3. Công thức tính $\varphi(n)$

Nếu số tự nhiên n có dạng phân tích tiêu chuẩn $n = p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}$ thì

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right)$$

Định lý 1.2. *Định lý Euler*

Nếu $a, n \in \mathbb{Z}, n > 0, (a, n) = 1$ thì $a^{\varphi(n)} \equiv 1 (\bmod n)$

Định lý 1.3. *Định lý Fermat*

Nếu p là số nguyên tố và a là số nguyên không chia hết cho p thì ta có $a^{p-1} \equiv 1 \pmod{p}$

Định lý 1.4. *Định lý Wilson*

Nếu p là số nguyên tố thì $(p-1)! \equiv -1 \pmod{p}$

2 Cấp của phần tử

Định nghĩa 2.1. *Cho $n \in \mathbb{N}^*$, $(a,n) = 1$, cấp của a theo modulo n là số nguyên dương k nhỏ nhất sao cho* $a^k \equiv 1 \pmod{n}$*, ta kí hiệu cấp của a theo modulo n là* $\mathrm{ord}_n a$.

Ví dụ 2.1. *Cấp của 2 theo modulo 3 là 2, cấp của 2 theo modulo 5 là 4, cấp của 4 theo modulo 5 là 2.*

Định lý 2.1. *Cho số nguyên a có cấp k theo modulo n. Khi đó* $a^h \equiv 1 \pmod{n}$ *nếu và chỉ nếu* $k \mid h$*, đặc biệt* $k \mid \varphi(n)$.

Chứng minh. Giả sử $k \mid h$ thì tồn tại $j \in \mathbb{Z}$ sao cho $h = k.j$. Vì $a^k \equiv 1 \pmod{n}$ nên $\left(a^k\right)^j \equiv 1^j \pmod{n} \Leftrightarrow a^h \equiv 1 \pmod{n}$ Ngược lại, giả sử h là số nguyên thỏa mãn $a^h \equiv 1 \pmod{n}$. Theo thuật toán Euclide, tồn tại các số nguyên q, r sao cho $h = qk + r$, $0 \le r < k$. Khi đó $a^h = (a^q)^k.a^r$. Từ đó suy ra: $a^r \equiv 1 \pmod{n}$. Vì $0 \le r < k$ và k là số nguyên dương nhỏ nhất sao cho $a^k \equiv 1 \pmod{n}$ nên $r = 0$. Vậy $h \mid k$. □

Ví dụ 2.2. *Tính cấp của 2 theo modulo 13.*

Vì $\varphi(13) = 12$ nên cấp của 2 phải là một trong các số: 1, 2, 3, 4, 6, 12. Ta có:

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 3,\ 2^6 \equiv 12,\ 2^{12} \equiv 1 \pmod{13}$$

Khi đó 2 có cấp 12 theo modulo 13.

Định lý 2.2. *Nếu số nguyên a có cấp k theo modulo n thì* $a^i \equiv a^j \pmod{n}$ *nếu và chỉ nếu* $i \equiv j \pmod{k}$.

Chứng minh. Giả sử $a^i \equiv a^j \pmod{n}$, $i \ge j$. Vì a nguyên tố cùng nhau với n nên $a^{i-j} \equiv 1 \pmod{n}$. Khi đó, ta có $k \mid (i-j)$, suy ra $i \equiv j \pmod{k}$.

Ngược lại, giả sử $i \equiv j \,(\mathrm{mod}\, k)$. Khi đó tồn tại $q \in \mathbb{Z}$ sao cho $i = j + kq$. Do đó $a^i \equiv a^{j+kq} \equiv a^j.\left(a^k\right)^q \equiv a^j \,(\,\mathrm{mod}\, n)$. Điều phải chứng minh. □

Hệ quả 2.1. *Nếu a có cấp k theo modulo n thì các số nguyên $a, a^2, ..., a^k$ không đồng dư với nhau từng đôi một theo modulo n.*

Chứng minh. Giả sử ngược lại rằng, $a^i \equiv a^j \,(\mathrm{mod}\, n)$, với $1 \leq i \leq j \leq k$. Khi đó theo định lý trên, ta có: $i \equiv j \,(\mathrm{mod}\, k)$, suy ra $i = j$. Điều phải chứng minh. □

Định lý 2.3. *Nếu số nguyên a có cấp k theo modulo n và $h > 0$ thì a^h có cấp là $\frac{k}{(h,k)}$ theo modulo n.*

Chứng minh. Đặt $d = (h, k)$, khi đó tồn tại $h_1, k_1 \in \mathbb{Z}$ sao cho $h = h_1 d$, $k = k_1 d$, với $(h_1, k_1) = 1$. Ta có:

$$\left(a^h\right)^{k_1} \equiv \left(a^{h_1 d}\right)^{\frac{k}{d}} \equiv \left(a^k\right)^{h_1} \equiv 1 \,(\mathrm{mod}\, n)$$

Giả sử a^h có cấp r theo modulo n. Khi đó: $r \,|k_1$ (1). Mặt khác, vì a có cấp k theo modulo n nên từ:

$$a^{hr} \equiv \left(a^h\right)^r \equiv 1 \,(\mathrm{mod}\, n) \Rightarrow k \,|hr \;\text{ hay } k_1 d \,|h_1 dr \Rightarrow k_1 \,|h_1 r.$$

Mà $(h_1, k_1) = 1$ nên $k_1 \,|r$ (2). Từ (1) và (2) suy ra: $k_1 = r$. Điều phải chứng minh. □

Từ định lý trên ta có hệ quả sau:

Hệ quả 2.2. *Nếu số nguyên a có cấp k theo modulo n thì a^h cũng có cấp k nếu và chỉ nếu $(h, k) = 1$.*

Ví dụ 2.3. *Cấp của 2 và lũy thừa của 2 theo modulo 13*

Ta có cấp của 2 theo modulo 13 là 12 và cấp của 2^2 và 2^3 theo modulo 13 lần lượt là 6 và 4. Ta dễ dàng kiểm tra: $6 = \frac{12}{(2,12)}$, $4 = \frac{12}{(3,12)}$ Theo định lý trên, các số nguyên là lũy thừa của 2 cũng có cấp 12 theo modulo 13 là các lũy thừa 2^k, với $(k, 12) = 1$, cụ thể là: $2^1, 2^5, 2^7$ và 2^{11}

Định lý 2.4. *Nếu a có cấp h theo modulo n, b có cấp k theo modulo n và $(h, k) = 1$ thì ab có cấp hk theo modulo n.*

Chứng minh. Giả sử ab có cấp r theo modulo n. Do $(ab)^{hk} \equiv \left(a^h\right)^k.\left(b^k\right)^h \equiv 1 \,(\mathrm{mod}\, n)$ nên $r \,|hk$. Vì vậy, để chứng minh $r = hk$ ta phải chứng minh $hk \,|r$.

Ta có: $b^{rh} \equiv \left(a^h\right)^r b^{rh} \equiv (ab)^{rh} \equiv 1 \,(\mathrm{mod}\, n)$ nên $k \,|rh$. Vì $(h,k) = 1$ nên $k \,|r$.
Hoàn toàn tương tự, ta cũng có: $h \,|r$. Từ đó và $(h,k) = 1$ suy ra $hk \,|r$. Vậy $r = hk$. □

Nhận xét. Định lý trên sẽ không còn đúng nếu thiếu giả thiết $(h,k) = 1$. Ví dụ, 2 và 3 có cùng cấp 4 theo modulo 5 nhưng $6 = 2.3$ có cấp $1 (\neq 4.4)$ theo modulo 5.
Trong trường hợp $(h,k) > 1$, dù không suy ra được cấp của ab là hk theo modulo n nhưng ta dễ dàng chứng minh được r là ước của hk.

Hệ quả 2.3. *Nếu p là một số nguyên tố, a, n là các số nguyên dương thỏa mãn $(a,m) = 1$, $a \not\equiv 1 \,(\mathrm{mod}\, n)$ và $a^p \equiv 1 \,(\mathrm{mod}\, n)$ thì cấp của a theo modulo n là p.*

Chứng minh. Thật vậy, giả sử h là cấp của a theo modulo n. Khi đó, ta có: $h \,|p \,,\ h \neq 1$. Do p là số nguyên tố nên $h = p$. □

Từ định lý thặng dư Trung hoa ta có hệ quả sau:

Hệ quả 2.4. *Nếu a, m, n là các số nguyên đôi một nguyên tố cùng nhau, a có cấp h theo modulo m và có cấp k theo modulo n thì a có cấp $[h,k]$ theo modulo mn.*

Chứng minh. Thật vậy, gọi r là cấp của a theo modulo mn, ta có:

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

Khi đó, $h \,|r \,,\ k \,|r \Rightarrow [h,k] \,|r$. Để chứng minh $r = [h,k]$, ta cần chứng minh $r \,|[h,k]$. Giả sử $[h,k] = hk_1 = h_1 k$. Ta có

$$a^{[h,k]} = \left(a^h\right)^{k_1} \equiv 1 \,(\mathrm{mod}\, m) \,,$$
$$a^{[h,k]} = \left(a^k\right)^{h_1} \equiv 1 \,(\mathrm{mod}\, n) \,.$$

Theo định lý thặng dư Trung hoa suy ra $a^{[h,k]} \equiv 1 \,(\mathrm{mod}\, mn)$, từ đó suy ra $r \,|[h,k]$.
Vậy $r = [h,k]$ □

Ta đã biết cấp của một số nguyên a theo modulo n luôn là một ước số của $\varphi(n)$. Trong nhiều trường hợp cụ thể của n, tồn tại những số nguyên a sao cho cấp của a theo modulo n đúng bằng $\varphi(n)$. Khi đó ta có thể biểu diễn hệ thặng dư thu gọn dưới dạng sau

$$\left\{1, a, a^2, ..., a^{\varphi(n)}\right\}$$

Biểu diễn này đem lại rất nhiều thuận lợi khi xét tích các phần tử trong hệ thặng dư thu gọn, ta có thể quy phép nhân các phần tử trong hệ thặng dư thu gọn trên về phép cộng modulo $\varphi(n)$. Cụ thể hơn, ta có thể tương ứng phần tử a^i, a^j trong hệ thặng dư với các phần tử i, j trong tập $\{1, 2, ..., \varphi(n)\}$. Khi đó tích $a^i.a^j$ được tương ứng với phần tử $i + j$.

3 Căn nguyên thủy

Định nghĩa 3.1. *Nếu $(a, n) = 1$ và a có cấp $\varphi(n)$ theo modulo n thì a là một căn nguyên thủy của số nguyên n.*

Hay nói cách khác, n có a là một căn nguyên thủy modulo n nếu $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Ví dụ 3.1. *3 là một căn nguyên thủy của 7 vì:* $3^1 \equiv 3, 3^2 \equiv 2, 3^3 \equiv 6, 3^6 \equiv 1 \pmod{7}$

Ta có thể chứng minh căn nguyên thủy tồn tại với bất kỳ modulo nguyên tố nào, và đây là kết quả quan trọng cơ bản. Mặc dù có thể có căn nguyên thủy của n với cả n không phải là số nguyên tố (ví dụ, 2 là một căn nguyên thủy của 9 vì $2^{\varphi(9)} = 2^6 \equiv 1 \pmod{9}$). Cũng không có lý do gì để tin tưởng là mọi số nguyên n đều sở hữu 1 căn nguyên thủy, vì sự tồn tại của căn nguyên thủy phù thuộc vào từng trường hợp đặc biệt hơn là một quy luật chung.

Ví dụ 3.2. *Chứng tỏ rằng nếu $F_n = 2^{2^n} + 1$ với $n > 1$, là một số nguyên tố thì 2 không phải là căn nguyên thủy của F_n (rõ ràng 2 là căn nguyên thủy của $5 = F_1$).*

Từ sự phân tích: $2^{2^{n+1}} - 1 = \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right)$, ta có: $2^{2^{n+1}} \equiv 1 \pmod{F_n}$. Từ đó suy ra, cấp của 2 theo modulo F_n không vượt quá 2^{n+1}. Nhưng với giả thiết F_n là số nguyên tố thì

$$\varphi(F_n) = F_n - 1 = 2^{2^n}.$$

Bằng quy nạp đơn giản dễ dàng nhận được $2^{2^n} > 2^{n+1}$, với $n > 1$. Do vậy cấp của 2 theo modulo F_n nhỏ hơn $\varphi(F_n)$. Do đó, 2 không thể là căn nguyên thủy của F_n.

Từ định nghĩa của căn nguyên thủy, ta dễ dàng có các kết quả sau:

Định lý 3.1. *Nếu a là một căn nguyên thủy modulo n thì $a^k \equiv 1 \pmod{n}$ nếu và chỉ nếu $\varphi(n) | k$.*

Định lý 3.2. *Nếu a là một căn nguyên thủy modulo n thì* $\left\{a, a^2, ..., a^{\varphi(n)}\right\}$ *lập thành hệ thặng dư thu gọn modulo n.*

Định lý 3.3. *Nếu a là một căn nguyên thủy modulo n thì b cũng là căn nguyên thủy modulo n khi và chỉ khi* $b \equiv a^k \pmod{n}$, $(k, \varphi(n)) = 1$.

Chứng minh. Điều kiện đủ của định lý là hiển nhiên vì:

$$\mathrm{ord}_n b = \mathrm{ord}_n a^k = \frac{\mathrm{ord}_n a}{(\mathrm{ord}_n a,\ k)} = \frac{\varphi(n)}{(k, \varphi(n))} = \varphi(n).$$

Với điều kiện cần, ta giả sử b là một căn nguyên thủy modulo n thì $(b, n) = 1$ hay b nằm trong hệ thặng dư thu gọn modulo n. Khi đó tồn tại k sao cho $b \equiv a^k \pmod{n}$. Đồng thời

$$\varphi(n) = \mathrm{ord}_n b = \mathrm{ord}_n a^k = \frac{\mathrm{ord}_n a}{(\mathrm{ord}_n a, k)} = \frac{\varphi(n)}{(\varphi(n), k)}.$$

Suy ra $(\varphi(n), k) = 1$. □

Một trong những tính chất quan trọng của căn nguyên thủy nằm ở định lý sau:

Định lý 3.4. *Cho* $(a, n) = 1$ *và* $a_1, a_2, ..., a_{\varphi(n)}$ *là các số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n thì*

$$a, a^2, ..., a^{\varphi(n)}$$

đồng dư theo modulo n với $a_1, a_2, ..., a_{\varphi(n)}$ *theo một thứ tự nào đó.*

Chứng minh. Vì a nguyên tố cùng nhau với n nên các lũy thừa của a cũng nguyên tố cùng nhau với n. Do vậy mỗi a^k đồng dư modulo với một số a_i nào đó. Mà ta đã biết $\varphi(n)$ số trong tập $\left\{a, a^2, ..., a^{\varphi(n)}\right\}$ không đồng dư với nhau. Do vậy các lũy thừa này phải đồng dư (không nhất thiết theo thứ tự xuất hiện) các số nguyên $a_1, a_2, ..., a_{\varphi(n)}$. □

Hệ quả 3.1. *Nếu n có một căn nguyên thủy thì nó có chính xác* $\varphi(\varphi(n))$ *căn nguyện thủy.*

Chứng minh. Giả sử a là một căn nguyên thủy của n. Theo định lý trên, các căn nguyên thủy khác của n được tìm trong tập hợp $a, a^2, ..., a^{\varphi(n)}$. Nhưng số các lũy thừa $a^k, 1 \leq k \leq \varphi(n)$ mà có cấp $\varphi(n)$ bằng với số các số nguyên k sao cho $(k, \varphi(n)) = 1$. Rõ ràng có $\varphi(\varphi(n))$ số k thỏa mãn. Vậy có $\varphi(\varphi(n))$ căn nguyên thủy. □

Kết quả trên có thể giải thích qua trường hợp $a = 2$ và $n = 9$. Vì $\varphi(9) = 6$ nên 6 lũy thừa đầu tiên của 2 phải đồng dư theo modulo 9, theo một thứ tự nào đó với các số nguyên dương nhỏ hơn 9 và nguyên tố cùng nhau với 9. Các số nguyên dương nhỏ hơn 9 và nguyên tố cùng nhau với 9 là: 1,2,4,5,7, 8 và khi đó ta có:

$$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 7, 2^5 \equiv 5, 2^6 \equiv 1 \pmod 9.$$

Theo hệ quả trên ta có chính xác $\varphi(\varphi(9)) = \varphi(6) = 2$ căn nguyên thủy của 9 và chúng là các số 2 và 5.

Định lý 3.5. *Mọi số nguyên dương có dạng p^2 với p là một số nguyên tố đều có căn nguyên thủy.*

Chứng minh. Gọi a là một căn nguyên thủy của p. Đặt $\text{ord}_{p^2} a = k$ thì $a^k \equiv 1 \left(\text{mod}\, p^2\right)$ nên $a^k \equiv 1 \pmod p$, suy ra $\text{ord}_p a = p-1 \,|k$, hơn nữa $k \left|\varphi\left(p^2\right) = p(p-1)\right.$. Vậy nên $k = p-1$ hoặc $k = p(p-1)$.
Nếu $k = p(p-1) = \varphi\left(p^2\right)$ thì theo định nghĩa a là căn nguyên thủy của p^2.
Nếu $k = p-1$ thì $a^{p-1} \equiv 1 \left(\text{mod}\, p^2\right)$.
Đặt $b = a + p$, ta có $b \equiv a \pmod p$ nên $\text{ord}_p b = \text{ord}_p a = p-1$. Lập luận tương tự như trên ta cũng có $\text{ord}_{p^2} b \in \{p-1; p(p-1)\}$. Mặt khác:

$$b^{p-1} = (a+p)^{p-1} = \sum_{i=0}^{p-1} C_{p-1}^i a^i p^{p-1-i} \equiv a^{p-1} + a^{p-2} p(p-1) \equiv 1 - a^{p-2} \left(\text{mod}\, p^2\right).$$

Vậy nếu $\text{ord}_{p^2} b = p-1$ thì $a^{p-2} \equiv 0 \left(\text{mod}\, p^2\right)$, mâu thuẫn vì a là căn nguyên thủy của p nên $(a,p) = 1$. Do đó, $\text{ord}_{p^2} b = p(p-1) = \varphi\left(p^2\right)$, tức là $b = a + p$ là căn nguyên thủy của p^2.
Định lý được chứng minh. □

Định lý 3.6. *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 a là một căn nguyên thủy của p^2, ta sẽ chứng minh a cũng là căn nguyên thủy của p^k, với mọi k nguyên dương. Đặt $m = \text{ord}_{p^k} a$, ta có $a^m \equiv 1 \left(\text{mod}\, p^k\right)$ nên $m \left|\varphi\left(p^k\right) = p^{k-1}(p-1)\right.$. Hơn nữa, $a^m \equiv 1 \left(\text{mod}\, p^2\right)$ nên $\varphi\left(p^2\right) = p(p-1) \,|m$. Do đó, $m = p^t(p-1)$, với $1 \le t \le k-1$. Để chứng minh định lý, ta chỉ cần chứng minh rằng: $p^k \not| a^{p^t(p-1)} - 1, \forall t \le k-2$. Nhưng

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

Nên ta chỉ cần chứng minh $p^k \not| \, a^{p^{k-2}(p-1)} - 1, \forall k \in \mathbb{N}^*$. Ta sẽ dùng quy nạp. Với $k = 1$ thì điều ấy là hiển nhiên. Giả sử $p^k \not| \, a^{p^{k-2}(p-1)} - 1$, ta có $\varphi\left(p^{k-1}\right) = p^{k-2}(p-1)$ nên $p^{k-1} \left| a^{p^{k-2}(p-1)} - 1 \right.$. Tức là:

$$a^{p^{k-2}(p-1)} = 1 + qp^{k-1} \left(q \not\equiv 0 \left(\mathrm{mod}\, p\right)\right).$$

Từ đó:

$$a^{p^{k-1}(p-1)} - 1 = \left(1 + qp^{k-1}\right)^p - 1 = \sum_{i=0}^{p} C_p^i \left(qp^{k-1}\right)^i - 1 \equiv qp^k \not\equiv 0 \left(\mathrm{mod}\, p^{k+1}\right).$$

Theo nguyên lý quy nạp toán học, định lý được chứng minh. □

Định lý 3.7. *Cho p và q là hai số nguyên tố sao cho $(p-1) \vdots q^\alpha$, với $\alpha \geq 1$. Khi đó có đúng $q^\alpha - q^{\alpha-1}$ lớp thặng dư phân biệt có cấp q^α modulo p.*

Chứng minh. Xét phương trình

$$x^{q^\alpha} - 1 \equiv 0 \left(\mathrm{mod}\, p\right).$$

Phương trình này có đúng q^α nghiệm phân biệt modulo p. Vì q là một số nguyên tố nên mỗi nghiệm cho ta một lớp thặng dư có cấp là q^β, trong đó β là một số nguyên nhỏ hơn hoặc bằng α. Như vậy một lớp thặng dư a có cấp q^α modulo p nếu nó là nghiệm của phương trình trên và $a^{q^{\alpha-1}} \not\equiv 1 \left(\mathrm{mod}\, p\right)$, tức là nó không là nghiệm của phương trình

$$x^{q^{\alpha-1}} - 1 \equiv 0 \left(\mathrm{mod}\, p\right)$$

Mỗi nghiệm trong số $q^{\alpha-1}$ nghiệm của phương trình dưới đều là nghiệm của phương trình trên. Do đó số lớp thặng dư phân biệt có cấp q^α modulo p là $q^\alpha - q^{\alpha-1}$.
Định lý được chứng minh. □

Định lý 3.8. *Mọi số nguyên dương có dạng $2p^k$, trong đó p là số nguyên tố lẻ còn k là số nguyên dương bất kỳ đều có căn nguyên thủy.*

Chứng minh. Trước hết, nếu p là số nguyên tố lẻ thì $\varphi\left(p^k\right) = \varphi\left(2p^k\right) = p^{k-1}(p-1)$. Gọi a là một căn nguyên thủy modulo p^k, ta có $a^{\varphi\left(p^k\right)} \equiv 1 \left(\mathrm{mod}\, p^k\right)$. Đến đây, ta chia làm 2 khả năng:

Nếu a lẻ thì ta có: $a^{\varphi\left(p^k\right)} \equiv 1 \left(\mathrm{mod}\, 2\right)$ và do đó $a^{\varphi\left(p^k\right)} \equiv 1 \left(\mathrm{mod}\, 2p^k\right)$.

Nếu a chẵn thì $a + p^k$ lẻ nên $\left(a + p^k\right)^{\varphi\left(p^k\right)} \equiv a^{\varphi\left(p^k\right)} \equiv 1 \left(\mathrm{mod}\, p^k\right)$, hơn nữa:

$$\left(a + p^k\right)^{\varphi\left(p^k\right)} \equiv 1 \left(\mathrm{mod}\, 2\right) \text{ nên suy ra } \left(a + p^k\right)^{\varphi\left(p^k\right)} \equiv 1 \left(\mathrm{mod}\, 2p^k\right)$$

Mặt khác, nếu có số nguyên dương $m < \varphi\left(p^k\right)$ sao cho

$$a^m \equiv 1 \left(\mathrm{mod}\, 2p^k\right) \text{ hoặc } \left(a + p^k\right)^m \equiv 1 \left(\mathrm{mod}\, 2p^k\right)$$

thì ta đều suy ra $a^m \equiv 1 \left(\mathrm{mod}\, p^k\right)$, điều này mâu thuẫn với giả thiết a là căn nguyên thủy modulo p^k. Do vậy, tồn tại a' sao cho $\mathrm{ord}_{2p^k} a' = \varphi\left(2p^k\right)$, tức là a' là căn nguyên thủy modulo $2p^k$.

Định lý được chứng minh. □

Định lý 3.9. *Nếu số nguyên dương n không có một trong 4 dạng: 2, 4, p^k, $2p^k$, trong đó p là số nguyên tố lẻ và k là số nguyên dương nào đó thì n không có căn nguyên thủy.*

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

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

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

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

Đặt $\Phi = \left[\varphi\left(p_1^{\alpha_1}\right), \varphi\left(p_2^{\alpha_2}\right), ..., \varphi\left(p_s^{\alpha_s}\right)\right]$, ta có $\varphi\left(p_i^{\alpha_i}\right) | \Phi, \forall i = 1, 2, ..., s.$ nên $a^\Phi \equiv 1 \left(\mathrm{mod}\, n\right)$. Nhưng a là căn nguyên thủy modulo n nên:

$$\mathrm{ord}_n a = \varphi(n) = \varphi\left(p_1^{\alpha_1}\right)\varphi\left(p_2^{\alpha_2}\right)...\varphi\left(p_s^{\alpha_s}\right) | \Phi.$$

Tức là:

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

Suy ra: $\left(\varphi\left(p_i^{\alpha_i}\right), \varphi\left(p_j^{\alpha_j}\right)\right) = 1, \forall i, j.$ 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 cho ta kết luận của định lý. □

4 Một số ví dụ áp dụng

Ví dụ 4.1. *Cho a có cấp 3 modulo p. Tìm cấp của a+1 modulo p.*

Giải:

Ta có: $a \not\equiv 1 \left(\mathrm{mod}\, p\right), a^2 \not\equiv 1 \left(\mathrm{mod}\, p\right)$ nên từ:

$$a^3 - 1 = (a - 1)\left(a^2 + a + 1\right) \equiv 0 \left(\mathrm{mod}\, p\right) \text{ suy ra: } a + 1 \equiv -a^2 \left(\mathrm{mod}\, p\right).$$

Do a có cấp 3 modulo p, -1 có cấp 2 modulo p nên $-a^2$ có cấp 6 modulo p. Vậy cấp của $a + 1$ modulo p là 6.

Ví dụ 4.2. *Xét số Fermat $F_n = 2^{2^n} + 1 (n \geq 2)$. Chứng minh rằng nếu p là ước nguyên tố của F_n thì $p \equiv 1 \left(\mathrm{mod}\, 2^{n+1}\right)$.*

Giải:

Đặt: $k = \mathrm{ord}_p 2$. Ta có: $p \,|F_n$ nên $2^{2^n} \equiv -1 \,(\mathrm{mod}\, p)$, suy ra rằng $2^{2^{n+1}} \equiv 1 \,(\mathrm{mod}\, p)$. Theo tính chất của cấp thì $k \,\big|2^{n+1}$, tuy nhiên $k \not| 2^n$, vì nếu không thì $-1 \equiv 2^{2^n} \equiv 1 \,(\mathrm{mod}\, p)$, suy ra $2 \,|p$, tức là $p = 2$, vô lý do F_n là số lẻ với $n \geq 2$.

Vậy $k = 2^{n+1}$. Nhưng vì $k = \mathrm{ord}_p 2$ nên $k \,|(p-1)$, tức là $p \equiv 1 \left(\mathrm{mod}\, 2^{n+1}\right)$.
Bài toán được chứng minh.

Ví dụ 4.3. *Cho $m, k \in \mathbb{N}^*$, k lẻ. Giả sử $p = k.2^m + 1$ là một số nguyên tố lẻ và tồn tại số nguyên dương n sao cho $p \,|F_n = 2^{2^n} + 1$. Chứng minh rằng $k^{2^{m-1}} \equiv 1 \,(\mathrm{mod}\, p)$.*

Giải:

Đặt $h = \mathrm{ord}_p 2$. Ta có $p \,|F_n$ nên $2^{2^n} \equiv -1 \,(\mathrm{mod}\, p)$, suy ra $2^{2^{n+1}} \equiv 1 \,(\mathrm{mod}\, p)$. Theo tính chất của cấp thì $2^{n+1} \vdots h$. Nhưng nếu $h \,|2^n$ thì $2^{2^n} \equiv 1 \,(\mathrm{mod}\, p)$, vô lý. Cho nên $h \,\big|2^{n+1}$ và $h \not| 2^n$, từ đó $h = 2^{n+1}$. Từ ví dụ trên, suy ra $p - 1 = k.2^m \vdots 2^{n+1}$. Vì k lẻ nên $m \geq n + 1$. Ta có:

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

Do p là ước nguyên tố của F_n nên $2^{2^{m-1}} \equiv 1 \,(\mathrm{mod}\, p)$. Nhân hai vế với $k^{2^{m-1}}$ ta có:

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

Bài toán được chứng minh.

Ví dụ 4.4. *Tồn tại hay không các số nguyên dương phân biệt $a_1, a_2, ..., a_n$ thỏa mãn:*

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

Giải:

Ta có nhận xét sau: Gọi p là ước nguyên tố nhỏ nhất của n, q là ước nguyên tố nhỏ nhất của $2^n - 1$. Khi đó: $q > p$.

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

Gọi p_i, q_i tương ứng là các ước nguyên tố nhỏ nhất của a_i, $2^{a_i} - 1$, $\forall i = 1, 2, ..., n$. 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 $p_i > p_{i+1}$, $\forall i = 1,2,...,n$, 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: $p_1 > p_2 > ... > p_n > p_1$ (vô lý). Vậy không tồn tại các số nguyên dương phân biệt $a_1, a_2, ..., a_n$ thỏa mãn yêu cầu bài toán.

Ví dụ 4.5. ***(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:

$$\min_{n \vdots 2003} S(n).$$

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 $10^k + 1 \equiv 0 \pmod{2003}$, thế thì $10^{2k} \equiv 1 \pmod{2003}$, do đó $2k \vdots 1001$, tức là $k \vdots 1001$, suy ra $10^k \equiv 1 \pmod{2003}$, vô lý. Vậy nên không tồn tại n sao cho $n \vdots 2003$ và $S(n) = 2$.

Bây giờ ta sẽ chứng minh rằng tồn tại: $n \vdots 2003$ và $S(n) = 3$.

Gọi a_i, b_i tương ứng là số dư trong phép chia 10^i và $-10^i - 1$ cho 2003, $i = 1,2,...,1001$. Rõ ràng là $a_i, b_i \notin \{0, 2002\}$ nên a_i, b_i chỉ có thể nhận các giá trị: $1,2,...,2001$. 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 cần tìm là 3.

Ví dụ 4.6. *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 $kp^k \log_a p$.*

Giải:

Ta xét số M xác định bởi:

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

Rõ ràng $M \left| a^{p^k} - 1 \right.$. 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 $a^{p^k} \equiv 1 \pmod{q}$ nên $h \left| p^k \right.$,

nhưng nếu $h \leq p^{k-1}$ thì $h \left| p^{k-1} \right.$, do đó $a^{p^{k-1}.m} \equiv 1 \pmod{q}$, với m nguyên dương, điều này dẫn đến $M \equiv p \pmod{q}$

(vô lý do $q \left| M \right.$ nên $q \not| a$, tức là $(q,p) = 1$). Vậy nên $h = p^k$ và theo tính chất của cấp của số nguyên thì $p^k \left| (q-1) \right.$. Như vậy, mọi ước nguyên tố của M đều có dạng $p^k.k_i + 1$, 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:

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

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

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

Logarithm hai vế ta được:

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

Mặt khác, ta lại có:

$$\left(p^k.k_i + 1\right)^{a_i} = \sum_{t=0}^{a_i} C_{a_i}^t \left(p^k.k_i\right)^t \equiv p^k.a_i k_i + 1 \left(\mathrm{mod}\, p^{2k}\right)$$

Suy ra:

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

Nhưng $p \left| a \right.$ nên $M = a^{p^{k-1}(p-1)} + a^{p^{k-1}(p-2)} + ... + a^{p^{k-1}} + 1 \equiv 1 \pmod{p}$ nên ta có:

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

hay

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

Điều này là vô lý vì ta có $\sum_{i=1}^{s} a_i k_i < p^k$. Từ đó suy ra điều phải chứng minh.

Ví dụ 4.7. *Cho n là một số nguyên dương có căn nguyên thủy. Chứng minh rằng:*

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

Giải:

Giả sử r là một căn nguyên thủy của n, khi đó $r, r^2, ..., r^{\varphi(n)}$ lập thành hệ thặng dư đầy đủ modulo n. Ta có:

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

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

Ví dụ 4.8. *Cho p là số nguyên tố lẻ. Chứng minh rằng a là căn nguyên thủy modulo p khi và chỉ khi* $a^{\frac{p-1}{q}} \not\equiv 1 \pmod p$ *, với mọi ước nguyên tố q của p-1.*

Giải:

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

Ngược lại, giả sử $a^{\frac{p-1}{q}} \not\equiv 1 \pmod p$, với mọi ước nguyên tố q của $p-1$. Ta đặt $k = \text{ord}_p a$, thế thì $k \mid p-1$, nhưng vì $a^{\frac{p-1}{q}} \not\equiv 1 \pmod p$ nên $k \not\mid \frac{p-1}{q}$, với mọi ước nguyên tố q của p. Vì thế ta có $k = p-1$. Vậy $\text{ord}_p a = p-1$.

Ví dụ 4.9. *Tìm các số nguyên p, q thỏa mãn điều kiện:* $a^{3pq} \equiv a \pmod{3pq}$, $\forall a \in \mathbb{N}^*$

Giải:

Ta có: $a^{3pq} \equiv (a^p)^{3q} \equiv a^{3q} \pmod p$ nên $a^{3q} \equiv a \pmod p$, $\forall a \in \mathbb{N}^*$. Xét $a = r$ là một căn nguyên thủy modulo p, ta có: $r^{3q-1} \equiv 1 \pmod p$ 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 giả sử $p \geq q$. Vì $3q-1 \vdots p-1$ nên:

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

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

1. $\frac{3q-1}{p-1} = 1$. Ta có: $3q-1 = p-1$, từ đó $p = 3q$ (vô lý).
2. $\frac{3q-1}{p-1} = 2$. Ta có: $3q = 2p-1$ hay $q = \frac{2p-1}{3}$. 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, $q = \frac{2p-1}{3} \in \mathbb{N}^*$ nên ta có

$p \equiv 2 \pmod 3$. Vậy $(p,q) \in \{(5,3),(17,11)\}$.
3. $\frac{3q-1}{p-1} = 3$ thì $3q-1 = 3(p-1) \vdots 3$ (vô lý).
4. $\frac{3q-1}{p-1} = 4$ thì $4(p-1) = 3q-1 \leq 3p-1$ nên $p \leq 3$.
Vậy ta có các kết quả $(p,q) \in \{(3,3),(5,3),(17,11)\}$. Tuy nhiên không phải cả 3 kết quả đều chấp nhận được. Thật vậy, xét $a=3$, ta có $3^{27}-3 = 3\left(3^{26}-1\right) \not\equiv 0 \pmod{27}$ và $3^{45}-3 = 3\left(3^{44}-1\right) \not\equiv 0 \pmod{45}$, do đó các kết quả $(p,q)=(5,3)$ và $(p,q)=(3,3)$ bị loại.
Với $(p,q)=(17,11)$, ta có: $3.11.17 = 561$. Ta kiểm tra thấy $a^{560} \equiv 1 \pmod{561}, \forall a \in \mathbb{N}^*$.
Vậy $(p,q) \in \{(17,11),(11,17)\}$

Ví dụ 4.10. *Cho p là một số nguyên tố, a, n là các số nguyên dương, (a,n)=1.Chứng minh rằng:*
a) Phương trình $x^n \equiv a \pmod p$ *hoặc có* $(n, p-1)$ *nghiệm hoặc vô nghiệm tùy theo*

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

b) Nếu $(n, p-1) = 1$ *thì phương trình* $x^n \equiv a \pmod p$ *có đúng một nghiệm.*

Giải:
a) Giả sử g là một căn nguyên thủy của p, $g^k \equiv a \pmod p$. Nếu tồn tại số nguyên x sao cho $x^n \equiv a \pmod p$ thì $(x,p)=1$. Do đó, tồn tại số nguyên dương u sao cho $g^u \equiv x \pmod p$. Khi đó,

$$g^{nu} \equiv g^k \pmod p \text{ hay } nu \equiv k \pmod{p-1}$$

Đặt $d = (n, p-1)$, khi đó phương trình $nu \equiv k \pmod{p-1}$ có d nghiệm nếu $k \vdots d$ và vô nghiệm nếu $k \not\vdots d$.
Nếu $k \vdots d$ thì $\frac{k(p-1)}{d} \equiv 0 \pmod{p-1}$ nên

$$a^{\frac{p-1}{d}} \equiv g^{\frac{k(p-1)}{d}} \equiv \left(g^{p-1}\right)^{\frac{k}{d}} \equiv 1 \pmod p.$$

Nếu $k \not\vdots d$ thì $\frac{k(p-1)}{d} \not\equiv 0 \pmod{p-1}$ nên

$$a^{\frac{p-1}{d}} \equiv g^{\frac{k(p-1)}{d}} \not\equiv 1 \pmod p.$$

Điều phải chứng minh.
b) Đây là trường hợp riêng của a) với $(n, p-1) = 1$.

Ví dụ 4.11. ***(Balkan 1999)***
Cho p là một số nguyên tố có dạng $3l+2$. Đặt

$$S = \left\{ y^3 - x^3 - 1 \,|\, x, y \text{ là các số nguyên dương }, 0 \leq x, y \leq p-1 \right\}$$

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

Giải:

Trước hết, ta có nhận xét sau: Nếu p là một số nguyên tố, k, x, y là các số nguyên dương thỏa mãn $(k, p-1) = 1$ và $x^k \equiv y^k \pmod{p}$ thì $x \equiv y \pmod{p}$.
Theo giả thiết ta có: $(3, p-1) = 1$ nên $\left\{1^3, 2^3, ..., p^3\right\}$ lập thành một hệ thặng dư đầy đủ modulo p. Do đó, với mỗi $0 \leq y \leq p-1$ tồn tại duy nhất số nguyên x, $0 \leq x \leq p-1$ sao cho $x^3 \equiv y^2 - 1 \pmod{p}$. Tức là trong tập S có nhiều nhất p số chia hết cho p. Điều phải chứng minh.

Ví dụ 4.12. *Cho g là một căn nguyên thủy của số nguyên tố p, số nguyên dương $a \equiv g^k \pmod{p}$ có cấp h modulo p và $a.\bar{a} \equiv 1 \pmod{p}$. Chứng minh rằng $\bar{a}$ cũng có cấp h modulo p và $\bar{a} \equiv g^{p-1-k} \pmod{p}$*

Giải:

Hiển nhiên $a\bar{a} \equiv g^k \bar{a} \equiv 1 \equiv g^{p-1} \pmod{p}$ nên $\bar{a} \equiv g^{p-1-k} \pmod{p}$. Gọi k là cấp của $\bar{a}$ modulo p.
Vì $a^h \equiv 1 \pmod{p}$ nên $\bar{a}^h \equiv (a.\bar{a})^h \equiv 1 \pmod{p}$, từ đó suy ra $h \vdots k$.
Vì $\bar{a}^k \equiv 1 \pmod{p}$ nên $a^k \equiv (a.\bar{a})^k \equiv 1 \pmod{p}$, từ đó suy ra $k \vdots h$.
Khi đó $h = k$, tức là cấp của $\bar{a}$ là h. Điều phải chứng minh.

Ví dụ 4.13. *Cho p, q là hai số nguyên tố lẻ thỏa mãn $p = 2q+1$. Chứng minh rằng $-a^2$ luôn là một căn nguyên thủy modulo p với mọi số nguyên dương a, $1 < a \leq q$.*

Giải:

Giả sử $q = 2k+1$, suy ra $p = 2q+1 = 4k+3$ nên -1 không phải là một số chính phương modulo p. Gọi g là một căn nguyên thủy modulo p, khi đó tồn tại các số nguyên dương $1 \leq s, t \leq p-1$ sao cho $-1 \equiv g^s, a \equiv g^t \pmod{p}$. Do -1 không là số chính phương modulo p nên s lẻ, do đó $(s+2t)\,q$ là một số lẻ và không chia hết cho $p-1$. Từ đó,

$$\left(-a^2\right)^q \equiv \left(g^s g^{2t}\right)^q \equiv g^{(s+2t)q} \not\equiv 1 \pmod{p}.$$

Mặt khác, vì $1 < a \leq q$ nên $a^2 \not\equiv 1 \pmod{p}$, do đó

$$\left(-a^2\right)^2 \equiv a^4 \not\equiv 1 \pmod{p}.$$

Gọi cấp của $-a^2$ modulo p là h. Khi đó $h \,|(p-1)$ nên h chỉ có thể nhận các giá trị là 2, q hoặc $2q$. Từ chứng minh trên ta suy ra $h = 2q = p-1$. Vậy $-a^2$ là một căn nguyên thủy modulo p. Điều phải chứng minh.

Ví dụ 4.14. *Chứng minh rằng:*
a) Nếu $a.a'$ là hai căn nguyên thủy phân biệt modulo p thì $a.a'$ không phải là một căn nguyên thủy.
b) Nếu a là một căn nguyên thủy modulo p^2 thì a là một căn nguyên thủy modulo p.
c) Hãy chứng minh định lý Wilson dựa vào căn nguyên thủy.

Giải:
a) Giả sử $a' \equiv a^k \pmod{p}$. Do a' là một căn nguyên thủy nên $(k, p-1) = 1$, suy ra k là một số lẻ. Do k lẻ nên $k+1 \vdots 2$ và $\frac{(k+1)(p-1)}{2} \vdots p-1$, từ đó ta có:

$$\left(a.a'\right)^{\frac{p-1}{2}} = \left(a^{\frac{k+1}{2}}\right)^{(p-1)} \equiv a^{p-1} \equiv 1 \pmod{p}.$$

Từ đó suy ra $a.a'$ không là một căn nguyên thủy.
b) Gọi cấp của a modulo p là h, khi đó $h \,|p-1$. Do $a^h \equiv 1 \pmod{p}$ nên tồn tại số nguyên dương q sao cho $a^h = pq + 1$. Ta có:

$$a^{ph} = (pq+1)^p = (pq)^p + C_p^{p-1}(pq)^{p-1} + C_p^{p-2}(pq)^{p-2} + ... + C_p^2(pq)^2 + C_p^1(pq) + 1$$

Do $C_p^1 = p$ nên $a^{ph} \equiv 1 \left(\mathrm{mod}\, p^2\right)$. Từ đó, $ph \vdots \varphi\left(p^2\right)$, tức là: $ph \vdots p\,(p-1)$ hay $h \vdots p-1$. Vì $h \,\big|\, p-1$ nên $h = p-1$, suy ra a là một căn nguyên thủy của p. Điều phải chứng minh.
c) Vì $a^1, a^2, ..., a^{p-1}$ là một hệ thặng dư thu gọn modulo p nên

$$(p-1)! \equiv a^1.a^2...a^{p-1} \equiv a^{\frac{p(p-1)}{2}} \equiv a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

Điều phải chứng minh.

5 Bài tập

Bài 1. Cho p, q là các số nguyên tố khác nhau sao cho tồn tại một số nguyên dương b thỏa mãn

$$\left(b^{q-1} + b^{q-1} + ... + 1\right) \vdots p$$

Chứng minh rằng: $p \equiv 1 \pmod{q}$.

Bài 2. Cho b là một số nguyên. Chứng minh rằng tồn tại vô số cặp số nguyên (p, q) thỏa mãn

$$\frac{q-1}{p} = k \in \mathbb{Z}, \ \ b \text{ là lũy thừa bậc } k \text{ modulo } p.$$

Bài 3. Cho b, t, k là các số nguyên dương lớn hơn 1. Chứng minh rằng điều kiện cần và đủ để tồn tại một số nguyên dương n thỏa mãn

$$b^{t-1} \leq n < b^t, \, n^k \equiv n \left(\mathrm{mod}\, b^t\right)$$

là một trong hai điều kiện sau xảy ra:

i) b không là lũy thừa của một số nguyên tố,

ii) $\left(k-1, \varphi\left(b^t\right)\right) > 1$.

Bài 4. Tìm tất cả các số nguyên $n > 1$ sao cho:

$$a^{25} - a \vdots n, \, \forall a \in \mathbb{Z}^+.$$

Bài 5. Tìm tất cả các cặp số nguyên tố p, q sao cho:

$$pq \,|(5^p - 2^p)\left(5^q - 2^q\right).$$

Bài 6. Tìm tất cả các cặp số nguyên tố p, q thỏa mãn:

$$a^{3pq} \equiv a \pmod{3pq}, \, \forall a \in \mathbb{Z}.$$

Bài 7. Tìm tất cả các số nguyên $n > 1$ sao cho $\frac{2^n+1}{n^2}$ là một số nguyên.

Bài 8. Với mỗi số nguyên a, đặt:

$$n_a = 101a - 100.2^a.$$

Chứng minh rằng nếu $0 \leq a, b, c, d \leq 99, n_a + n_b \equiv n_c + n_d \pmod{10100}$ thì $\{a, b\} = \{c, d\}$.

Bài 9. Cho b là một số nguyên dương thỏa mãn $b+1 = q$ là một số nguyên tố. Với mỗi số nguyên y, kí hiệu $\pi(y)$ là ước số nguyên tố nhỏ nhất của y. Chứng minh rằng nếu tồn tại một số nguyên dương y và một số nguyên tố $p \leq \pi(y)$ sao cho $b^y + 1 \vdots p$ thì $p = q$.

Bài 10. Cho b là một số nguyên dương thỏa mãn $b + 1 = q \geq 5$ là số nguyên tố. Gọi p là ước số nguyên tố lớn nhất của $b^y + 1$, q là ước số nguyên tố nhỏ nhất của y. Chứng minh rằng:

$$p \geq q + 2.$$