CẤP CỦA MỘT SỐ NGUYÊN VÀ ỨNG DỤNG

Trần Thị Hồng Minh*
Trường ĐH Sư phạm – ĐH Thái Nguyên

TÓM TẮT

Trong lí thuyết nhóm, cấp của một phần tử là một trong những khái niệm quan trọng và có nhiều ứng dụng. Việc tìm hiểu những tính chất và ứng dụng về cấp của một phần tử là rất cần thiết đối với các sinh viên sư phạm, các giảng viên dạy chuyên ngành Đại số và Lý thuyết số. Bài viết này sẽ trình bày một số tính chất quan trọng về cấp của một số nguyên và ứng dụng của nó trong số học.

Từ khóa: *số nguyên, phần tử, khái niệm, Đại số, Lý thuyết số*

CƠ SỞ LÍ THUYẾT*

Định nghĩa

Định nghĩa 1.1.1 ([2]). Cho một nhóm hữu hạn G có phần tử đơn vị là e. Cấp của phần tử $u \in G$ là số nguyên dương nhỏ nhất n thỏa mãn $u^n = e$.

Định nghĩa 1.1.2. Cho $n > 1$ và a là các số nguyên dương thỏa mãn $\gcd(a,n) = 1$. Số nguyên dương k nhỏ nhất thỏa mãn $a^k \equiv 1 \pmod n$ được gọi là cấp của a theo modulo n, kí hiệu là $k = \mathrm{ord}_n(a)$.

Chú ý. Cấp của *a* định nghĩa như trên chính là cấp của $\bar{a}$ trong nhóm $\mathbb{Z}_n^* = \{\bar{a} | a \in \mathbb{Z}, \gcd(a,n) = 1\}$ với phép nhân $\bar{a}.\bar{b} = \overline{ab}$.

Một số tính chất

Định lý 1.2.1 ([2]). Với các giả thiết như trong Định nghĩa 1.1.1 và x nguyên dương thì

$$a^x \equiv 1 \pmod n \Leftrightarrow \mathrm{ord}_n(a) \mid x.$$

Chứng minh. Giả sử $a^x \equiv 1 \pmod n$. Đặt $k = \mathrm{ord}_n(a)$. Áp dụng thuật toán Euclid thì

$$x = kq + r, 0 \le r < k.$$

Khi đó $1 \equiv a^x \equiv \left(a^k\right)^q \equiv a^r \pmod n$.

Suy ra $a^r \equiv 1 \pmod n$. Từ đó suy ra $r = 0$.

Vậy $k \mid x$.

Chiều ngược lại hiển nhiên.

Hệ quả 1.2.2. Cho a, n thỏa mãn $n > 1, \gcd(a,n) = 1$. Khi đó $\varphi(n) \vdots \mathrm{ord}_n(a)$.

MỘT SỐ VÍ DỤ ỨNG DỤNG CẤP CỦA MỘT SỐ NGUYÊN TRONG SỐ HỌC

Ví dụ 1 (6th IMO) a)Tìm tất cả các số nguyên dương n sao cho $2^n - 1 \vdots 7$.

b) Chứng minh rằng với mọi số nguyên dương n thì $2^n + 1 \not\vdots 7$.

Chứng minh. a) Ta có $\mathrm{ord}_7(2) = 3$ vì

$$2^1 \equiv 2 \pmod 7, 2^2 \equiv 4 \pmod 7, 2^3 \equiv 1 \pmod 7$$

Do đó

$$2^n \equiv 1 \pmod 7 \Leftrightarrow n \vdots 3 \Leftrightarrow n = 3k,$$

với k nguyên dương.

b) Giả sử tồn tại n nguyên dương sao cho $2^n \equiv -1 \pmod 7$. Khi đó

$$2^{2n} \equiv 1 \pmod 7 \Rightarrow 2n \vdots 3 \Rightarrow n \vdots 3.$$

Mặt khác, $n \vdots 3$ thì $2^n \equiv 1 \pmod 7$. Từ đó có điều phải chứng minh.

Ví dụ 2 (IMO Sorlist 2006). Tìm tất cả các cặp số nguyên dương x, y thỏa mãn

$$\frac{x^7 - 1}{x - 1} = y^5 - 1.$$

Chứng minh. Giả sử p không đồng dư với 1 modulo 7, và là ước nguyên tố của

$$\frac{x^7 - 1}{x - 1} = x^6 + x^5 + x^4 + x^3 + x^2 + 1$$

* *Tel: 0973 268338, Email: minh.tranhong.md@gmail.com*

Đặt $k = \text{ord}_x(p)$. Khi đó $x^7 \equiv 1 (\text{mod } p) \Rightarrow 7 \vdots k$. Theo định lý Fermat nhỏ thì $p-1 \vdots k$. Vì p không đồng dư với 1 modulo 7 nên $\gcd(7, p-1) = 1$. Từ đó suy ra $k = 1$ hay $x^1 \equiv 1 (\text{mod } p)$.

Ta lại có

$$0 \equiv x^6 + x^5 + ... + 1 \equiv 7 (\text{mod } p) \Rightarrow p = 7$$

Như vậy, nếu $m \mid \dfrac{x^7 - 1}{x - 1}$ thì $m \equiv 0 (\text{mod } 7)$ hoặc $m \equiv 1 (\text{mod } 7)$.

Mặt khác

$$\frac{x^7 - 1}{x - 1} = y^5 - 1 = (y-1)(y^4 + y^3 + ... + 1) \Rightarrow y - 1 \mid \frac{x^7 - 1}{x - 1}$$

$$\Rightarrow y \equiv 1, 2 (\text{mod } 7) \Rightarrow y^4 + y^3 + ... + 1 \equiv 5, 3 (\text{mod } 7)$$

vô lí.

Vậy không tồn tại x, y thỏa mãn yêu cầu bài toán.

Ví dụ 3. Cho p là số nguyên tố dạng $4k+1$. Giả sử rằng $2p+1$ cũng là số nguyên tố. Chứng minh rằng không tồn tại số tự nhiên k sao cho $k < 2p$ và $2^k \equiv 1 (\text{mod } 2p+1)$.

Chứng minh. Giả sử rằng có số tự nhiên k như vậy. Đặt $t = \text{ord}_{2p+1}(2)$, ta được

$$2^t \equiv 1 \ (\text{mod } 2p+1) \Rightarrow t \mid (2p+1) - 1 = 2p$$

Theo bài ra ta có

$$2^h \equiv 1 (\text{mod } 2p+1) \Rightarrow t \mid k.$$

Mặt khác $k < 2p$ suy ra $t = 1$ hoặc $t = 2$ hoặc $t = p$.

Vì p là số nguyên tố dạng $4k+1$ nên $p \geq 5$, $t \neq 1, t \neq 2 \Rightarrow t = p$. Suy ra:

$$2^{t+1} \equiv 2 (\text{mod } 2p+1)$$

Do đó $\left(\dfrac{2}{2p+1}\right) = 1$ (kí hiệu Legendre). Điều này là không thể vì $2p+1 \equiv 3 (\text{mod } 8)$

Vậy có điều phải chứng minh.

Ví dụ 4. Cho p là một số nguyên tố. Chứng minh rằng tồn tại một số nguyên tố q sao cho với mọi số nguyên dương n ta có $n^p - p \,\dot{:}\, q$.

Chứng minh. Ta có

$$\frac{p^p - 1}{p-1} = p^{p-1} + p^{p-2} + ... + 1 \equiv p + 1 \neq 1 (\text{mod } p^2)$$

Nếu tất cả các ước nguyên tố của $\dfrac{p^p - 1}{p-1}$ đều đồng dư với 1 modulo p^2 thì $\dfrac{p^p - 1}{p-1} \equiv 1 \left(\text{mod } p^2\right)$, vô lý. Vậy tồn tại ước nguyên tố q của $\dfrac{p^p - 1}{p-1}$ sao cho $q \neq 1 \left(\text{mod } p^2\right)$. Ta sẽ chứng minh số q như vậy thỏa mãn bài toán.

Trước tiên, ta thấy rằng:

+) Nếu $p - 1 \vdots q$ thì $p \equiv 1 (\text{mod } q)$ suy ra $p^p \equiv 1 (\text{mod } q)$.

+) Nếu $p - 1 \,\dot{:}\, q$ thì $\gcd(p-1, q) = 1$. Mà

$$\frac{p^p - 1}{p-1} \vdots q \Rightarrow p^p - 1 \vdots q \Rightarrow p^p \equiv 1 (\text{mod } q)$$

. Vậy ta luôn có $p^p \equiv 1 (\text{mod } q)$.

Giả sử rằng tồn tại n nguyên dương sao cho $n^p \equiv p (\text{mod } q)$. Khi đó

$$n^{p^2} \equiv p^p \equiv 1 (\text{mod } q).$$

Đặt $k = \text{ord}_q(n)$ thì $k \mid \text{p}^2 \Rightarrow \left[\begin{array}{l} k = 1 \\ k = p \\ k = p^2 \end{array}\right.$.

+)Nếu $k = 1 \Rightarrow n^1 \equiv 1 (\text{mod } q) \Rightarrow p \equiv 1 (\text{mod } q) \Rightarrow$

$$p^{p-1} + p^{p-2} + ... + 1 \equiv p (\text{mod } q)$$

Mà $q \mid \dfrac{p^p - 1}{p-1} = p^{\to p-1} + p^{p-2} + ... + 1$

nên $p \equiv 0 (\mathrm{mod}\, q)$, vô lí.

+) Nếu $k = p \Rightarrow p \equiv n^p \equiv 1 (\mathrm{mod}\, q) \Rightarrow p \equiv 1 (\mathrm{mod}\, q)$, theo chứng minh trên, trường hợp này cũng không xảy ra.

+) Nếu $k = p^2 \Rightarrow p^2 \mid \varphi(q) = q-1 \Rightarrow q \equiv 1 (\mathrm{mod}\, p^2)$, không thỏa mãn theo cách chọn q.

Vậy có điều phải chứng minh.

Ví dụ 5. Cho $n \in \mathbb{N}, n > 1$ thoả mãn $3^n - 1 \vdots n$. Chứng minh rằng n là số chẵn.

Chứng minh. Do $n \in \mathbb{N}, n > 1$ suy ra $n \geq 2$. Gọi p là ước nguyên tố bé nhất của n. Đặt $h = \mathrm{ord}_3(p)$.

Do

$3^n - 1 \vdots p \Rightarrow p \neq 3$

$\Rightarrow \gcd(p,3) = 1 \Rightarrow 3^{P-1} \equiv 1 (\mathrm{mod}\, p) \Rightarrow p - 1 \vdots h \Rightarrow p > h$ và $n \vdots h$.

Mà p là ước nguyên tố nhỏ nhất của n suy ra $h = 1$.

Vậy

$3 \equiv 1 (\mathrm{mod}\, p) \Rightarrow 2 \equiv 0 (\mathrm{mod}\, p) \Rightarrow p = 2 \Rightarrow n$ chẵn.

Ví dụ 6. Cho p là số nguyên tố lẻ, q và r là các số nguyên tố thỏa mãn $p \mid q^r + 1$. Chứng minh rằng: $2r \mid p-1$ hoặc $p \mid q^2 - 1$.

Chứng minh. Đặt $h = \mathrm{ord}_p q \Rightarrow q^h \equiv 1 (\mathrm{mod}\, p)$. Theo tính chất về cấp suy ra $h \mid p-1$. Ta có

$q^r \equiv -1 (\mathrm{mod}\, p) \Rightarrow q^{2r} \equiv 1 (\mathrm{mod}\, p)$

Suy ra $\begin{cases} h \mid 2r \\ h \nmid r \end{cases} \Leftrightarrow \left[\begin{array}{l} h = 2 \\ h = 2r \end{array} \right.$.

Nếu $h = 2$ thì $q^2 \equiv 1 (\mathrm{mod}\, p) \Leftrightarrow q^2 - 1 \vdots p$. Nếu $h = 2r$ thì $p - 1 \vdots 2r$.

Vậy có điều phải chứng minh.

Ví dụ 7. Tìm tất cả các bộ (p, q, r) nguyên tố thỏa mãn

$p \mid q^r + 1, q \mid r^p + 1, r \mid p^q + 1.$

Chứng minh. Rõ ràng các nguyên tố p, q, r phải khác nhau. Giả sử $p, q, r > 2$. Theo kết quả của Ví dụ 6, ta có $2r \mid p-1$ hoặc $p \mid q^2 - 1$.

Nếu $2r \mid p-1$ thì $p \equiv 1 (\mathrm{mod}\, r) \Rightarrow 0 \equiv p^q + 1 \equiv 2 (\mathrm{mod}\, r) \Rightarrow r = 2$ (loại). Vậy $p \mid q^2 - 1$.

Xét $p \mid q-1$ thì $q \equiv 1 (\mathrm{mod}\, p) \Rightarrow 0 \equiv q^r + 1 \equiv 2 (\mathrm{mod}\, p) \Rightarrow p = 2$ (loại). Suy ra $p \mid q+1$. Mà $q+1$ chẵn, p lẻ nên $p \mid \frac{q+1}{2}$.

Hoàn toàn tương tự thì $q \mid \frac{r+1}{2}$, $r \mid \frac{p+1}{2}$.

Suy ra $p + q + r \leq \frac{q+1}{2} + \frac{r+1}{2} + \frac{p+1}{2}$.

Do đó $p + q + r \leq 3$, vô lý. Vậy phải có ít nhất một số bằng 2. Giả sử $p = 2$. Khi đó q, r lẻ và $q \mid r^2 + 1$ và $r \mid 2^q + 1$.

Ta lại có $\mathrm{ord}_r(2) \mid 2q$. Nếu $\mathrm{ord}_r(2) \vdots q \Rightarrow q \mid r-1$ thì $q \mid (r^2 + 1) = 2 \Rightarrow q = 2$ (loại).

Vậy $\mathrm{ord}_r(2) \mid 2 \Rightarrow r \mid 2^2 - 1$ hay $r \mid 3 \Rightarrow r = 3 \Rightarrow q \mid 10 \Rightarrow q = 5$.

Vậy bộ $(p, q, r) = (2, 5, 3); (3, 2, 5); (5, 3, 2)$ là các bộ thỏa mãn đầu bài.

Ví dụ 8. Cho số nguyên $a > 1$ và số nguyên dương n. Chứng minh rằng : Nếu p là ước nguyên tố lẻ của $a^{2^n} + 1$ thì $p - 1 \vdots 2^{n+1}$.

Chứng minh. Do p là ước của $a^{2^n}+1$ nên $a \vdots p$. Theo giả thiết ta có

$$a^{2^n} \equiv -1(\text{mod } p) \Rightarrow \left(a^{2^n}\right)^2$$

$$\equiv 1(\text{mod } p) \Rightarrow a^{2^{n+1}} \equiv 1(\text{mod } p).$$

Đặt $h = \text{ord}_p(a)$ suy ra $2^{n+1} \vdots h$ và $2^n \not\vdots h \Rightarrow h = 2^{n+1}$. Từ đó có điều phải chứng minh.

Ví dụ 9. Cho p là số nguyên tố lẻ thỏa mãn $p \mid \left(a^{2^n}+1\right)$. Chứng minh rằng $p \equiv 1\left(\text{mod } 2^{n+1}\right)$.

Chứng minh. Gọi h là cấp của a theo modulo p. Ta có

$$a^{2^n} \equiv -1(\text{mod } p) \Leftrightarrow a^{2^{n+1}} \equiv 1(\text{mod } p)$$

Suy ra $h \mid 2^{n+1}$ mà h không là ước của 2^n nên $h = 2^{n+1}$. Do $h \mid p-1$ nên $p \equiv 1(\text{mod } h)$ hay $p \equiv 1\left(\text{mod } 2^{n+1}\right)$.

TÀI LIỆU THAM KHẢO

1. Phan Huy Khải, *Các chuyên đề Số học*, Nxb Giáo dục, 2005.
2. Nguyễn Vũ Lương, Nguyễn Ngọc Thắng, Nguyễn Lưu Sơn, Phạm Văn Hùng, *Các bài giảng số học*, Nxb Đại Học Quốc Gia Hà Nội, 2006.
3. Nguyễn Văn Mậu, Trần Nam Dũng, Đặng Hùng Thắng, Đặng Huy Ruận, *Các vấn đề chọn lọc của số học*, Nxb Giáo dục, 2008.
4. Đặng Hùng Thắng, Nguyễn Văn Ngọc, Vũ Kim Thuỷ, *Bài giảng số học*, Nxb Giáo dục, 1997.
5. Titu Andreescu, Dorin Andrica, Zuming Feng, *104 Number theory problems from the training of the USA IMO team*, Nxb Birkhauser, 2006.

SUMMARY

ORDER OF PRINCIPLES AND APPLICATIONS

Tran Thi Hong Minh*
College of Education - TNU

In group theory, the order of an element is one of the important concepts and has many applications. Understanding the properties and applications of order of element are essential for. This article presents some important properties about order of an integer number and its application in number theory.

Keywords: *principles, element, number theory*

Ngày nhận bài:18/3/2015; Ngày phản biện:03/4/2015; Ngày duyệt đăng: 31/5/2015
Phản biện khoa học: *TS. Trần Nguyên An – Trường Đại học Sư phạm - ĐHTN*

* *Tel: 0973 268338, Email: minh.tranhong.md@gmail.com*