PHẦN 6. KỸ THUẬT SỐ MŨ ĐÚNG VÀ ĐỊNH LÝ LTE

Cho số nguyên n và p là số nguyên tố, ký hiệu $k = v_p(n)$ là số mũ đúng của p trong n nếu như n chia hết cho p^k nhưng không chia hết cho p^{k+1}. Quy ước $v_p(0) = +\infty$.

Các tính chất quan trọng:

- $v_p(ab) = v_p(a) + v_p(b),\ v_p(a^n) = n \cdot v_p(a).$
- $v_p(a) \ge v_p(b), \forall p$ khi và chỉ khi $b \mid a$.
- $v_p(a)$ chẵn với mọi p khi và chỉ khi n là số chính phương.
- $v_p(a \pm b) \ge \min\left\{v_p(a), v_p(b)\right\}$, đẳng thức xảy ra khi $v_p(a) \ne v_p(b)$.
- (Legendre) $v_p(n!) = \left[\dfrac{n}{p}\right] + \left[\dfrac{n}{p^2}\right] + \cdots$
- $v_p(a^n - b^n) = v_p(a - b)$ nếu $p \mid a - b$ và a, b, n không chia hết cho p. (*đây là phiên bản dễ của định lý LTE*). Nếu n lẻ thì có thể đổi $b \to -b$ và có $v_p(a^n + b^n) = v_p(a + b)$.

(Định lý LTE cho số $p = 2$) Cho hai số nguyên lẻ x, y thỏa mãn $2 \mid x - y$ và n là số nguyên dương chẵn. Khi đó:

$$v_2\left(x^n - y^n\right) = v_2\left(x - y\right) + v_2\left(x + y\right) + v_2\left(n\right) - 1.$$

(Định lý LTE cho số p lẻ) Cho hai số nguyên x, y; n là số nguyên dương và p là số nguyên tố lẻ thỏa mãn:

$$p \mid x - y;\ p \nmid x;\ p \nmid y.\ \text{Ta có } v_p\left(a^n - b^n\right) = v_p\left(a - b\right) + v_p\left(n\right).$$

Nếu n lẻ thì ta cũng có $v_p(a^n + b^n) = v_p(a + b) + v_p(n)$.

Bài 6.1. *(Vĩnh Long)* Chứng minh rằng tồn tại vô số số nguyên dương n để $n \mid 2^n + 1$.

Lời giải.

Ta chỉ cần chọn $n = 3^k$ với $k \in \mathbb{Z}^+$ thì theo định lý LTE

$$v_3(2^n + 1) = v_3(2 + 1) + v_3(n) = k + 1.$$

Suy ra $n = 3^k \mid 2^n + 1$.

Bài 6.2. *(Hà Nam)* Cho q là số nguyên tố lẻ và đặt

$$A = (2q)^{2q} + (2q)! + ((2q)!)^{2q}.$$

Chứng minh rằng A có một ước nguyên tố $p > 2q$.

Lời giải.

Giả sử ngược lại rằng mọi ước nguyên tố p của Q đều không vượt quá $2q$. Khi đó, rõ ràng

$$p \mid (2q)!, p \mid \left((2q)!\right)^{2q} \text{ nên } p \mid 2q.$$

Từ đó suy ra $p = 2$ hoặc $p = q$.

Số Q sẽ có dạng $2^m q^n$ với $m, n \in \mathbb{N}$. Theo định lý Legendre thì

$$v_2((2q)!) = \frac{2q}{2} + \frac{2q}{2^2} + \cdots \le 2q\left(\frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots\right) < 2q \text{ và } v_q((2q)!) = 2 \text{ vì } q > 2.$$

Từ đó suy ra $Q < 2^{2q} q^2 < (2q)^{2q}$, vô lý.

Vậy nên Q có ước nguyên tố lớn hơn $2q$.

Bài 6.3. *(Olympic Gặp gỡ Toán học)* Cho a, b, c là các số nguyên dương mà $\frac{a}{b} + \frac{b}{c} + \frac{c}{a} \in \mathbb{Z}^+$. Chứng minh rằng abc là một lập phương đúng.

Lời giải.

Theo giả thiết, ta có $abc \mid a^2c + b^2a + c^2b$.

Do bài toán không thay đổi nếu thay $(a,b,c) \to (ka,kb,kc)$ nên không mất tính tổng quát, có thể giả sử $\gcd(a,b,c) = 1$.

Xét số $p \mid abc$ và đặt $v_p(a) = x,\ v_p(b) = y,\ v_p(c) = z$ thì một trong ba số này phải bằng 0. Ta cũng có thể giả sử $x = 0$ và $y + z > 0$. Khi đó $v_p(abc) = y + z$ và

$$v_p(a^2c) = z,\ v_p(b^2a) = 2y,\ v_p(c^2b) = 2z + y\,.$$

Nếu $z > 2y$ thì $2y = \min\{z, 2y, 2z + y\}$ nên $y + z \le 2y \to z \le y$, mâu thuẫn.

Nếu $z < 2y$ thì $z = \min\{z, 2y, 2z + y\}$ nên $y + z \le z$, vô lý.

Do đó $z = 2y$ vàa $v_p(abc) = 3y$, chia hết cho 3. Điều này đúng với mọi ước nguyên tố của abc nên từ đó suy ra abc phải là một lập phương đúng.

Bài 6.4. *(Thanh Hóa)* Tìm bộ ba các số nguyên dương (p, n, k) thỏa mãn p là số nguyên tố Fermat và

$$p^n + n = (n+1)^k \qquad (1).$$

(Số nguyên tố Fermat là số nguyên tố có dạng $2^{2^x} + 1$ với x là số tự nhiên).

Lời giải.

Đặt $\alpha = 2^x$. Ta xét các trường hợp sau:

Nếu $n=1$ thì (1) viết lại là $p=2^k-1=2^\alpha+1\Rightarrow k=2;\ \alpha=1\Rightarrow p=3.$

Nếu $n\ge 2.$ Ta gọi r là một ước nguyên tố của n.

Từ phương trình ta suy ra $p^n\equiv 1\pmod n\Rightarrow p^n\equiv 1\pmod r.$ Do đó $(b,r)=1.$ Đặt $k=\operatorname{ord}_p(r)$ thì $k\mid r-1,n$ nên $k\mid \gcd(r-1,n)=1\to k=1.$ Vì $r\mid p-1\Rightarrow r\mid 2^\alpha\Rightarrow r=2\Rightarrow 2\mid n.$

Ta có $(1)\Leftrightarrow p^n-1=(n+1)\left[(n+1)^{k+1}-1\right]\Rightarrow v_2\left(p^n-1\right)=v_2\left((n+1)^{k-1}-1\right).$ Nếu $k-1$ lẻ thì $v_2\left((n+1)^{k-1}-1\right)=v_2(n)<v_2\left(p^2-1\right)+v_2(n)-1=v_2\left(p^n-1\right)$ mâu thuẫn, vậy $k-1$ chẵn.

Áp dụng định lý LTE, ta có

$$v_2\left(p^n-1\right)=v_2\left((n+1)^{k-1}-1\right)\Leftrightarrow v_2(p-1)+v_2(p+1)=v_2(n+2)+v_2(k-1).$$

Nếu $v_2(k-1)\ge v_2(p-1)\Rightarrow p-1\mid k\Rightarrow (n+1)^k\equiv n+1\pmod p$ (theo định lí *Fermat* nhỏ). Tuy nhiên theo (1) thì $n\equiv (n+1)^k\equiv n+1\pmod p$, vô lý. Do đó

$$v_2(k-1)<v_2(p-1)\Rightarrow 1\le v_2(p+1)=v_2\left(2^\alpha+2\right)<v_2(n+2)\Rightarrow n\equiv 2\pmod 4.$$

Nếu $p>5$ thì $2^{2^x}+1>5\Rightarrow x\ge 2\Rightarrow p\equiv 2\pmod 5$ nên

$$p^n\equiv 4\pmod 5 \text{ và } 4+n\equiv (n+1)^k\pmod 5.$$

Mà $4+n\not\equiv (n+1)\pmod 5\Rightarrow k\not\equiv 1\pmod 4$ nên $k\equiv 3\pmod 4\Rightarrow 4+n\equiv (n+1)^3\pmod 5.$

Với $n\equiv 0\pmod 5\Rightarrow 4+n-(n+1)^3\equiv 3\pmod 5$ mâu thuẫn, tương tự với các trường hợp: $n\equiv 1\pmod 5;\ n\equiv 2\pmod 5;\ n\equiv 3\pmod 5;\ n\equiv 4\pmod 5$ đều dẫn đến mâu thuẫn.

Vì thế nên $n+4\not\equiv (n+1)^3\pmod 5$. Ta loại trường hợp $p>5.$ Tiếp theo,

Nếu $p=5$ thì $\alpha=2.$ Khi đó $3=v_2(n+2)+v_2(k-1).$ Do

$$v_2(n+2)\ge 2\Rightarrow v_2(n+2)=2;\ v_2(k-1)=1.$$

Ta cũng có $5^n+n=(n+1)^k$. Với $n=2\Rightarrow k=3$. Còn với $n\ge 3,$ gọi q là ước nguyên tố lẻ của n thì $q\mid 5^{(n.q-1)}-1=5^2-1=24.$ $q\mid 3\Rightarrow q=3\ \Rightarrow n\equiv 0\pmod 6.$ Kết hợp với

$$n\equiv 2\pmod 4\Rightarrow 5^n\equiv -1\pmod{13}\Rightarrow n-1\equiv (n+1)^k\pmod{13}.$$

Lại áp dụng định lý LTE, ta có

$$v_3\left(5^n-1\right)=v_3\left((n+1)^{k-1}-1\right)\Leftrightarrow 1+v_3\left(\frac{n}{2}\right)=v_3(k-1)+v_3(n)\Rightarrow 3\mid k-1.$$

Ta cũng có $k \equiv 3 \pmod 4 \Rightarrow k \equiv 7 \pmod{12}$. Theo định lí *Fermat* nhỏ suy ra:

$$(n+1)^k \equiv (n+1)^7 \equiv \pm(n+1) \pmod{13} \Rightarrow n-1 \equiv -n-1 \pmod{13} \Rightarrow n \equiv \pmod{13}, \text{ vô lí.}$$

(vì với $13 \mid n \Rightarrow 5^n \equiv 1 \pmod{13}$, mâu thuẫn do $5^n \equiv 5 \pmod{13}$).

Vậy nên tất cả các bộ số cần tìm là $(p,n,k)=(3,1,2)$; $(p,n,k)=(5,2,3)$.

Bài 6.5. *(Kiểm tra đội tuyển Vĩnh Phúc)* Tìm tất cả các số nguyên dương n sao cho $(n!)^n$ chia hết $(n^2-1)!$.

Lời giải. Với mỗi số nguyên tố p và mỗi số nguyên dương q ký hiệu $\nu_p(q)$ là số mũ đúng của p trong phân tích tiêu chuẩn ra thừa số nguyên tố của $q!$.

Đầu tiên ta chứng minh rằng $n=4$ và $n=p$ là số nguyên tố thì $(n!)^n \nmid (n^2-1)!$.

Thật vậy,

- Nếu $n=4$ thì $\nu_2(4!)^4 = 4\nu_2(24) = 4.3 = 12 > 11 = \nu_2(4^2-1)!$, vì vậy $(n!)^n \nmid (n^2-1)!$
- Nếu $n=p$ thì $\nu_n(n!)^n = n.\nu_2(n!) = n > n-1 = \nu_n(n^2-1)!$ vì vậy $(n!)^n \nmid (n^2-1)!$

Tiếp theo, ta chứng minh rằng khi $n \neq 4$ và $n \neq p \in \wp$ thì $(n!)^n \mid (n^2-1)!$

Gọi p là một ước nguyên tố bất kỳ của n. Ta sẽ chứng minh rằng $n.\nu_p(n!) \le \nu_p(n^2-1)!$

Gọi $n = p^d.k$ với $k,d \in N^*, (k,p)=1$ đưa về

$$n.\nu_p(n!) \le \nu_p(n^2-1)! \Leftrightarrow n.\nu_p(n!) \le \nu_p(n^2!) - \nu_p(n^2) = \nu_p(n^2!) - 2d$$

$$\Leftrightarrow 2d + p^d.k.\sum_{j\in N^*}\left[\frac{p^d k}{p^j}\right] \le \sum_{j\in N^*}\left[\frac{p^{2d}k^2}{p^j}\right]$$

Nhưng ta cũng có

$$\sum_{j\in N^*}\left[\frac{p^{2d}k^2}{p^j}\right] = \sum_{j\in N^*}\left[p^d\cdot k\cdot\frac{p^d k}{p^j}\right] = p^d\cdot k\sum_{j\in N^*}\left[\frac{p^d k}{p^j}\right] + \sum_{j\in N^*}\left[p^d\cdot k\cdot\left\{\frac{p^d k}{p^j}\right\}\right].$$

Bất đẳng thức cần chứng minh tương đương với

$$\sum_{j\in N}\left[p^d\cdot k\cdot\left\{\frac{p^d k}{p^j}\right\}\right] \ge 2d.$$

Hay cần chứng minh rằng $\sum_{j=d+1}^{2d}\left[p^d \cdot k \cdot \left\{\frac{p^d k}{p^j}\right\}\right] \ge 2d$ hoặc $\sum_{j=1}^{d}\left[p^d \cdot k \cdot \left\{\frac{k}{p^j}\right\}\right] \ge 2d$

Nhận xét: nếu $x, y \in N^*$ và x không chia hết cho y thì $\left\{\frac{y}{x}\right\} \ge \frac{1}{x}$.

Từ đó, ta có

$$\sum_{j=1}^{d}\left[p^d \cdot k \cdot \left\{\frac{k}{p^j}\right\}\right] \ge \sum_{j=1}^{d}\left[p^d \cdot k \cdot \frac{1}{p^j}\right] = \sum_{s=0}^{d-1}\left[p^s \cdot k\right] = \sum_{s=0}^{d-1} p^s \cdot k = k\left(1+p+p^2+\cdots+p^{d-1}\right).$$

Cuối cùng, dễ dàng chứng minh: $k\left(1+p+p^2+\cdots+p^{d-1}\right) \ge 2d$ bằng quy nạp.

- Nếu $d=0$ thì bất đẳng thức trên đúng
- Nếu $d=1$, chúng ta phải có $k \ge 2$ (ngược lại n là số nguyên tố) và BĐT đúng.
- Nếu $d=2$, ta cần chứng minh rằng $k(1+p) \ge 4$. Nếu $p=2$ thì $k \ge 2$ (ngược lại thì $n=4$) và bất đẳng thức đúng, trong khi $p \ge 3$.
- Nếu $d \ge 3$, thì $k\left(1+p+p^2+\cdots+p^{d-1}\right) \ge 1+2+2^2+\cdots+2^{d-1} = 2^d - 1 \ge 2d$.

Bài toán được giải quyết hoàn toàn.