Mathley # 10/2015

Mathley là nhóm giải toán trên mạng xuất bản bài toán và lời giải định kỳ, bài viết phù hợp với học sinh trung học có năng khiếu toán học và các bạn trẻ yêu toán học, tham gia các cuộc thi học sinh giỏi toán. Mỗi năm có sáu ấn bản điện tử được ra đời nhằm phục vụ phong trào giải toán. **Mathley** is an online problem solving corner with prolems, solutions, and materials freely accessible to junior up to high school students. The corner is is made public six times per year on a regular basis dedicated to the promotion of problem solving among junior and high school students.

Email: mathley@hus.edu.vn.
Website: www.hexagon.edu.vn/mathley.html

CÁC BÀI TOÁN/PROBLEMS

1. *Trần Quang Hùng, Trường THPT chuyên Khoa học Tự nhiên, Đại học Quốc Gia Hà Nội.* Cho tam giác ABC nhọn nội tiếp đường tròn (O) cố định với B, C cố định và A di chuyển trên (O), tâm nội tiếp I, phân giác AD. K, L lần lượt là tâm ngoại tiếp tam giác CAD, ABD. Đường thẳng qua O lần lượt song song DL, DK theo thứ tự cắt đường thẳng qua I lần lượt vuông góc IB, IC tại M, N. Chứng minh rằng MN luôn tiếp xúc một đường tròn cố định khi A di chuyển trên (O).

Let ABC be an acute triangle inscribed in a circle (O) that is fixed, and two of the vertices B, C are fixed while vertex A varies on the circumference of the circle. Let I be the center of the incircle, and AD the angle bisector. Let K, L be the circumcenters of CAD, ABD. A line through O parallel to DL, DK intersects the line that is through I perpendiculaar to IB, IC at M, N respectively. Proe that MN is tangent to a fixed circle when A varies on the circle (O).

2. *Trần Quang Hùng, Nguyễn Lê Phước, Thanh Xuân, Hà Nội.* Cho tứ giác $ABCD$ nội tiếp, hai đường chéo AC và BD cắt nhau tại G. M là trung điểm của CD. E, F lần lượt thuộc BC, AD sao cho $ME \parallel AC$ và $MF \parallel BD$. Gọi H là hình chiếu của G lên CD. Đường tròn ngoại tiếp tam giác MEF cắt CD tại N khác M. Chứng minh rằng $MN = MH$.

A quadrilateral $ABCD$ is inscribed in a circle and its two diagonals AC, BD meet at G. Let M be the center of CD, E, F be the points on BC, AD respectively such tht $ME \parallel AC$ and $MF \parallel BD$. Point H is the projection of G onto CD. The circumcircle of MEF meets CD at N distinct from M. Prove that $MN = MH$.

3. *Đỗ Thanh Sơn, Trường THPT chuyên Khoa học Tự nhiên, Đại học Quốc Gia Hà Nội.* Cho tam giác ABC và điểm P nằm trong tam giác ABC sao cho $AP \perp BC$. E, F là hình chiếu của P lên CA, AB. Giả sử tiếp tuyến tại E, F của đường tròn ngoại tiếp tam giác AEF cắt nhau trên BC. Chứng minh rằng P là trực tâm tam giác ABC.

A point P is interior to the triangle ABC such that $AP \perp BC$. Let E, F be the projections of CA, AB. Suppose that the tangents at E, F of the circumcircles of triangle AEF meets at a point on BC. Prove that P is the orthocenter of triangle ABC.

4. *Nguyễn Minh Hà, Trường THPT chuyên Sư phạm, Đại học Sư phạm Hà Nội.* Cho tam giác ABC và các điểm E, F sao cho các tam giác ABE, ACF đồng dạng ngược hướng, theo thứ tự cân tại E, F, theo thứ tự có trực tâm là H, K. Gọi BE, CK lần lượt cắt CF, CH tại M, N. Chứng minh rằng MN đi qua tâm đường tròn ngoại tiếp tam giác ABC.

Points E, F are in the plane of triangle ABC so that triangles ABE and ACF are the opposite directed, and the two triangles are isosceles in that $BE = AE$, $AF = CF$. Let H, K be the orthocenter of triangle ABE, ACF respectively. Points M, N are the intersections of BE and CF; CK and CH. Prove that MN passes through the center of the circumcircle of triangle ABC.

Hãy quan sát số mũ!

Titu Andreeescu
Gabriel Dopinescu

Phạm Huy Hoàng dịch từ mục **Look at the exponent!** trong cuốn sách *Problems from the book*.

Trong bài viết này, ta sử dụng những kí hiệu sau

- $\#A$ là số phần tử của tập hợp A.
- $a \mid b$ nghĩa là a là ước của b, $a \nmid b$ nghĩa là a không là ước của b.
- $\gcd(a_1, a_2, ..., a_n)$ là ước số chung lớn nhất của các số $a_1, a_2, ..., a_n$ nguyên dương.
- $\text{lcm}(a_1, a_2, ..., a_n)$ là bội số chung nhỏ nhất của các số $a_1, a_2, ..., a_n$ nguyên dương.
- $\lfloor x \rfloor$ là phần nguyên của số thực x, là số nguyên lớn nhất không vượt quá x.

0.1 Lý thuyết và ví dụ

Hầu hết trong các bài toán chứng minh chia hết, chúng ta thường đưa về các phép đồng dư và sử dụng các định lý số học kinh điển như định lý Fermat, định lý Euler, hay định lý Wilson. Nhưng khi đối mặt với bài toán chứng minh

$$\text{lcm}(a,b,c)^2 \mid \text{lcm}(a,b).\text{lcm}(b,c).\text{lcm}(c,a)\,, \forall a,b,c \in \mathbb{N}^*,$$

thì việc sử dụng các định lý cổ điển sẽ rất khó khăn. Tuy nhiên, có một phương pháp tự nhiên nhưng cũng khá thông minh để chứng minh các lớp bài toán chia hết: nếu ta cần chứng minh $a \mid b$, thì ta chỉ cần chứng minh số mũ của mọi số nguyên tố trong phân tích tiêu chuẩn của a không vượt qua số mũ của các số nguyên tố đó trong phân tích tiêu chuẩn của b. Để tiện cho việc theo dõi, ta kí hiệu $v_p(a)$ là số mũ của số nguyên tố p trong phân tích tiêu chuẩn của a. Tất nhiên, nếu $p \nmid a$ thì $v_p(a) = 0$.
Một số tính chất quan trọng nhưng cũng khá dễ chứng minh của $v_p(a)$:

1. $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$.
2. $v_p(ab) = v_p(a) + v_p(b)$ với mọi a, b nguyên dương. Từ tính chất này ta thấy rằng nếu a, b nguyên dương và $a \mid b$ khi và chỉ khi với mọi p nguyên tố thì $v_p(a) \leq v_p(b)$, và $a = b$ khi và chỉ khi $v_p(a) = v_p(b)$ với mọi số nguyên tố p.
3. $v_p\left(\gcd(a_1, a_2, ..., a_n)\right) = \min_{i=\overline{1,n}}\{v_p(a_i)\}$.
4. $v_p\left(\text{lcm}(a_1, a_2, ..., a_n)\right) = \max_{i=\overline{1,n}}\{v_p(a_i)\}$.
5. (Công thức Jacobi) $v_p(n!) = \displaystyle\sum_{k\geq 0}\left\lfloor \frac{n}{p^k} \right\rfloor = \frac{n - s_p(n)}{p-1}$, trong đó $s_p(n)$ là tổng các chữ số của n khi viết dưới cơ số p. Nhận thấy rằng tính chất ba và bốn là kết quả trực tiếp từ đinh nghĩa. Một tính chất không hiển nhiên lắm là tính chất năm; tính chất này được suy ra từ kết quả rằng trong các số từ 1 đến n, có $\left\lfloor \frac{n}{p} \right\rfloor$ số chia hết cho p, $\left\lfloor \frac{n}{p^2} \right\rfloor$ số chia hết cho p^2 và tương tự cho các trường hợp còn lại. Dấu bằng thứ hai của tính chất năm cũng không khó để chứng minh, ta viết $n = a_0 + a_1 p + \cdots + a_k p^k$, trong đó $a_i \in \{0, 1, \cdots, p-1\}$ và $a_k \neq 0$. Khi đó ta có:

$$\sum_{k\geq 0}\left\lfloor \frac{n}{p^k} \right\rfloor = a_1 + a_2 p + \cdots + a_k p^{k-1} + a_2 + a_3 p + \cdots + a_k p^{k-2} + \cdots + a_k.$$

   Sử dụng tính chất tổng của cấp số nhân ta có ngay điều cần chứng minh.

Ta sẽ đến phần ví dụ áp dụng.

Ví dụ 1. *Cho a, b là các số nguyên sao cho $a \mid b^2, b^3 \mid a^4, a^5 \mid b^6, b^7 \mid a^8, ...$ Chứng minh rằng $a = b$.*

Chứng minh. Theo như ý tưởng phần trên, chúng ta sẽ chứng minh rằng $v_p(a) = v_p(b)$ với mọi p nguyên tố. Giả thiết cho ta rằng $a \mid b^2, b^3 \mid a^4, a^5 \mid b^6, b^7 \mid a^8, ...$ hay ta có thể viết lại là $a^{4n+1} \mid b^{4n+2}$ và $b^{4n+3} \mid a^{4n+4}$ với mọi n nguyên dương.
Quan hệ $a^{4n+1} \mid b^{4n+2}$ có thể viết lại dưới dạng $(4n+1)v_p(a) \leq (4n+2)v_p(b)$ với mọi n, từ đó ta có:

$$v_p(a) \leq \lim_{x\to\infty} \frac{4n+2}{4n+1} v_p(b) = v_p(b).$$

Chứng minh tương tự, sử dụng điều kiện $b^{4n+3} \mid a^{4n+4}$ ta có $v_p(b) \leq v_p(a)$. Từ đó ta có với mọi p nguyên tố thì $v_p(a) = v_p(b)$. □

Ví dụ 2. *Chứng minh rằng*

$$\mathrm{lcm}(a,b,c)^2 \mid \mathrm{lcm}(a,b) \cdot \mathrm{lcm}(b,c) \cdot \mathrm{lcm}(c,a)$$

với mọi bộ ba số a, b, c nguyên dương.

Chứng minh. Gọi p là một số nguyên tố bất kì. Chúng ta có $v_p\left(\mathrm{lcm}(a,b,c)^2\right) = 2\max\{x,y,z\}$ và

$$v_p\left(\mathrm{lcm}(a,b) \cdot \mathrm{lcm}(b,c) \cdot \mathrm{lcm}(c,a)\right) = \max\{x,y\} + \max\{y,z\} + \max\{z,x\},$$

trong đó $x = v_p(a), y = v_p(b), z = v_p(c)$. Điều cần chứng minh tương đương với $\max\{x,y\} + \max\{y,z\} + \max\{z,x\} \geq 2\max\{x,y,z\}$, với mọi x, y, z nguyên dương. Nhưng bất đẳng thức này dễ dàng được suy ra nhờ tính đối xứng: chúng ta hoàn toàn có thể giả sử rằng $x \geq y \geq z$ và bất đẳng thức trở thành $2x + y \geq 2x$. □

Chúng ta sẽ tiếp cận với bài toán khó hơn. Những bài toán tiếp theo đều dựa trên những quan sát ở phần đầu của bài viết.

Ví dụ 3 (Paul Erdos)**.** *Chứng minh rằng tồn tại hằng số c sao cho với mọi a, b, n nguyên dương thỏa mãn $a!.b! \mid n!$ thì ta có $a + b < n + c\ln n$.*

Chứng minh. Quan sát bài toán trên, ta chưa thấy một đánh giá nào xác đáng để suy ra được c. Vậy chúng ta sẽ bắt đầu từ giả thiết $a!.b! \mid n!$. Khi đó $v_2(a!) + v_2(b!) \leq v_2(n!)$, mà theo công thức Jacobi, bất đẳng thức trên có dạng $a - s_2(a) + b - s_2(b) \leq n - s_2(n) < n$. Như vậy ta đã gần đạt được bất đẳng thức mong muốn:

$$a + b < n + s_2(a) + s_2(b).$$

Chúng ta cần quan sát thêm rằng, tổng các chữ số của một số A khi được viết dưới hệ nhị phân sẽ không vượt quá số các chữ số của A khi viết dưới hệ nhị phân. Thật vậy, gọi k là số các chữ số của A khi viết dưới hệ nhị phân, ta có $2^{k-1} \leq A < 2^k$, từ đó tổn các chữ số của A trong hê nhị phân không vượt quá $1 + \lfloor \log_2 A \rfloor$. Do đó ta có đánh giá mới sau:

$$a + b < n + s_2(a) + s_2(b) \leq n + 2 + \log_2 ab \leq n + 2 + \log_2 n$$

(vì ta có $a, b < n$) và từ đó ta có ngay điều cần chứng minh. □

Bài toán sau đây đã từng xuất hiện trong tạp chí Kvant và đã tốn rất nhiều thời gian để có được lời giải đơn giản của S. Konyagin. Trong bài viết, chúng tôi không đề cập đến chứng minh của anh ta mà bằng một chứng minh khác đơn giản hơn.

Ví dụ 4 (Kvant)**.** *Có tồn tại hay không một tập hợp vô hạn các số nguyên dương mà với cách chọn bất kì một số phần tử trong tập thì tổng các phần tử đó không là một bình phương đúng?*

Chứng minh. Chúng ta chọn $A = \{2^n.3^{n+1} | n > 1\}$. Như vậy tổng của một số các phần tử thuộc A sẽ có dạng $2^x.3^{x+1}.y$, với $(y,6) = 1$. Ta thấy rằng đây không phải là bình phương đúng. Thật vậy, giả sử $2^x.3^{x+1}.y = k^2$ thì do $(y,6) = 1$ và $(2,3) = 1$ nên $x, x+1$ đều chia hết cho 2, mà đây là điều vô lý. Do đó tập A là một sự lựa chọn đúng đắn. □

Bài toán sau đây cho thấy vẻ đẹp của Số học sơ cấp. Nó tổng hợp nhiều ý tưởng và kĩ thuật, và cho một kết quả rất đẹp. Bạn đọc có thể thử sức với cách nhìn tổ hợp bằng cách đếm các ma trận khả nghịch với các phần tử thuộc trường $\mathbb{Z}/2\mathbb{Z}$.

Ví dụ 5. *Chứng minh rằng với mọi n nguyên dương, $n!$ là ước của*

$$\prod_{k=0}^{n-1} \left(2^n - 2^k\right).$$

Chứng minh. Chúng ta sẽ xét một số nguyên tố p bất kì, và chỉ cần $p \leq n$. Đầu tiên chúng ta sẽ xem xét với $p = 2$. Ta có

$$v_2(n!) = n - s_2(n) \leq n - 1$$

và cũng có

$$v_2\left(\prod_{k=0}^{n-1}\left(2^n - 2^k\right)\right) = \sum_{k=0}^{n-1} v_2\left(2^n - 2^k\right) = 0 + 1 + ... + n - 1 \geq n - 1.$$

Bây giờ với p nguyên tố lớn hơn 2. Từ định lý Fermat nhỏ ta có $p \mid 2^{p-1} - 1$ do đó $p \mid 2^{k(p-1)} - 1$ với mọi $k \geq 1$. Ta có

$$\prod_{k=0}^{n-1}\left(2^n - 2^k\right) = 2^{\frac{n(n-1)}{2}} \prod_{k=1}^{n-1}\left(2^k - 1\right),$$

từ đó ta suy ra

$$\begin{aligned} v_p\left(\prod_{k=0}^{n-1}\left(2^n - 2^k\right)\right) &= \sum_{k=1}^{n} v_p\left(2^k - 1\right) \\ &\geq \sum_{1 \leq k(p-1) \leq n} v_p\left(2^{k(p-1)} - 1\right) \\ &\geq \#\left\{k | 1 \leq k(p-1) \leq n\right\}. \end{aligned}$$

Mặt khác, ta có

$$\#\left\{k | 1 \leq k(p-1) \leq n\right\} = \left\lfloor \frac{n}{p-1} \right\rfloor,$$

nên dẫn đến

$$v_p\left(\prod_{k=0}^{n-1}\left(2^n - 2^k\right)\right) \geq \left\lfloor \frac{n}{p-1} \right\rfloor.$$

Nhưng

$$v_p\left(n!\right) = \frac{n - s_p(n)}{p-1} \leq \frac{n-1}{p-1} < \frac{n}{p-1},$$

mà do $v_p(n!)$ là số nguyên nên

$$v_p\left(n!\right) \leq \left\lfloor \frac{n}{p-1} \right\rfloor.$$

Từ các bất đẳng thức trên, ta rút ra được

$$v_p\left(\prod_{k=0}^{n-1}\left(2^n - 2^k\right)\right) \geq v_p\left(n!\right).$$

Bài toán được chứng minh xong. □

Việc giải phương trình Diophante cũng sử dụng được những quan sát về số mũ. Sau đây là một bài toán khó tại một kì thi của Nga.

Ví dụ 6 (Tuymaada Olympiad)**.** *Chứng minh rằng phương trình*

$$\frac{1}{10^n} = \frac{1}{n_1!} + \frac{1}{n_2!} + ... + \frac{1}{n_k!}$$

không có nghiệm nguyên thỏa mãn $1 \geq n_1 \geq n_2 \geq ... \geq n_k$.

Chứng minh. Ta có

$$10^n\left((n_1 + 1)...(n_k - 1)n_k + ... + (n_{k-1} + 1)...(n_k - 1)n_k + 1\right) = n_k!$$

cho ta thấy n_k là ước của 10^n. Do đó ta có thể viết $n_k = 2^x.5^y$. Đặt

$$S = (n_1 + 1)...(n_k - 1)n_k + ... + (n_{k-1} + 1)...(n_k - 1)n_k + 1.$$

Đầu tiên, giả sử rằng x, y đều là số dương. Khi đó $\gcd(S, 10) = 1$, và dẫn tới $v_2(n_k!) = v_5(n_k!)$. Theo công thức Jacobi ta có $\left\lfloor \frac{n_k}{2^j} \right\rfloor = \left\lfloor \frac{n_k}{5^j} \right\rfloor$ với mọi j (vì ta đã có $\left\lfloor \frac{n_k}{2^j} \right\rfloor \geq \left\lfloor \frac{n_k}{5^j} \right\rfloor$) và từ đó suy ra $n_k \leq 3$. Bằng phép thử đơn giản, thay n_k lần lượt các giá trị không vượt quá 3, ta thấy phương trình vô nghiệm.
Tiếp theo, giả sử $y = 0$. Khi đó S là số lẻ và $v_2(n_k!) = n \leq v_5(n_k!)$. Mà trên thực tế ta luôn có $v_2(n_k!) \geq v_5(n_k!)$ nên $v_2(n_k!) = v_5(n_k!)$, và lại trở lại trường hợp trên: vô nghiệm.
Khi đó ta có $x = 0$. Một quan sát quan trọng trong bài toán này: nếu $n_k > n_{k-1} + 1$, thì S là số lẻ và ta lại có $v_2(n_k!) \leq v_5(n_k!)$, trở lại trường hợp trên. Khi đó ta có $n_k = n_{k-1} + 1$. Chú ý rằng n_k là lũy thừa của 5, ta suy ra $S \equiv 2 (\mathrm{mod} 4)$ và $v_2(n_k!) = n + 1 \leq v_5(n_k!) + 1$. Từ đó ta có

$$\left\lfloor \frac{n_k}{2} \right\rfloor \leq \left\lfloor \frac{n_k}{5} \right\rfloor + 1,$$

và giải bất phương trình này ta được $n_k \leq 6$. Do n_k là lũy thừa của 5 nên $n_k = 5, n_{k-1} = 4$ và $n_i \leq 4$. Thử các trường hợp ta có ngay phương trình vô nghiệm. □

Trong kì thi APMO năm 1997, có một bài toán yêu cầu chứng minh tồn tại số tự nhiên n thỏa mãn $100 < n < 1997$ mà thỏa mãn $n \mid 2^n + 2$. Chúng tôi xin mời bạn đọc chứng minh rằng giá trị 2.11.43 là một giá trị thỏa mãn, và sẽ hướng dẫn các bạn làm thế nào để tìm được số này. Tuy nhiên, bằng chứng minh toán học thì tất cả các nghiệm của bài toán trên đều là lẻ. Chứng minh điều này quả thực là khó và lời giải đầu tiên của bài toán này thuộc về Schinzel.

Ví dụ 7 (Schinzel)**.** *Chứng minh rằng với mọi $n > 1$ ta không thể có $n \mid 2^{n-1} + 1$.*

Chứng minh. Mặc dù lời giải rất ngắn, nhưng trong đó có rất nhiều kĩ thuật và sự khéo léo. Giả sử rằng n là một nghiệm thỏa mãn. Viết $n = \prod_{i=1}^{s} p_i^{k_i}$ với $p_1 < p_2 < ... < p_s$ là các số nguyên tố. Ý tưởng ở đây là quan sát $v_2(p_i - 1)$. Chọn p_i để đại lượng này được giảm đến mức tối thiểu và viết $p_i = 1 + 2^{r_i} m_i$ với m_i lẻ. Khi đó $n \equiv 1 (\mathrm{mod} 2^{r_i})$ và ta có thể viết $n - 1 = 2^{r_i}.t$. Ta có $2^{2^{r_i}.t} \equiv -1 (\mathrm{mod} p_i)$, dẫn tới

$$-1 \equiv 2^{2^{r_i}.t.m_i} \equiv 2^{(p_i-1)t} \equiv 1 (\mathrm{mod} p_i)$$

(dấu đồng dư cuối cùng thu được bằng cách sử dụng định lý Fermat nhỏ). Do đó $p_i = 2$, hiển nhiên dẫn tới mâu thuẫn. □

Bài toán sau đây là một bài toán khó, nhưng những ý tưởng được sử dụng cực kì hữu hiệu trong nhiều bài toán khác.

Ví dụ 8 (Gabriel Dopinescu - Mathlinks contest)**.** *Cho a, b là hai số hữu tỉ dương phân biệt thỏa mãn với mọi n nguyên dương thì $a^n - b^n$ là số nguyên. Chứng minh rằng a và b là hai số nguyên.*

Chứng minh. Đầu tiên, ta viết lại a, b dưới dạng $a = \frac{x}{z}, b = \frac{y}{z}$, với x, y, z là ba số nguyên dương, đôi một nguyên tố cùng nhau và $x \neq y$. Từ giả thiết ta có $z^n \mid x^n - y^n$ với mọi số nguyên dương n trong tập vô hạn $M \subset \mathbb{N}^*$. Giả sử phản chứng rằng $z > 1$ và chọn p là ước nguyên tố của z. Nếu $p \nmid x$ thì hiển nhiên $p \nmid y$.
Để giải bai toán, ta cần hai bổ đề sau (***N.D**: hai bổ đề này gọi là "phép nâng lũy thừa" - "lifting the exponent", rất hữu hiệu trong các bài toán. Sau đây tôi sẽ trình bày cách chứng minh hai bổ đề này theo tài liệu của Amir Hossein Parvardi để bài viết ngắn gọn và cô đọng*):

Bổ đề 1. *Cho x, y là hai số nguyên (không nhất thiết dương) và n nguyên dương, p là một số nguyên tố lẻ sao cho $p \mid x - y$ và $p \nmid x, p \nmid y$. Ta có*

$$v_p(x^n \pm y^n) = v_p(x \pm y) + v_p(n).$$

Chứng minh bổ đề. Ta chỉ cần chứng minh cho trường hợp dấu trừ, trường hợp cộng là hệ quả.
Ta sử dụng quy nạp với $v_p(n)$. Đầu tiên, ta sẽ chứng minh

$$v_p(x^p - y^p) = v_p(x - y) + 1 \tag{1}$$

Để chứng minh điều này, ta sẽ chứng minh

$$p \mid x^{p-1} + x^{p-2}y + ... + xy^{p-2} + y^{p-1} \tag{2}$$

và

$$p^2 \nmid x^{p-1} + x^{p-2}y + ... + xy^{p-2} + y^{p-1}. \tag{3}$$

Với (2), ta chú ý rằng

$$x^{p-1} + x^{p-2}y + ... + xy^{p-2} + y^{p-1} \equiv px^{p-1} \equiv 0 (\mathrm{mod} p).$$

Đặt $y = x + kp$, với k là số nguyên. Với mỗi số nguyên $1 \leq t < p$ ta có

$$\begin{aligned} y^t x^{p-1-t} &\equiv (x + kp)^t x^{p-1-t} \\ &\equiv x^{p-1-t} \left(x^t + t.(kp)(x^{t-1}) \right) \\ &\equiv x^{p-1} + tkpx^{p-2} (\mathrm{mod} p^2) \end{aligned}$$

Điều đó cho thấy

$$y^t x^{p-1-t} \equiv x^{p-1} + tkpx^{p-2} (\mathrm{mod} p^2), \forall t = \overline{1, p-1}.$$

Sử dụng điều này ta có:

$$\begin{aligned} x^{p-1} + x^{p-2}y + ... + xy^{p-2} + y^{p-1} &\equiv x^{p-1} + \sum_{t=1}^{p-1} \left(x^{p-1} + tkpx^{p-2} \right) \\ &\equiv px^{p-1} + \left(\frac{p(p-1)}{2} \right) kpx^{p-2} \\ &\equiv px^{p-1} (\mathrm{mod} p^2) \end{aligned}$$

Như vậy (3) đúng và do đó (1) đúng. Trở lại bổ đề: Chúng ta muốn chứng minh rằng

$$v_p(x^n - y^n) = v_p(x - y) + v_p(n).$$

Giả sử rằng $n = p^\alpha.b$ với $\gcd(b, p) = 1$. Khi đó:

$$\begin{aligned} v_p\left(x^n - y^n\right) &= v_p\left(x^{p^\alpha b} - y^{p^\alpha b}\right) \\ &= v_p\left(x^{p^\alpha} - y^{p^\alpha}\right) \\ &= v_p\left(\left(x^{p^{\alpha-1}}\right)^p - \left(y^{p^{\alpha-1}}\right)^p\right) \\ &= v_p\left(x^{p^{\alpha-1}} - y^{p^{\alpha-1}}\right) + 1 = v_p\left(x^{p^{\alpha-2}} - y^{p^{\alpha-2}}\right) + 2 \\ &\vdots \\ &= v_p(x - y) + \alpha = v_p(x - y) + v_p(n) \end{aligned}$$

Bài toán được chứng minh hoàn toàn. □

Bổ đề 2. *Với trường hợp $p = 2$:*

1. *Cho x, y là hai số lẻ thỏa mãn $4 \mid x - y$. Khi đó ta có*

$$v_2(x^n - y^n) = v_2(x - y) + v_2(n).$$

2. *Cho x, y là hai số lẻ và n là số chẵn. Khi đó*

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

Gợi ý - Bạn đọc chứng minh dựa theo ý tưởng bài trên. Bổ đề này được chứng minh dựa trên hằng đẳng thức quen thuộc sau:

$$x^{2^n} - y^{2^n} = \left(x^{2^{n-1}} + y^{2^{n-1}}\right)\left(x^{2^{n-2}} + y^{2^{n-2}}\right) ... \left(x^2 + y^2\right)(x + y)(x - y).$$

□

Chúng ta trở lại bài toán: từ hai bổ đề trên ta có, tồn tại vô số số nguyên dương m mà

$$m \leq v_p(A^m - B^m) = v_p(A - B) + v_p(m) \leq v_p(A - B) + \left\lfloor \log_p m \right\rfloor,$$

đây là một điều vô lý khi m tùy ý và p là ước nguyên tố không vượt quá $A - B$. Khi đó ta có $p \mid x$ và $p \mid y$, trái với điều giả sử. Vậy $z = 1$ và a, b là hai số nguyên. □

Chúng ta đến với bài toán khó sau, khi mà ý tưởng nhìn vào số mũ cực kì hữu hiệu. Bài toán này xuất hiện lần đầu tiên trên AMM (America Mathematical Monthly) nhưng vào vài năm trở lại đây, nó đã được dùng lại trong khá nhiều các cuộc thi quốc tế và khu vực.

Ví dụ 9 (Armond E. Spencer - AMM E2637)**.** *Chứng minh rằng với mọi số $a_1, a_2, ..., a_n$ nguyên thì*

$$\prod_{1\le i<j\le n} \frac{a_i - a_j}{i-j}$$

là một số nguyên.

Chứng minh. Xét số nguyên tố p và ta sẽ chứng minh với mọi $k \ge 1$, có nhiều số chia hết cho p^k trong dãy $\left(a_i - a_j\right)_{1\le i<j\le n}$ hơn trong dãy $(i-j)_{1\le i<j\le n}$. Bởi vì:

$$v_p\left(\prod_{1\le i<j\le n}\left(a_i - a_j\right)\right) = \sum_{k\ge 1} N_{p^k}\left(\prod_{1\le i<j\le n}\left(a_i - a_j\right)\right)$$

với N_{p^k} ($\{(i,j)|1 \le i < j \le n\}$) là số các số trong dãy mà là bội của p và

$$v_p\left(\prod_{1\le i<j\le n}(i-j)\right) = \sum_{k\ge 1} N_{p^k}\left(\prod_{1\le i<j\le n}(i-j)\right),$$

bài toán chúng ta được giải khi điều ở trên được chứng minh. Cố định $k \ge 1$ và giả sử có đúng b_i chỉ số $j \in \{1, 2, ..., n\}$ thỏa mãn $a_j \equiv i (\mathrm{mod} p^k)$, với mỗi $i \in \{1, 2, ..., p^k - 1\}$. Khi đó:

$$N_{p^k}\left(\prod_{1\le i<j\le n}\left(a_i - a_j\right)\right) = \sum_{i=0}^{p^k-1} C_{b_i}^2.$$

Ta sẽ xem điều gì sẽ xảy ra nếu $a_i = i$. Nếu $i = 0$, khi đó số các số $1 \le j \le n$ thỏa mãn $j \equiv 0 (\mathrm{mod} p^k)$ là $\lfloor \frac{n}{p^k} \rfloor$. Nếu $i > 0$ thì mọi số $1 \le j \le n$ mà $j \equiv i (\mathrm{mod} p^k)$ có dạng $rp^k + i$ với $0 \le r \le \lfloor \frac{n}{p^k} \rfloor$. Khi đó ta có $1 + \lfloor \frac{n-i}{p^k} \rfloor$ chỉ số trong trường hợp này. Vì vậy

$$N_{p^k}\left(\prod_{1\le i<j\le n}(i-j)\right) = \sum_{i=0}^{p^k-1} C^2_{1+\left\lfloor \frac{n-i}{p^k}\right\rfloor} + C^2_{\left\lfloor \frac{n}{p^k}\right\rfloor} \tag{4}$$

Trong (4), thay $j = p^k - 1$ ta được

$$N_{p^k}\left(\prod_{1\le i<j\le n}(i-j)\right) = \sum_{j=0}^{p^k-1} C^2_{1+\left\lfloor \frac{n+j}{p^k}\right\rfloor}.$$

Như vậy ta cần chứng minh

$$\sum_{i=0}^{p^k-1} C_{b_i}^2 = \sum_{j=0}^{p^k-1} C^2_{1+\left\lfloor \frac{n+j}{p^k}\right\rfloor}.$$

Bây giờ, quan sát rằng chúng ta sẽ phải tìm min của $\sum_{i=0}^{p^k-1} C_{x_i}^2$ với $\sum_{i=0}^{p^k-1} x_i = n$ (điều này suy ra do

$$\sum_{i=0}^{p^k-1} b_i = \sum_{j=0}^{p^k-1} \left\lfloor \frac{n+j}{p^k} \right\rfloor,$$

trực tiếp từ định nghĩa của b_i). Với điều này, giả sử rằng $x_0 \le x_1 \le x_2 \le ... \le x_{p^k-1}$ là bộ p^k số nhỏ nhất (theo nghĩa tổng) (bộ số này tồn tại vì phương trình $\sum_{i=1}^{p^k-1} x_i = n$ có hữu hạn nghiệm). Nếu $x_{p^k-1} > x_0 + 1$, ta xét bộ $\left(x_0 + 1, x_1, ..., x_{p^k-2}, x_{p^k-1} - 1\right)$, có tổng các phần tử là n nhưng

$$C^2_{x_0+1} + C^2_{x_1} + ... + C^2_{x_{p^k-2}} + C^2_{x_{p^k-1}-1} < C^2_{x_0} + C^2_{x_1} + ... + C^2_{x_{p^k-2}} + C^2_{x_{p^k-1}}.$$

Bất đẳng thức này đúng do nó tương đương với $x_{p^k-1} > x_0 + 1$. Nhưng điều này mâu thuẫn với giả thiết bộ ($\left(x_0, x_1, x_2, ..., x_{p^k-1}\right)$. Do đó $x_{p^k-1} \le x_0$. □

Trên đây là một số bài toán tiêu biểu mà chúng tôi muốn giới thiệu. Các bài toán còn lại của cuốn sách vượt quá khuôn khổ chương trình toán học phổ thông, xin không trình bày tại đây.

0.2 Bài tập ứng dụng

Chú ý: Trong bài viết này, tôi chỉ chọn ra những bài toán là ứng dụng sâu sắc của các kết quả đã nêu ở trên.

Bài toán 1. *Cho* $0 < a_1 < ... < a_n$. *Tìm số m lớn nhất sao cho ta có thể tìm được các số nguyên* $0 < b_1 < b_2 < ... < b_m$ *thỏa mãn*

$$\sum_{k=1}^{n} 2^{a_k} = \sum_{k=1}^{m} b_k \text{ và } \prod_{k=1}^{n} (2^{a_k})! = \prod_{k=1}^{n} b_k!$$

Bài toán 2. *1. Chứng minh đẳng thức:*

$$(n+1)\operatorname{lcm}\left\{\left(C_n^i\right)_{i=0}^{n}\right\} = \operatorname{lcm}\left\{(i)_{i=1}^{n+1}\right\}.$$

2. ***(Hệ quả, Romanian TST 1990)*** *Chứng minh rằng bội chung nhỏ nhất của các số* $1, 2, ..., n$ *bằng bội chung nhỏ nhất của các số* C_n^i, $i = \overline{1, n}$ *khi và chỉ khi* $n + 1$ *là số nguyên tố.*

Bài toán 3 (Iran TST 2008, vòng 2)**.** *Chứng minh khi a là số nguyên dương mà* $4(a^n + 1)$ *là số lập phương đúng với mọi n nguyên dương thì* $a = 1$

Bài toán 4 (IMO 2000)**.** *Có tồn tại hay không một số nguyên dương n sao cho n có đúng 2000 ước nguyên tố và* $n \mid 2^n + 1$*?*

Bài toán 5 (China Western Olympiad 2010)**.** *Cho* m, k *là hai số nguyên không âm và* $p = 2^{2^m} + 1$ *là số nguyên tố. Chứng minh rằng*

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

2. $2^{2^{m+1}}.p^k$ *là số nguyên dương n nhỏ nhất thỏa mãn phương trình đồng dư* $2^n \equiv 1 \left(\mathrm{mod}\, p^{k+1}\right)$.

Bài toán 6 (China TST 2009)**.** *Cho* $a > b > 1$ *là hai số nguyên và b lẻ, n là một số nguyên dương. Nếu* $b^n \mid a^n - 1$*, chứng minh rằng* $a^b > \frac{3^n}{n}$.

Bài toán 7 (IMO Shortlist 2007)**.** *Tìm tất cả các toàn ánh* $f : \mathbb{N}^* \to \mathbb{N}^*$ *sao cho với mọi* m, n *nguyên dương và với mọi p nguyên tố, số* $f(m + n)$ *chia hết cho p khi và chỉ khi* $f(m) + f(n)$ *chia hết cho p.*

Bài toán 8 (Romania TST 2009)**.** *Cho* $a, n \geq 2$ *là các số nguyên có tính chất sau: Tồn tại k nguyên dương không bé hơn* 2 *sao cho* $n \mid (a-1)^k$*. Chứng minh rằng* $n \mid a^{n-1} + a^{n-2} + ... + a + 1$.