

Số học qua các định lý và bài toán

Trần Nam Dũng
Trường ĐH KHTN Tp HCM

*Quý hồ tinh bất quý hồ đa
Thà giải sai một bài toán đúng, còn hơn giải đúng một bài toán sai.*

Với sự xuất hiện của Internet và sự bùng nổ các cuộc thi toán trên toàn thế giới, ngày nay học sinh không còn thiếu những bài toán để giải mà trái lại, học sinh sẽ có quá nhiều các đề toán các loại. Nhưng cũng chính vì có quá nhiều như vậy nên học sinh thường không đủ kiên nhẫn và hứng thú để tự mình giải các bài toán, mà động tác thường gặp nhất là tham khảo lời giải. Điều này giúp học sinh biết rất nhiều bài toán. Và điều này không phải là không có ích cho học sinh, đặc biệt là khi “trúng tử”.

Tuy nhiên, qua kinh nghiệm giảng dạy các đội tuyển những năm qua, chúng tôi nhận thấy rằng các học thông qua việc giải thật nhiều các bài toán không phải là cách tốt nhất. Bởi đơn giản là số lượng các bài toán (mới và cũ) là rất lớn, có thể nói là vô hạn, mà thời gian và trí nhớ của chúng ta là hữu hạn.

Vì vậy học những kiến thức cơ bản, những phương pháp cơ bản, những kỹ thuật tư duy cơ bản mới là điều quan trọng nhất. Có được những phân cơ bản này, ta có thể áp dụng và rèn kỹ năng giải toán thông qua một số bài toán tiêu biểu.

Và cách tốt nhất để học được các phương pháp cơ bản, những kỹ thuật tư duy là thông qua chứng minh của các định lý cơ bản. Học chứng minh định lý, ta vừa nắm được các định nghĩa, khái niệm, tính chất cơ bản, vừa học được những kỹ thuật chứng minh xuất sắc nhất được đúc kết và tinh chỉnh qua hàng thế kỷ.

Với cách nhìn nhận như vậy, chúng tôi đã thử nghiệm giảng dạy các chuyên đề Số học, Tổ hợp, Đại số ... qua các định lý và bài toán và thu được những kết quả khá khả quan. Học sinh nắm vững kiến thức nền tảng, có khả năng tư duy để xử lý vấn đề, có cách tiếp cận bài toán mới một cách bài bản.

Chuyên đề “Số học qua các định lý và bài toán” được đúc kết từ những bài giảng của chúng tôi cho các đội tuyển của các trường và các tỉnh và một số tài liệu tham khảo nằm ở cuối bài viết.

Có 103 định lý và bài toán được chọn lọc cho chuyên đề này, tập trung trong 11 chủ đề nhỏ (mỗi chủ đề 7 bài) và 2 bộ bài tập tổng hợp (mỗi bộ 13 bài). Các định lý và bài toán đều không có lời giải và chứng minh chi tiết, vì vậy khi sử dụng phải có sự chuẩn bị trước khá kỹ lưỡng. Tuy nhiên, cách trình bày của tài liệu mang tính dẫn dắt nên các giáo viên và học sinh có thể tự khai phá (đó chính là điều mà chúng tôi mong đợi nhất, và nó cũng sẽ đem lại hiệu quả cao nhất cho người đọc). Một số định lý và bài toán khó có kèm theo các hướng dẫn.

Cuối cùng, cũng cần phải nói thêm rằng ngoại trừ một số chủ đề đầu tiên, chuyên đề này là một chuyên đề tương đối khó, tùy theo đối tượng học sinh mà các thầy cô giáo có thể điều chỉnh, gia giảm cho thích hợp.

1. Số nguyên tố và hợp số

Bài toán 1. Chứng minh rằng một số nguyên $N > 1$ bất kỳ có ít nhất một ước nguyên tố.

Bài toán 2 (Định lý cơ bản của số học). Chứng minh rằng mọi số nguyên $N > 1$ đều biểu diễn được dưới dạng

$$N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_t^{\alpha_t}$$

trong đó $p_1, p_2, \dots, p_t$ là các số nguyên tố phân biệt, $\alpha_1, \alpha_2, \dots, \alpha_t$ là các số nguyên dương. Hơn nữa, biểu diễn này là duy nhất nếu không tính đến việc thay đổi thứ tự các thừa số.

Bài toán 3 (Euclid). Chứng minh tập hợp số nguyên tố là vô hạn.

Bài toán 4. Chứng minh rằng trong các số $n + 1, n + 2, n + 3, \dots, n! + 1$ có ít nhất một số nguyên tố.

Bài toán 5. Chứng minh rằng với mọi số nguyên dương n , tồn tại n số nguyên dương liên tiếp đều là hợp số.

Bài toán 6. Chứng minh rằng tồn tại vô số số nguyên tố dạng $4k + 3$.

Bài toán 7. Chứng minh rằng tổng

$$1 + \frac{1}{2} + \dots + \frac{1}{n}$$

không nguyên với mọi $n > 1$.

Hướng dẫn. Xét k sao cho $2k \leq n < 2k + 1$.

2. Phép chia có dư, thuật toán Euclid

Bài toán 8. Cho a, b là các số nguyên, $b > 1$. Chứng minh rằng tồn tại duy nhất cặp số nguyên (q, r) thỏa mãn đồng thời các điều kiện

i) $a = bq + r$;

ii) $0 \leq r < b$.

Ước số chung lớn nhất của hai số nguyên a, b là số nguyên m sao cho

i) $m|a, m|b$;

ii) Nếu $m'|a, m'|b$ thì $m' \leq m$.

Ước số chung lớn nhất của hai số a và b được ký hiệu là (a, b) .

Nếu $(a, b) = 1$ ta nói a và b nguyên tố cùng nhau.

Bài toán 9. Chứng minh rằng nếu $d|a, d|b$ thì $d|(a, b)$. Tức là mọi ước số chung của a và b đều là ước của (a, b) .

Bài toán 10. Chứng minh rằng nếu $a = bq + r$ thì $(a, b) = (b, r)$. Đặc biệt, ta có $(a, b) = (a - b, b)$.

Bài toán 11 (Định lý Bezout). Chứng minh rằng $(a, b) = 1$ khi và chỉ khi tồn tại các số nguyên x, y sao cho $ax + by = 1$.

Bài toán 12. Cho a, b là các số nguyên dương nguyên tố cùng nhau, $b > 1$. Chứng minh rằng với mọi số nguyên N , tồn tại duy nhất cặp số nguyên x, y thỏa mãn điều kiện $N = ax + by$ và $0 \leq x < b$.

Bài toán 13 (Định lý Sylvester). Cho a, b là các số nguyên dương nguyên tố cùng nhau. Chứng minh rằng $N_0 = ab - a - b$ là số nguyên lớn nhất không biểu diễn được dưới dạng $ax + by$ với x, y là các số nguyên không âm. Hơn nữa, với mọi p, q nguyên với $p + q = N_0$, có đúng một trong hai số p, q biểu diễn được dưới dạng $ax + by$ với x, y là các số nguyên không âm (mà ta sẽ gọi tắt là biểu diễn được).

Bài toán 14 (IMO 1983). Cho a, b, c là các số nguyên dương đôi một nguyên tố cùng nhau. Chứng minh rằng $2abc - ab - bc - ca$ là số nguyên lớn nhất không biểu diễn được dưới dạng $abx + bcy + caz$ với x, y, z là các số nguyên không âm.

3. Định lý Wilson, Fermat, Euler

Cho a, b, m là các số nguyên, $m > 1$. Ta viết $a \equiv b \pmod{m}$ và đọc a đồng dư b mô-đun m khi (và chỉ khi) $a - b$ chia hết cho m .

Ta nói $\{a_1, a_2, \dots, a_t\}$ là một hệ thặng dư đầy đủ mô-đun m nếu với mọi số nguyên x , tồn tại duy nhất chỉ số $i \in \{1, 2, \dots, t\}$ sao cho $x \equiv a_i \pmod{m}$.

Chú ý là nếu $\{a_1, a_2, \dots, a_t\}$ là một hệ thặng dư đầy đủ mô-đun m khi và chỉ khi $t = m$ và $a_i \not\equiv a_j \pmod{m}$ với mọi $i \neq j$ ($\neq$ ở đây hiểu là không đồng dư).

Bài toán 15. Cho p là số nguyên tố, $p > 3$. Chứng minh rằng với mọi số nguyên dương $x, 1 < x < p - 1$, tồn tại duy nhất số nguyên dương $y < p$ sao cho $xy \equiv \pm 1 \pmod{p}$, hơn nữa $y \neq x$.

Bài toán 16 (Định lý Wilson). Chứng minh rằng p là số nguyên tố khi và chỉ khi $(p - 1)! + 1$ chia hết cho p .

Bài toán 17 (Định lý Fermat). a) (Chứng minh quy nạp) Chứng minh rằng nếu p là số nguyên tố và a là số nguyên thì ta có $a^p \equiv a$ chia hết cho p .

b) (Chứng minh đồng dư) Cho p là số nguyên tố, $(a, p) = 1$. Chứng minh rằng với mọi x thuộc $E = \{1, 2, \dots, p - 1\}$ tồn tại duy nhất y thuộc E sao cho $ax \equiv y \pmod{p}$. Từ đó suy ra $ap - 1 \equiv 1 \pmod{p}$.

c) (Chứng minh tổ hợp). Đường tròn được chia thành p cung bằng nhau. Có bao nhiêu cách tô p cung bằng a màu. Hai cách tô được coi là giống nhau nếu có thể thu được

từ nhau qua một phép quay.

Với số nguyên $m > 1$, ta gọi $\lambda(m)$ là số các số nguyên dương nhỏ hơn m và nguyên tố cùng nhau với m .

Ta nói $\{a_1, a_2, \dots, a_s\}$ là một hệ thặng dư thu gọn mô-đulo m nếu với mọi số nguyên x nguyên tố cùng nhau với m , tồn tại duy nhất chỉ số $i \in \{1, 2, \dots, s\}$ sao cho $x \equiv a_i \pmod{m}$.

Chú ý là nếu $\{a_1, a_2, \dots, a_s\}$ là một hệ thặng dư thu gọn đủ mô-đulo m khi và chỉ khi $s = \varphi(m)$, $(a_i, m) = 1$ với mọi $i = 1, 2, \dots, s$ và $a_i \not\equiv a_j \pmod{m}$ với mọi $i \neq j$ ($\neq$ đầu tiên ở đây hiểu là không đồng dư).

Bài toán 18. a) Chứng minh nếu $\{a_1, a_2, \dots, a_s\}$ là một hệ thặng dư thu gọn mô-đulo m và $(a, m) = 1$ thì $\{aa_1, aa_2, \dots, aa_s\}$ là một hệ thặng dư thu gọn mô-đulo m .

b) (Định lý Euler). Chứng minh rằng nếu $(a, m) = 1$ thì $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Bài toán 19. a) Chứng minh rằng nếu p là số nguyên tố dạng $4k + 1$ thì tồn tại số nguyên dương N sao cho $N^2 + 1$ chia hết cho p .

b) Chứng minh rằng số $N^2 + 1$ không có ước nguyên tố dạng $4k + 3$.

Bài toán 20. Chứng minh các phương trình sau không có nghiệm nguyên dương

a) $4xy^2x^2y = z^2$ (Euler)

b) $x^2 - y^3 = 7$ (Lebesgue)

Bài toán 21 (Định lý Fermat-Euler về tổng hai bình phương). Chứng minh rằng nếu p là số nguyên tố dạng $4k+1$ thì tồn tại các số nguyên a, b sao cho $p = a^2 + b^2$.

Hướng dẫn. Sử dụng số N ở câu a) bài 5. Xét các số có dạng $a + Nb$ với

$$0 \leq a, b \leq \lfloor \sqrt{p} \rfloor$$

. Hãy chứng minh rằng tồn tại $(a', b') \neq (a, b)$ sao cho $a' + Nb' \equiv a + Nb \pmod{p}$.

4. Định lý Trung hoa về số dư

Bài toán 22.

a) Hãy tìm số nguyên dương N nhỏ nhất sao cho N chia 2 dư 1, chia 3 dư 2, chia 4 dư 3, chia 5 dư 4, chia 6 dư 5, chia 7 dư 6, chia 8 dư 7, chia 9 dư 8.

b)* Hãy tìm số nguyên dương N nhỏ nhất sao cho N chia 3 dư 1, chia 5 dư 2, chia 7 dư 3, chia 9 dư 4, chia 11 dư 5.

Bài toán 23. Cho $m_1, m_2, \dots, m_n$ là các số nguyên dương đôi một nguyên tố cùng nhau. Đặt $M_1 = m_2 \dots m_n$. Chứng minh rằng

$$x_1 = M_1^{\phi(m_1)}$$

là nghiệm của hệ phương trình đồng dư
$$\begin{cases} x \equiv 1 \pmod{m_1} \\ x \equiv 0 \pmod{m_2} \\ \dots \\ x \equiv 0 \pmod{m_n} \end{cases}$$

Bài toán 24 (Định lý Trung hoa về số dư). Cho $m_1, m_2, \dots, m_n$ là các số nguyên dương đôi một nguyên tố cùng nhau, $a_1, a_2, \dots, a_n$ là các số nguyên bất kỳ. Chứng minh rằng hệ phương trình đồng dư sau luôn có nghiệm

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

Hơn nữa, hai nghiệm bất kỳ của hệ khác nhau một bội số của $M = m_1 m_2 \dots m_n$.

Bài toán 25. Tìm số dư trong phép chia 192012 cho 70.

Bài toán 26. Xét đa thức $P(x) = (2x + 1)(3x + 1)$. Chứng minh rằng mọi n nguyên dương, tồn tại x nguyên để $P(x)$ chia hết cho n .

Bài toán 27. Chứng minh rằng với mọi số nguyên dương N tồn tại N số nguyên dương liên tiếp mà mỗi số đều chia hết cho bình phương của một số nguyên tố.

Bài toán 28. Cho p là số nguyên tố. Chứng minh rằng tồn tại một bội số của p sao cho 10 chữ số tận cùng của nó đôi một khác nhau.

5. Các hàm số học

Một hàm xác định trên tập hợp các số nguyên dương được gọi là một hàm số học.

Hàm số học f được gọi là nhân tính nếu với mọi cặp số nguyên m, n nguyên tố cùng nhau thì $f(mn) = f(m)f(n)$.

Người ta quan tâm đến tính nhân tính, vì nếu f nhân tính thì để tính $f(n)$ với mọi n , ta chỉ cần biết cách tính $f(p^*)$ với p là số nguyên tố.

Nếu n là số nguyên dương bất kỳ, ta gọi $\tau(n)$ là số các ước nguyên dương của n , $\sigma(n)$ là tổng các ước nguyên dương của n và $\varphi(n)$ là số các số nguyên dương $< n$ và nguyên tố cùng nhau với n .

Bài toán 29. Nếu f là một hàm nhân tính thì hàm xác định bởi công thức

$$F(n) = \sum_{d|n} f(d)$$

cũng là hàm nhân tính.

Bài toán 30. a) Chứng minh rằng các hàm $\tau(n)$ và $\sigma(n)$ là các hàm nhân tính.

b)* Chứng minh rằng hàm $\varphi(n)$ là hàm nhân tính.

c) Chứng minh rằng

$$\tau(p^\alpha) = \alpha + 1, \sigma(p^\alpha) = 1 + p + \dots + p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}, \phi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

Số nguyên dương n được gọi là số hoàn hảo nếu tổng các ước dương của n gấp hai lần số đó: $\sigma(n) = 2n$.

Bài toán 31 (Định lý Euclid - Euler). Chứng minh rằng số chẵn n là số hoàn hảo khi và chỉ khi $n = 2^m - 1(2^m - 1)$, trong đó m là số nguyên dương sao cho $2^m - 1$ là số nguyên tố.

Bài toán 32. Chứng minh rằng với mọi số nguyên dương n ta có

a)

$$\sum_{k=1}^n \tau(k) = \sum_{k=1}^n \left[\frac{n}{k} \right]$$

;

b)

$$\sum_{k=1}^n \sigma(k) = \sum_{k=1}^n k \left[\frac{n}{k} \right]$$

Hàm Mobius $\mu(n)$ là hàm số được xác định như sau: Nếu n chia hết cho bình phương một số nguyên tố thì $\mu(n) = 0$. Nếu $n = p_1 \cdot p_2 \dots p_k$ thì $\mu(n) = (-1)^k$. Ta cũng quy ước một cách tự nhiên rằng $\mu(1) = 1$.

Bài toán 33. a) Chứng minh rằng hàm $\mu(n)$ là hàm nhân tính.

b) Chứng minh rằng với mọi $n > 1$ ta có

$$\sum_{d|n} \mu(d) = 0.$$

Bài toán 34 (Công thức nghịch đảo Mobius). Xét hàm số học f và xét

$$F(n) = \sum_{d|n} f(d)$$

Ta có công thức

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

Bài toán 35. a) Chứng minh rằng với mọi số nguyên dương n ta có bất đẳng thức

$$\tau(n) \leq 2\sqrt{n}$$

b) Tìm tất cả các số nguyên dương k sao cho tồn tại số nguyên dương n thỏa mãn điều kiện

$$\frac{\tau(n^2)}{\tau(n)} = k.$$

6. Bậc theo mô-đulo

Cho m là số nguyên dương > 1 , a là số nguyên sao cho $(a, m) = 1$. Theo định lý Euler thì $a^{\varphi(m)} \equiv 1 \pmod{m}$. Như vậy tập hợp các số nguyên dương k sao cho $a^k \equiv 1 \pmod{m}$ là khác rỗng. Gọi h là số nguyên dương nhỏ nhất thỏa mãn điều kiện $a^h \equiv 1 \pmod{m}$. Ta gọi h là bậc của a mô-đulo m và ký hiệu là $h = \text{ord}_m(a)$.

Bài toán 36. Cho $(a, n) = 1$ và h là số nguyên dương nhỏ nhất sao cho $ah \equiv 1 \pmod{n}$. Khi đó với mọi số nguyên dương m sao cho $a^m \equiv 1 \pmod{n}$ ta có m chia hết cho h .

Bài toán 37. Chứng minh rằng mọi ước số nguyên tố của số

$$F_n = 2^{2^n} + 1$$

có số dư bằng 1 khi chia cho $2n + 1$.

Bài toán 38. Chứng minh rằng không tồn tại số lẻ $n > 1$ sao cho $3n + 1$ chia hết cho n .

Hướng dẫn. Chứng minh bằng phản chứng. Xét p là ước số nguyên tố nhỏ nhất của n .

Bài toán 39. Cho p là số nguyên tố lẻ và q và r_a là các số nguyên tố sao cho p chia hết $qr + 1$. Chứng minh rằng hoặc $2r \mid p - 1$ hoặc $p \mid q^2 - 1$.

Bài toán 40. [AIME 2001] Có bao nhiêu bội số nguyên dương của số 1001 có thể viết dưới dạng $10j - 10i$, trong đó i và j là các số nguyên và $0 \leq i < j \leq 99$.

Bài toán 41 (VMO 2001). Cho số nguyên dương n và cho hai số nguyên nguyên tố cùng nhau a, b lớn hơn 1. Giả sử p, q là hai ước lẻ lớn hơn 1 của

$$a^{6^n} + b^{6^n}$$

. Hãy tìm số dư trong phép chia

$$p^{6^n} + q^{6^n}$$

cho $6 \cdot (12)^n$.

Bài toán 42. Cho $n > 1, a > 0$ là các số nguyên và p là số nguyên tố sao cho $a^p \equiv 1 \pmod{p^n}$. Chứng minh rằng $a \equiv 1 \pmod{p^{n-1}}$.

7. Công thức Legendre về lũy thừa của p trong $n!$

Với mỗi số thực x , ta gọi $[x]$ là số nguyên lớn nhất không vượt quá x (đọc là phần nguyên x). Hàm phần nguyên có những ứng dụng quan trọng trong số học. Một trong những tính chất cơ bản thường dùng, đó là: Cho k là một số nguyên bất kỳ, khi đó trong n số nguyên dương đầu tiên, có đúng $[n/k]$ số chia hết cho k .

Bài toán 43 (Công thức Legendre). Cho n là số nguyên dương > 1 và p là số nguyên tố. Khi đó số mũ của p trong phân tích tiêu chuẩn của $n!$ ra thừa số nguyên tố được tính theo công thức

$$\alpha_p(n!) = \left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \left[\frac{n}{p^3} \right] + \dots$$

Bài toán 44. Chứng minh các tính chất sau của hàm phần nguyên

- a) $[x + y] \geq [x] + [y]$ với mọi x, y thuộc $\mathbb{R}$.
- b) $[x] + [x + 1/2] = [2x]$,
- c) $[x] + [x + 1/3] + [x + 2/3] = [3x]$,
- d) $\left[\left[\frac{x}{m} \right] \frac{1}{n} \right] = \left[\frac{x}{mn} \right]$ với mọi x thực và m, n nguyên dương.

Bài toán 45. Chứng minh rằng tích của n số nguyên liên tiếp luôn chia hết cho $n!$

Bài toán 46 (APMO 2001). Tìm số nguyên N lớn nhất sao cho số các số thuộc tập hợp $1, 2, \dots, N$ và chia hết cho 3 bằng số các số thuộc tập đó và chia hết cho 5 hoặc 7.

Bài toán 47. Tìm tất cả các số nguyên dương n sao cho $(n-1)!$ không chia hết cho n^2 .

Bài toán 48. Chứng minh rằng với mọi số nguyên dương $n \geq 3$, tích $(2n-1)(2n-2)(2n-4) \dots (2n-2n+1)$ chia hết cho $n!$.

Bài toán 49. Chứng minh rằng C_n^k là số lẻ với mọi $k = 0, 1, 2, \dots, n$ khi và chỉ khi n có dạng $2^m - 1$.

8. Định lý Lagrange, định lý Wolstenhome, định lý Lucas

Bài toán 50. Cho p là số nguyên tố lẻ đặt $f(x) = (x+1) \dots (x+p-1)$.

- a) Chứng minh rằng $pf(x) = (x+1)f(x+1) - xf(x)$.
- b) Giả sử $f(x) = x^{p-1} + a_1x^{p-2} + \dots + a_{p-2}x + a_{p-1}$. Từ đẳng thức trên, hãy suy ra rằng

$$pa_i = \sum_{j=0}^i C_{p-j}^{j+1} a_j$$

(ở đây $a_0 = 1$)

- c) (Định lý Lagrange) Chứng minh rằng a_i chia hết cho p với mọi $i = 1, 2, \dots, p-2$.

Bài toán 51 (Định lý Wolstenhome). a) Nếu $p > 3$ là số nguyên tố, thì mẫu số của phân số

$$1 + \frac{1}{2} + \dots + \frac{1}{p-1}$$

chia hết cho p^2 .

- b) Chứng minh rằng nếu $p > 3$ là số nguyên tố, thì

$$C_{2p-1}^{p-1} \equiv 1 \pmod{p^3}$$

Bài toán 52 (Định lý Lucas). Cho p là số nguyên tố

- a) Chứng minh rằng nếu m là số nguyên không âm thì ta có

$$(1+x)^{p^m} \equiv 1 + x^{p^m} \pmod{p}$$

b) Cho $0 < m \leq n$ là các số nguyên dương. Giả sử m, n có biểu diễn trong hệ đếm cơ số p là $m = m_k m_{k-1} \dots m_1 m_0 = m_k p^k + m_{k-1} p^{k-1} + \dots + m_1 p + m_0$ $n = n_k n_{k-1} \dots n_1 n_0 = n_k p^k + n_{k-1} p^{k-1} + \dots + n_1 p + n_0$.

Chứng minh rằng

$$C_n^m \equiv C_{n_k}^{m_k} \cdot C_{n_{k-1}}^{m_{k-1}} \dots C_{n_0}^{m_0} \pmod{n}$$

Hướng dẫn. Sử dụng đẳng thức

$$(1+x)^n = \sum_{m=0}^n C_n^m x^m \equiv \prod_{i=0}^k (1+x^{p^i})^{n_i} \pmod{p}$$

Và chú ý về tính duy nhất của khai triển p -phân.

Bài toán 53. Chứng minh sự tương đương của các mệnh đề sau

1)

$$C_{2p-1}^{p-1} \equiv 1 \pmod{p^4}$$

2)

$$\frac{1}{1} + \frac{1}{2} + \dots + \frac{1}{p-1} \equiv 0 \pmod{p^3}$$

3)

$$\frac{1}{1^2} + \frac{1}{2^2} + \dots + \frac{1}{(p-1)^2} \equiv 0 \pmod{p^2}$$

Bài toán 54. a) Chứng minh rằng với mọi số nguyên tố p và số nguyên dương n, k ta có

$$C_{pk}^{pn} - C_k^n \cdot p^2$$

b) Chứng minh rằng với mọi số nguyên tố $p \geq 5$ và số nguyên dương n, k ta có

$$C_{pk}^{pn} - C_k^n \cdot p^3$$

Bài toán 55. Chứng minh rằng với $n > 1$

$$C_{2^{n+1}}^{2^n} - C_{2^n}^{2^{n-1}}$$

chia hết cho 2^{2n+2} .

Bài toán 56 (Vietnam TST 2010). Gọi S_n là tổng bình phương các hệ số sau khai triển của $(1+x)^n$. Chứng minh rằng $1 + S_{2n}$ không chia hết cho 3.

9. Phương trình Pell

Bài toán 57. a) Chứng minh hằng đẳng thức $(a^2 + db^2)(x^2 + dy^2) = (ax + dby)^2 + d(ay - bx)^2 = (ax - dby)^2 + d(ay + bx)^2$.

b) Chứng minh rằng nếu phương trình $x^2 \circ dy^2 = 1$ có ít nhất một nghiệm nguyên dương thì nó có vô số nghiệm nguyên dương.

Bài toán 58 (Định lý về cấu trúc nghiệm của phương trình Pell loại 1). Cho d là số nguyên dương không chính phương. Xét phương trình $x^2 \circ dy^2 = 1$ (1). Giả sử (a, b) là nghiệm nguyên dương nhỏ nhất của (1) ($(x, y) < (x', y') \Leftrightarrow x < x'$ hoặc $x = x', y < y'$, ta gọi nghiệm này là nghiệm cơ sở).

Xét hai dãy số $\{x_n\}, \{y_n\}$ xác định bởi $x_1 = a, y_1 = b, x_{n+1} = ax_n + dby_n, y_{n+1} = bx_n + ay_n$.

a) Chứng minh rằng với mọi n nguyên dương thì (x_n, y_n) là nghiệm của (1).

b) Chứng minh rằng nếu (x, y) là nghiệm nguyên dương của (1) và $x > a$ thì $x' = ax \circ dby, y' = bx \circ ay$ cũng là nghiệm nguyên dương của (1).

c) Chứng minh rằng nếu (x, y) là nghiệm của (1) thì tồn tại n sao cho $x = x_n, y = y_n$.

Cho d là số nguyên dương không chính phương. Xét phương trình dạng Pell $x^2 \circ dy^2 = k$ với k là số nguyên khác 0.

Đặt $S = \{(x, y) \in \mathbb{N}^* | x^2 \circ dy^2 = k\}$ (2) và gọi (a, b) là nghiệm cơ sở của phương trình Pell tương ứng $x^2 \circ dy^2 = 1$.

Nghiệm (x_0, y_0) thuộc S được gọi là nghiệm cơ sở của (2) nếu không tồn tại $(x', y') \in S$ sao cho

$$\begin{cases} x = ax' + Dby' \\ y = ay' + bx' \end{cases}$$

Gọi S_0 là tập hợp tất cả các nghiệm cơ sở.

Bài toán 59 (Định lý về cấu trúc nghiệm của phương trình dạng Pell). a) Tập hợp các nghiệm cơ sở là hữu hạn và có thể tìm được bằng phương pháp vét cạn.

b) Nếu $S \neq \emptyset$ và (x, y) là một nghiệm của (2) thì tồn tại (x_0, y_0) thuộc S_0 và n thuộc $\mathbb{N}$ sao cho

$$x + \sqrt{d}y = (a + \sqrt{d}b)^n (x_0 + \sqrt{d}y_0)$$

Bài toán 60 (Việt Nam 1999). Cho hai dãy số $(x_n), (y_n)$ xác định như sau

$$x_1 = 1, x_2 = 4, x_{n+2} = 3x_{n+1} - x_n \text{ với mọi } n \geq 1,$$

$$y_1 = 1, y_2 = 2, y_{n+2} = 3y_{n+1} - y_n \text{ với mọi } n \geq 1.$$

Chứng minh rằng các số nguyên dương a, b thỏa mãn phương trình $a^2 - 5b^2 = -4$ khi và chỉ khi tồn tại số nguyên dương k sao cho $a = x_k, b = y_k$.

Bài toán 61 (Việt Nam TST 2002). Tìm tất cả các đa thức $p(x)$ với hệ số nguyên sao cho đa thức

$$q(x) = (x^2 + 6x + 10)(p(x))^2 \circ 1$$

là bình phương của một đa thức với hệ số nguyên.

Bài toán 62 (PTNK 2003). Tìm tất cả các số nguyên dương k sao cho phương trình $x^2 - (k^2 - 4)y^2 = -24$ có nghiệm nguyên dương.

Bài toán 63. a) (Định lý về cấu trúc nghiệm của phương trình dạng $Ax^2 \sim By^2 = 1$). Cho phương trình $Ax^2 \sim By^2 = 1$ (*) với A và AB không chính phương. Gọi (a, b) là nghiệm nhỏ nhất của phương trình Pell kết hợp $x^2 \sim AB y^2 = 1$. Giả sử phương trình (*) có nghiệm và $(x_0; y_0)$ là nghiệm nhỏ nhất của nó thì $(x_0; y_0)$ là nghiệm duy nhất của hệ phương trình $a = Ax^2 + By^2, b = 2xy$.

b) (Áp dụng, Vietnam TST 2009). Cho a, b là các số nguyên dương không chính phương sao cho a.b cũng không chính phương. Chứng minh rằng ít nhất một trong hai phương trình $ax^2 \sim by^2 = 1$ và $ax^2 \sim by^2 = \sim 1$ không có nghiệm nguyên dương.

10. Phương trình Markov và phương pháp bước nhảy Vi-ét.

Bài toán 64. Cho k là số nguyên dương. Xét phương trình nghiệm nguyên dương

$$x^2 + y^2 + z^2 = kxyz. \quad (1)$$

a) Chứng minh rằng nếu (x, y, z) là nghiệm nguyên dương của (1), thì (x, y, kxy - z) cũng là nghiệm nguyên dương của (1).

b) Chứng minh rằng nếu (x_0, y_0, z_0) là nghiệm của (1) sao cho $x_0 \leq y_0 \leq z_0$ và $x_0 + y_0 + z_0$ nhỏ nhất thì ta có $z_0/x_0 y_0 \leq k/2$.

c) Chứng minh rằng phương trình (1) có nghiệm nguyên dương khi và chỉ khi k = 1 hoặc k = 3.

Bài toán 65. Xét phương trình

$$x_1^2 + x_2^2 + \dots + x_n^2 = kx_1 x_2 \dots x_n. \quad (2)$$

Ta sẽ nói nghiệm $(x_1, x_2, \dots, x_n)$ của (2) là nghiệm cơ sở nếu $x_1 \leq x_2 \leq \dots \leq x_n$ và $x_1^2 + \dots + x_{n-1}^2 \geq x_n^2 \Leftrightarrow 2x_n \leq kx_1 \dots x_{n-1}$.

a) Chứng minh rằng nếu (2) có nghiệm thì (2) có nghiệm cơ sở.

b) Chứng minh rằng nếu $n > 2$, và $(x_1, x_2, \dots, x_n)$ là nghiệm cơ sở của (2) thì $x_1 \dots x_{n-2} \leq 2(n-1)/k$.

c) Chứng minh rằng nếu $x_1 \leq x_2 \leq \dots \leq x_n$ là các số nguyên dương bất kỳ thỏa mãn điều kiện $1 < x_n^2 \leq x_1^2 + \dots + x_{n-1}^2$, thì tỷ số $R = (x_1^2 + \dots + x_n^2)/x_1 x_2 \dots x_n$ không vượt quá $(n+3)/2$.

d) (Định lý về phương trình Markov). Nếu phương trình (2) có nghiệm và $n \neq k$, thì $n \geq 2k \sim 3$ khi $n \geq 5$ và $n > 4k \sim 6$ khi $n = 3, n = 4$.

Bài toán 66 (Việt Nam 2002). Tìm tất cả các số nguyên dương n sao cho phương trình

$$x + y + z + t = n\sqrt{xyzt}$$

có nghiệm nguyên dương.

Bài toán 67. a) Tìm tất cả các số nguyên dương k sao cho phương trình $x^2 + y^2 + 1 = kxy$ có nghiệm nguyên dương.

b) Tìm tất cả các nghiệm nguyên dương của phương trình $x^2 + y^2 + 1 = 3xy$.

Hướng dẫn. Xét dãy số (x_n) được xác định như sau: $x_1 = x_2 = 1$, $x_{n+1} = 3x_n - x_{n-1}$ với mọi $n \geq 2$. Hãy chứng minh rằng nếu x, y là các số nguyên dương với $x \leq y$ sao cho $x^2 + y^2 + 1 = 3xy$ thì tồn tại số tự nhiên n sao cho $x = x_n, y = x_{n+1}$.

Bài toán 68 (CRUX, Problem 1420). Nếu a, b, c là các số nguyên dương sao cho $0 < a^2 + b^2 \leq abc \leq c$. Chứng minh rằng $a^2 + b^2 \leq abc$ là số chính phương.

Bài toán 69 (IMO 88). Nếu $a, b, q = (a^2 + b^2)/(ab + 1)$ là các số nguyên dương thì q là số chính phương.

Bài toán 70 (Việt Nam 2012). Xét các số tự nhiên lẻ a, b mà a là ước số của $b^2 + 2$ và b là ước số của $a^2 + 2$. Chứng minh rằng a và b là các số hạng của dãy số tự nhiên (v_n) xác định bởi $v_1 = v_2 = 1$ và $v_n = 4v_{n-1}v_{n-2}$ với mọi $n \geq 2$.

11. Số chính phương mod p

Giả sử p là một số nguyên tố lẻ. Khi đó số nguyên a được gọi là số chính phương modulo p nếu $(a, p) = 1$ và đồng dư $x^2 \equiv a \pmod{p}$ có nghiệm.

Bài toán 71. Chứng minh các mệnh đề sau

a) Giả sử p là một số nguyên tố lẻ, a là số nguyên không chia hết cho p . Khi đó đồng dư $x^2 \equiv a \pmod{p}$ hoặc không có nghiệm, hoặc có đúng hai nghiệm không đồng dư modulo p .

b) Nếu p là một số nguyên tố lẻ thì trong các số $1, 2, \dots, p-1$ có đúng $\frac{p-1}{2}$ số chính phương modulo p .

Giả sử p là một số nguyên tố lẻ, a là số nguyên không chia hết cho p . Kí hiệu Legendre $\left(\frac{a}{p}\right)$ được định nghĩa như sau: $\left(\frac{a}{p}\right) = 1$ nếu a là số chính phương modulo p và $\left(\frac{a}{p}\right) = -1$ trong trường hợp ngược lại.

Bài toán 72. Giả sử p là một số nguyên tố lẻ, a, b là các số nguyên không chia hết cho p . Chứng minh các tính chất sau

a) (Tiêu chuẩn Euler).

$$\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

b) Nếu $a \neq b$ thì

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

c)

$$\left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

d)

$$\left(\frac{a^2}{p}\right) = 1.$$

Bài toán 73 (Bổ đề Gauss). Giả sử p là một số nguyên tố lẻ, a là số nguyên không chia hết cho p . Nếu trong các thặng dư dương bé nhất của các số nguyên $a, 2a, \dots, (p-1)a/2$ có s thặng dư lớn hơn $p/2$ thì

$$\left(\frac{a}{p}\right) = (-1)^s.$$

Hướng dẫn. Trong các thặng dư dương bé nhất nói trên, giả sử $u_1, u_2, \dots, u_s$ là các thặng dư lớn hơn $p/2$, $v_1, v_2, \dots, v_t$ là các thặng dư bé hơn $p/2$. Hãy chứng tỏ rằng $\{p - u_1, p - u_2, \dots, p - u_s, v_1, v_2, \dots, v_t\} = \{1, 2, \dots, (p-1)/2\}$.

Bài toán 74. Giả sử p là số nguyên tố lẻ, a là số lẻ không chia hết cho p . Chứng minh rằng

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)}$$

, trong đó

$$T(a, p) = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p} \right]$$

Bài toán 75 (Luật thuận nghịch bình phương). Giả sử p và q là những số nguyên tố lẻ khác nhau. Khi đó ta có

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

Bài toán 76. Chứng minh rằng 2 chính phương modulo p khi và chỉ khi $p \equiv \pm 1 \pmod{8}$.

Bài toán 77 (Euler). Chứng minh rằng phương trình $4xyz \sim x \sim y \sim t^2 = 0$ không có nghiệm nguyên dương.

12. Bài tập tổng hợp 1

Bài toán 78 (Đại học Vinh 2009). Giả sử m, n là hai số nguyên dương thỏa mãn n/d là số lẻ với $d = (m, n)$: Xác định $(a^m + 1, a^n - 1)$ với a là số nguyên dương lớn hơn 1.

Bài toán 79 (Đại học sư phạm HN 2009). Cho các số nguyên dương a, b, c, d thỏa mãn $ac + bd$ chia hết cho $a^2 + b^2$. Chứng minh rằng $(c^2 + d^2, a^2 + b^2) > 1$.

Bài toán 80. Gọi $S(n)$ là tổng các chữ số của số nguyên dương n . Chứng minh rằng ta có công thức

$$S(n) = n - 9 \left(\left[\frac{n}{10} \right] + \left[\frac{n}{100} \right] + \left[\frac{n}{1000} \right] + \dots \right)$$

Bài toán 81 (PTNK 2008). Với mỗi số nguyên dương n , gọi $S(n)$ là tổng các chữ số của n .

a) Chứng minh rằng các số $n = 999$ và $n = 2999$ không thể biểu diễn được dưới dạng $a + b$ với $S(a) = S(b)$.

b) Chứng minh rằng mọi số n , $999 < n < 2999$ đều biểu diễn được dưới dạng $a + b$ với $S(a) = S(b)$.

Bài toán 82 (PTNK 2009). a) Chứng minh tồn tại số n chẵn, $n > 2008$ sao cho $2009.n - 49$ là số chính phương.

b) Chứng minh không tồn tại số nguyên m sao cho $2009.m - 147$ là số chính phương.

Bài toán 83. Tìm tất cả các đa thức $f(x)$ với hệ số nguyên sao cho với mọi n nguyên dương ta có $f(n)$ là ước của $2n - 1$.

Hướng dẫn. Nếu f không phải là đa thức hằng thì tồn tại số nguyên dương n sao cho $|f(n)| > 1$. Nếu p là ước nguyên tố của $f(n)$ thì $p \mid f(n+p)$.

Bài toán 84. Cho a, b là các số nguyên dương sao cho

$$\frac{a+1}{b} + \frac{b+1}{a}$$

là số nguyên. Chứng minh rằng

$$(a, b) \leq \sqrt{a+b}.$$

Bài toán 85. Chứng minh rằng nếu a, b, c là các số nguyên và

$$\frac{a}{b} + \frac{b}{c} + \frac{c}{a} = 3$$

thì abc là lập phương của một số nguyên.

Hướng dẫn. Hãy chứng minh với mọi p nguyên tố thì $vp(abc)$ chia hết cho 3.

Bài toán 86. Các số nguyên dương a, b, c, d thỏa mãn điều kiện

$$a^2 + b^2 + a^b = c^2 + d^2 + cd.$$

Chứng minh rằng số $a + b + c + d$ là hợp số.

Bài toán 87 (Hưng Yên 2012). Cho p là số nguyên tố, a là số tự nhiên; p^α là ước đúng của số nguyên dương a nếu p^α chia hết a và $p^\alpha + 1$ không chia hết a , khi đó ta viết $p^\alpha \parallel a$.

Gọi a, n là các số nguyên dương, p là số nguyên tố lẻ. Giả sử $p^\alpha \parallel a - 1$ và $p^\alpha \parallel n$, trong đó $\alpha \geq 1; \beta \geq 0$. Chứng minh rằng $p^{\alpha-\beta} \parallel a^n - 1$.

Chú ý: Kết quả bài toán này tương đương với dạng 1 của Bổ đề nâng (Lifting The Exponent Lemma - LTE) sau đây:

Gọi $v_p(n)$ là số mũ của p trong khai triển ra thừa số nguyên tố của n . Cho p là số nguyên tố lẻ, x, y là các số nguyên sao cho x, y không chia hết cho p nhưng $x - y$ chia hết cho p , n là số nguyên dương. Khi đó $v_p(x^n - y^n) = v_p(x - y) + v_p(n)$.

Phương pháp chứng minh là sử dụng quy nạp toán học theo $v_p(n)$.

Ta có dạng 2 của LTE là: Cho p là số nguyên tố lẻ, x, y là các số nguyên sao cho x, y không chia hết cho p nhưng $x + y$ chia hết cho p , n là số nguyên dương lẻ. Khi đó $v_p(x^n + y^n) = v_p(x + y) + v_p(n)$.

Bài toán 88. Cho $p > 3$ là số nguyên tố. Giả sử a, b là các số nguyên sao cho $p \mid a + b$ và $p^2 \nmid a^3 + b^3$. Hãy chứng minh rằng hoặc $p^2 \mid a + b$, hoặc $p^3 \mid a^3 + b^3$.

Bài toán 89 (Ninh Bình 2009). Cho hai số nguyên dương p, q lớn hơn 1; nguyên tố cùng nhau. Chứng minh rằng tồn tại số nguyên k sao cho $(pq+1)n^k + 1$ là hợp số với mọi số nguyên dương n .

Hướng dẫn. Sử dụng định lý Trung hoa về số dư.

Bài toán 90 (Đại học KHTN 2009). Tìm tất cả các bộ bốn số tự nhiên a, b, c, d đôi một phân biệt thỏa mãn

$$a^2 \vee b^2 = b^2 \vee c^2 = c^2 \vee d^2.$$

Hướng dẫn. Dùng phương pháp xuống thang để chứng minh không tồn tại một bộ số như vậy. Tham khảo lời giải chi tiết ở [3].

13. Bài tập tổng hợp 2

Bài toán 91 (Việt Nam 2003, bảng B). Hỏi có tồn tại hay không các số nguyên x, y, u, v, t thỏa mãn điều kiện sau

$$x^2 + y^2 = (x + 1)^2 + u^2 = (x + 2)^2 + v^2 = (x + 3)^2 + t^2.$$

Bài toán 92 (Định lý Beatty). Chứng minh rằng nếu α, β là các số vô tỷ dương sao cho

$$\frac{1}{\alpha} + \frac{1}{\beta} = 1$$

thì các dãy số

$$([n\alpha]) = ([\alpha], [2\alpha], [3\alpha], \dots)$$

$$([n\beta]) = ([\beta], [2\beta], [3\beta], \dots)$$

lập thành một phân hoạch của tập hợp các số tự nhiên. Nói cách khác mỗi một số nguyên dương xuất hiện trong hợp của hai dãy số trên đúng một lần và hai dãy số không có số hạng chung.

Bài toán 93. Cho $n \geq 2$ là số nguyên dương. Chứng minh rằng

$$\sum_{k=2}^n \left[\frac{n^2}{k} \right] = \sum_{k=n+1}^{n^2} \left[\frac{n^2}{k} \right]$$

trong đó $[x]$ ký hiệu số nguyên lớn nhất không vượt quá x .

Bài toán 94 (Rio Plate 2002). Tìm tất cả các cặp số nguyên dương (a, b) sao cho

$$\frac{a^2b + b}{ab^2 + 9}$$

là một số nguyên.

Bài toán 95 (IMO 2003). Tìm tất cả các cặp số nguyên dương (a, b) sao cho số

$$\frac{a^2}{2ab^2 - b^3 + 1}$$

là số nguyên.

Bài toán 96 (IMO 2007). Cho a, b là các số nguyên dương sao cho $4ab - 1$ chia hết $(4a^2 - 1)^2$. Chứng minh rằng $a = b$.

Bài toán 97. Tìm tất cả các số nguyên dương n sao cho tồn tại số nguyên m sao cho $2n - 1$ là ước của $m^2 + 9$.

Bài toán 98. Tìm tất cả các số nguyên dương n sao cho tồn tại các số nguyên lẻ $x_1, x_2, \dots, x_n$ thỏa mãn điều kiện $x_1^2 + x_2^2 + \dots + x_n^2 = n^4$.

Hướng dẫn. Trước hết hãy tìm điều kiện cần bằng cách xét theo mô-đun 8. Sau đó tìm điều kiện đủ bằng cách xây dựng nghiệm.

Bài toán 99. Biết rằng tổng các chữ số của số nguyên dương N bằng 100, còn tổng các chữ số của $5N$ bằng 50. Chứng minh rằng N chẵn.

Hướng dẫn. Đặt $M = 5N$ thì $S(M) = 50$ và $S(2M) = S(10N) = S(N) = 100$. Suy ra phép cộng $M + M = 2M$ là phép cộng không nhớ.

Bài toán 100 (VMO 2004). Với mỗi số nguyên dương n , ký hiệu $S(n)$ là tổng tất cả các chữ số trong biểu diễn thập phân của n .

Xét các số nguyên dương m là bội của 2003. Hãy tìm giá trị nhỏ nhất của $S(m)$.

Hướng dẫn. Hãy chứng minh rằng không tồn tại n sao cho $10n + 1$ chia hết cho 2003 và tồn tại n sao cho $10n + 2$ chia hết cho 2003. Có thể sử dụng bậc của 10 theo modulo 2003.

Bài toán 101. Cho p là số nguyên tố và a, b, c là các số nguyên bất kỳ. Chứng minh rằng tồn tại các số nguyên x, y, z không đồng thời chia hết cho p sao cho $ax^2 + by^2 + cz^2$ chia hết cho p .

Hướng dẫn. Hãy chứng minh cho trường hợp $a = b = c = 1$. Một hướng tiếp cận khác là chứng minh phản chứng và sử dụng tính chất nếu $ax^2 + by^2 + cz^2$ không chia hết cho p thì $(ax^2 + by^2 + cz^2)^{p-1} \equiv 1 \pmod{p}$.

Bài toán 102. Gọi p_n là số nguyên tố thứ n . Đặt

$$S_n = \sum_{k=1}^n \frac{1}{p_k}$$

. Chứng minh rằng $\lim S_n = \infty$.

Hướng dẫn. Hãy chú ý rằng

$$\left(1 + \frac{1}{2} + \frac{1}{4} + \dots\right) \left(1 + \frac{1}{3} + \frac{1}{9} + \dots\right) \dots \left(1 + \frac{1}{p_n} + \frac{1}{p_n^2} + \dots\right) > 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p_n}.$$

Bài toán 103. Với số nguyên dương $n > 1$, gọi $A(n)$ là mệnh đề: “Từ $2n - 1$ số nguyên bất kỳ, luôn chọn được n số có tổng chia hết cho n ”.

- Chứng minh $A(3)$ đúng;
- Chứng minh $A(5)$ đúng;
- Chứng minh rằng nếu $A(m)$ đúng và $A(n)$ đúng thì $A(mn)$ cũng đúng.
- * Chứng minh rằng nếu p là số nguyên tố thì $A(p)$ đúng.

Hướng dẫn. Chứng minh phản chứng và để ý rằng nếu $(a_1 + a_2 + \dots + a_p)$ không chia hết cho p thì $(a_1 + a_2 + \dots + a_p)^{p-1} \equiv 1 \pmod{p}$

- (Định lý Erdos-Ginzburg-Ziv). Chứng minh $A(n)$ đúng với mọi $n > 1$.

Tài liệu tham khảo

- [1]. Đoàn Quỳnh, Trần Nam Dũng, Hà Huy Khoái, Đặng Hùng Thắng, Nguyễn Trọng Tuấn, Tài liệu chuyên toán Giải tích 12, NXB GD Việt Nam, 2012.
- [2]. Nguyễn Văn Mậu, Trần Nam Dũng, Đặng Hùng Thắng, Đặng Huy Ruận, Một số vấn đề số học chọn lọc, NXB GD, 2008.
- [3]. Trần Nam Dũng (chủ biên), Lời giải và bình luận đề thi các trường và các tỉnh năm học 2009-2010, Ebook, 2010.
- [4]. Tủ sách Toán học và Tuổi trẻ, Các bài thi Olympic Toán Trung học phổ thông Việt Nam (1990-2006), NXB GD 2007.
- [5]. Victor Shoup, A Computational Introduction to Number Theory and Algebra, Ebook.
- [6]. D.O. Shklyarsky, N.N. Chentsov, I.M. Iaglom, Selected Problems and Theorems in Elementary Mathematics, Mir Publishers Moscow 1979.
- [7] Amir Hossein Parvardi, Lifting The Exponent Lemma, ArtofProblemSolving.com