Các bài toán Lý thuyết Số
từ các kỳ thi Olympic Quốc gia và Quốc tế 2015-2024

Ban biên soạn

Tạp chí Pi
Hội toán học Việt Nam

Ngày 28 tháng 3 năm 2025

Mục lục

Mở đầu

Lời nói đầu

Cuốn sách này được biên soạn dành cho giáo viên và học sinh luyện thi Đội tuyển Quốc gia Việt Nam dự thi IMO. Tài liệu tập hợp *các bài toán mới trong vòng 10 năm trở lại đây* từ các kỳ thi quan trọng như IMO Shortlist, các cuộc thi quốc tế uy tín như MEMO, BMO, APMO, EGMO, cũng như các kỳ thi quốc gia của 20 nước hàng đầu thế giới.

Mỗi bài toán được *xếp hạng theo thang độ khó MOHS*, đi kèm với *danh sách các định lý, bổ đề, hằng đẳng thức quan trọng* cần thiết cho lời giải. Các yếu tố này được liên kết trong một hệ thống đồ thị tri thức, giúp người đọc dễ dàng tra cứu và hiểu rõ mối liên hệ giữa các công cụ toán học. Ngoài ra, mỗi bài toán còn được gắn *thẻ thông tin chi tiết* về kỳ thi (năm, vòng), giúp thuận tiện cho việc tìm kiếm và tham khảo.

Để hỗ trợ người học, mỗi bài toán có một *mã định danh duy nhất* (UUID), kèm theo *gợi ý* khi gặp khó khăn. Nếu có nhiều cách giải, tất cả sẽ được trình bày các chuyên đề liên quan đến cách giải để giúp người đọc mở rộng tư duy.

Cấu trúc sách gồm bốn phần chính tương ứng với bốn lĩnh vực quan trọng của toán học thi đấu: Đại số, Tổ hợp, Hình học và Số học. Mỗi phần chia thành các chương theo từng chuyên đề cụ thể với các bài toán liên quan.

Đây là một cuốn sách *mở, luôn được cập nhật và có sẵn trên Internet* để bất kỳ ai cũng có thể truy cập. Người dùng có thể đóng góp bằng cách đề xuất bài toán mới hoặc thay đổi mức độ khó, gợi ý, hoặc thêm lời giải mới cho bài toán bằng cách gửi *một tệp duy nhất theo định dạng LaTeX quy định*. Việc đóng góp tập trung vào nội dung mà không cần lo lắng về định dạng, tổ chức, mã LaTeX hay quy trình xuất bản.

Toàn bộ quá trình này được giám sát bởi các nhân sự được ủy quyền từ Hội Toán Học Việt Nam và Tạp chí Pi, nhằm đảm bảo chất lượng và tính nhất quán của tài liệu.

Chúng tôi hy vọng tài liệu này sẽ trở thành một nguồn tham khảo hữu ích, giúp giáo viên và học sinh tiến xa hơn trong hành trình chinh phục các kỳ thi toán quốc tế.

Ban Biên soạn

Phần I

Các bài toán

Chương 1

Lý thuyết số

1.1 2014

1.1.1. Cho a là một số tự nhiên lẻ không phải là một số chính phương, và $m, n \in \mathbb{N}$. Khi đó:

- $\{m(a+\sqrt{a})\} \neq \{n(a-\sqrt{a})\}$
- $[m(a+\sqrt{a})] \neq [n(a-\sqrt{a})]$

Trong đó, $\{\cdot\}$ ký hiệu phần thập phân (phần lẻ), và $[\cdot]$ ký hiệu phần nguyên.

1.1.2. Cho n là một số tự nhiên. Tính giá trị của biểu thức

$$\sum_{k=1}^{n^2} \# \left\{ d \in \mathbb{N} \,\middle|\, 1 \le d \le k \le d^2 \le n^2,\ k \equiv 0 \pmod{d} \right\}.$$

Trong đó, ký hiệu # biểu thị số phần tử của tập hợp.

1.2 2015

1.2.1. Chứng minh rằng với mọi số nguyên dương m, tồn tại vô số cặp số nguyên dương (x, y) nguyên tố cùng nhau sao cho:

$$x \mid y^2 + m, \text{ và } y \mid x^2 + m.$$

1.2.2. Chứng minh rằng với mọi số nguyên dương $n \geq 3$, tồn tại n số nguyên dương phân biệt sao cho tổng các lập phương của chúng cũng là một lập phương hoàn hảo.

1.2.3. Chứng minh rằng trong bất kỳ dãy 20 số nguyên dương liên tiếp nào cũng tồn tại một số nguyên d sao cho với mọi số nguyên dương n, bất đẳng thức sau luôn đúng:

$$n\sqrt{d} \cdot \left\{n\sqrt{d}\right\} > \frac{5}{2},$$

trong đó $\{x\}$ ký hiệu phần thập phân của x, tức là $\{x\} = x - \lfloor x \rfloor$.

1.2.4. Có tồn tại số nguyên tố nào có biểu diễn thập phân dưới dạng

$$3811\underbrace{11\ldots1}_{n \text{ chữ số } 1}?$$

1.2.5. Cho N là một số có ba chữ số phân biệt và khác 0. Ta gọi N là một số *tầm thường* nếu nó có tính chất sau: khi viết ra tất cả 6 hoán vị có ba chữ số từ các chữ số của N, trung bình cộng của chúng bằng chính N. Ví dụ: $N = 481$ là số *tầm thường* vì trung bình cộng của các số $\{418, 481, 148, 184, 814, 841\}$ bằng 481. Hãy xác định số *tầm thường* lớn nhất.

1.2.6. Cho dãy các số nguyên dương phân biệt $a_1, a_2, a_3, \ldots$, và một hằng số thực $0 < c < \frac{3}{2}$. Chứng minh rằng tồn tại vô hạn số nguyên dương k sao cho:

$$\operatorname{lcm}(a_k, a_{k+1}) > ck.$$

1.2.7. Cho n là một số nguyên dương. Chứng minh rằng với mọi số nguyên dương a, b, c không vượt quá $3n^2 + 4n$, tồn tại các số nguyên x, y, z có giá trị tuyệt đối không vượt quá $2n$ và không đồng thời bằng 0, sao cho

$$ax + by + cz = 0.$$

1.2.8. Cho n, m là các số nguyên lớn hơn 1, và $a_1, a_2, \ldots, a_m$ là các số nguyên dương không vượt quá n^m. Hãy chứng minh rằng tồn tại các số nguyên dương $b_1, b_2, \ldots, b_m \leq n$ sao cho:

$$\gcd(a_1 + b_1, a_2 + b_2, \ldots, a_m + b_m) < n.$$

1.2.9. Với $m, n > 1$, giả sử $a_1, \ldots, a_m$ là các số nguyên dương sao cho có ít nhất một $a_i \leq n^{2^{m-1}}$. Chứng minh rằng tồn tại các số nguyên $b_1, \ldots, b_m \in \{1, 2\}$ sao cho:

$$\gcd(a_1 + b_1, \ldots, a_m + b_m) < n.$$

1.2.10. Cho các số nguyên dương phân biệt đôi một $a_1 < a_2 < \cdots < a_n$, trong đó a_1 là số nguyên tố và $a_1 \geq n + 2$. Trên đoạn thẳng $I = [0, \prod_{i=1}^{n} a_i]$ trên trục số thực, đánh dấu tất cả các số nguyên chia hết cho ít nhất một trong các số $a_1, a_2, \ldots, a_n$. Các điểm này chia đoạn I thành nhiều đoạn con.

Chứng minh rằng tổng bình phương độ dài các đoạn con đó chia hết cho a_1.

1.2.11. Một số nguyên dương n được gọi là **trơn** nếu tồn tại các số nguyên $a_1, a_2, \ldots, a_n$ sao cho:

$$a_1 + a_2 + \cdots + a_n = a_1 \cdot a_2 \cdot \cdots \cdot a_n = n.$$

Hãy tìm tất cả các số trơn.

1.2.12. Chứng minh rằng nếu n là một số nguyên dương đủ lớn, thì trong bất kỳ tập hợp gồm n số nguyên dương khác nhau nào cũng tồn tại bốn số sao cho bội chung nhỏ nhất của chúng lớn hơn $n^{3,99}$.

1.2.13. Với mọi số tự nhiên $n > 1$, phân số $\frac{1}{n}$ với số chữ số thập phân hữu hạn dưới dạng thập phân vô hạn ví dụ như: 0.5 được viết là $\frac{1}{2} = 0.4\overline{9}$. Hãy xác định độ dài phần không tuần hoàn trong biểu diễn thập phân vô hạn của $\frac{1}{n}$.

1.2.14. Chứng minh rằng từ một tập gồm 11 số chính phương, ta luôn có thể chọn ra sáu số $a^2, b^2, c^2, d^2, e^2, f^2$ sao cho:

$$a^2 + b^2 + c^2 \equiv d^2 + e^2 + f^2 \pmod{12}$$

1.2.15. Cho số nguyên $n \geq 2$, và đặt:

$$A_n = \{2^n - 2^k \mid k \in \mathbb{Z},\, 0 \leq k < n\}.$$

Tìm số nguyên dương lớn nhất không thể biểu diễn được dưới dạng tổng của một hay nhiều (không nhất thiết khác nhau) phần tử trong tập A_n.

1.2.16. Gọi $M_0 \subset \mathbb{N}$ là một tập hợp hữu hạn, không rỗng chứa một số số tự nhiên. Ali tạo ra các tập $M_1, M_2, \ldots, M_n$ theo quy trình sau: Tại bước n, Ali chọn một phần tử $b_n \in M_{n-1}$, sau đó định nghĩa tập:

$$M_n = \{b_n m + 1 \mid m \in M_{n-1}\}.$$

Chứng minh rằng tồn tại một bước nào đó mà trong tập tạo ra, không có phần tử nào chia hết cho phần tử nào khác trong cùng tập.

1.2.17. Giả sử a_1, a_2, a_3 là ba số nguyên dương cho trước. Xét dãy số được xác định bởi công thức:

$$a_{n+1} = \operatorname{lcm}[a_n, a_{n-1}] - \operatorname{lcm}[a_{n-1}, a_{n-2}] \quad \text{với } n \geq 3,$$

trong đó $[a, b]$ ký hiệu bội chung nhỏ nhất của a và b, và chỉ được áp dụng với các số nguyên dương.

Chứng minh rằng tồn tại một số nguyên dương $k \leq a_3 + 4$ sao cho $a_k \leq 0$.

1.2.18. Tìm tất cả các số nguyên dương n sao cho

$$\frac{10^n}{n^3 + n^2 + n + 1}$$

là một số nguyên.

1.2.19. Cho n là một số nguyên dương. Các số $a_1, a_2, \ldots, a_k$ là các số nguyên dương không lặp lại, không lớn hơn n, và nguyên tố cùng nhau với n. Nếu $k > 8$, hãy chứng minh rằng:

$$\sum_{i=1}^{k} \left| a_i - \frac{n}{2} \right| < \frac{n(k-4)}{2}.$$

1.2.20. Tìm tất cả các cặp số nguyên dương (m, n) sao cho tồn tại hai số nguyên $a, b > 1$, nguyên tố cùng nhau, thỏa mãn:

$$\frac{a^m + b^m}{a^n + b^n} \in \mathbb{Z}.$$

1.2.21. Xét một số tự nhiên n sao cho tồn tại một số tự nhiên k và k số nguyên tố phân biệt sao cho $n = p_1 \cdot p_2 \cdots p_k$.

- Tìm số lượng các hàm $f : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$ sao cho tích $f(1) \cdot f(2) \cdots f(n)$ chia hết n.
- Với $n = 6$, hãy tìm số lượng các hàm $f : \{1, 2, 3, 4, 5, 6\} \longrightarrow \{1, 2, 3, 4, 5, 6\}$ sao cho tích $f(1) \cdot f(2) \cdot f(3) \cdot f(4) \cdot f(5) \cdot f(6)$ chia hết cho 36.

1.2.22. Gọi k là một số nguyên dương sao cho $k \equiv 1 \pmod 4$, và k không phải là số chính phương. Đặt

$$a = \frac{1+\sqrt{k}}{2}.$$

Chứng minh rằng

$$\left\{ \lfloor a^2 n \rfloor - \lfloor a \lfloor an \rfloor \rfloor : n \in \mathbb{N}_{>0} \right\} = \{1, 2, \dots, \lfloor a \rfloor\}.$$

1.2.23. Cho $a \in \mathbb{Z}$ và $n \in \mathbb{N}_{>0}$. Chứng minh rằng:

$$\sum_{k=1}^{n} a^{\gcd(k,n)}$$

luôn chia hết cho n, trong đó $\gcd(k, n)$ là ước chung lớn nhất của k và n.

1.2.24. Với hai số nguyên dương $k \leq n$, ký hiệu $M(n, k)$ là bội chung nhỏ nhất của dãy số $n, n-1, \dots, n-k+1$. Gọi $f(n)$ là số nguyên dương lớn nhất thỏa mãn:

$$M(n, 1) < M(n, 2) < \cdots < M(n, f(n)).$$

Chứng minh rằng:

- Với mọi số nguyên dương n, ta có $f(n) < 3\sqrt{n}$.
- Với mọi số nguyên dương N, tồn tại hữu hạn số n sao cho $f(n) \leq N$, tức là $f(n) > N$ với mọi n đủ lớn.

1.2.25. Cho số nguyên tố $p \geq 5$. Chứng minh rằng tập $\{1, 2, \dots, p-1\}$ có thể được chia thành hai tập con không rỗng sao cho tổng các phần tử của một tập con và tích các phần tử của tập con còn lại cho cùng một phần dư modulo p.

1.2.26. Cho số nguyên tố p, và dãy số nguyên dương $a_1, a_2, a_3, \dots$ thỏa mãn:

$$a_n a_{n+2} = a_{n+1}^2 + p \quad \text{với mọi số nguyên dương } n.$$

Chứng minh rằng với mọi n, ta có:

$$a_{n+1} \mid a_n + a_{n+2}.$$

1.2.27. Với mỗi số nguyên dương n, định nghĩa:

$$a_n = \sum_{k=1}^{\infty} \left\lfloor \frac{n + 2^{k-1}}{2^k} \right\rfloor,$$

trong đó $\lfloor x \rfloor$ là phần nguyên của x, tức là số nguyên lớn nhất không vượt quá x.

1.3 2023

1.3.1. Xác định tất cả các hợp số dương n thỏa mãn tính chất sau: nếu các ước số dương của n là $1 = d_1 < d_2 < \cdots < d_k = n$, thì $d_i \mid (d_{i+1} + d_{i+2})$ với mọi $1 \leq i \leq k-2$.

Phần II

Gợi ý

Chương 2

Lý thuyết số

2.1 2014

(1.1.1) (ROU 2014 MO/G9/P2) Do $a + \sqrt{a} > a$ và $a - \sqrt{a} < a$, nên phần thập phân của chúng không thể trùng nhau khi nhân với số nguyên. Hiệu $m(a + \sqrt{a}) - n(a - \sqrt{a})$ không thể là số nguyên, vì vậy phần nguyên của chúng cũng khác nhau. [**10M**]

(1.1.2) (ROU 2014 MO/G10/P1) Với mỗi số chia d, tìm những giá trị k thỏa $d \mid k$, $k \leq d^2$, và tổng lại theo d thay vì k. [**20M**]

2.2 2015

(1.2.1) (BGR 2015 EGMO TST/P4)[1] Thử chọn (x, y) vừa đủ điều kiện chia, kết hợp với sự nguyên tố cùng nhau của (x, y). Xem định lý Euclid về vô hạn số nguyên tố để tạo dãy vô hạn đáp ứng yêu cầu. [**25M**]

(1.2.2) (BGR 2015 EGMO TST/P6) Thử xây dựng một họ các bộ n số (có thể đồng dư hoặc biến thiên theo tham số) sao cho tổng lập phương thu được là (một giá trị tham số)^3. Các ví dụ quen thuộc là các "nhóm" số mà tổng lập phương khéo léo triệt tiêu và cộng dồn thành một khối lập phương. [**25M**]

(1.2.3) Hãy chọn d có dạng $5(4k+3)$ sao cho d không là chính phương và có ước nguyên tố $\equiv 3 \pmod 4$, rồi xét giá trị của $n^2 d$ giữa hai bình phương liên tiếp.

(1.2.4) Lưu ý rằng $381 = 3 \cdot 127$, $3811 = 37 \cdot 103$, và $38111 = 23 \cdot 1657$. Phân tích theo số lượng chữ số của số đã cho theo modulo 3.

(1.2.5) Trong tổng của các hoán vị vai trò của các chữ số là như nhau.

(1.2.6) Giả sử ngược lại: từ một chỉ số K trở đi, các giá trị $\operatorname{lcm}(a_k, a_{k+1})$ đều không vượt quá ck. Chứng minh $\frac{1}{a_k} + \frac{1}{a_{k+1}} \geq \frac{3}{ck}$, rồi tìm cận dưới cho tổng các số $\frac{1}{a_k} + \frac{1}{a_{k+1}}$.

(1.2.7) Ta xét tập giá trị mà biểu thức $ax + by + cz$ có thể đạt được khi $x, y, z \in [-n, n]$, và so sánh với số lượng bộ ba như vậy.

(1.2.8) Giải quyết các trường hợp biên: $\min_i a_i \geq n^m - 1$ qua việc chỉ ra sự tồn tại các bộ (b_i) cụ thể. Sau đó, giả sử phản chứng với $b_1, \ldots, b_m \in \{1, \ldots, n\}$ sao cho có một cặp $\gcd(a_i + b_i, a_j + b_j) = 1$.

(1.2.9) Sử dụng phương pháp trong bài 1.2.8. Giới hạn $n^{2^{m-1}}$ có thể được cải thiện thêm.

(1.2.10) (GBR 2015 TST/N3/P3) Mỗi đoạn con là khoảng giữa hai số nguyên không chia hết cho bất kỳ a_i, tức là nằm ngoài tập hợp các bội số. [**20M**]

(1.2.11) Phân tích $\pmod 4$ để xác định n là 0 hoặc 1 $\pmod 4$. Kiểm tra các trường hợp cụ thể và loại trừ $n = 4$. Xây dựng các ví dụ để chứng minh các số n thỏa mãn là những số $n \equiv 0$ hoặc $1 \pmod 4$, ngoại trừ $n = 4$.

(1.2.12) (HUN 2015 TST/KMA/633) Hãy sắp xếp các số đã cho theo thứ tự tăng dần, ước lượng kích thước của bội chung nhỏ nhất, và tìm cách chọn bốn số sở hữu lũy thừa nguyên tố lớn vượt mức $n^{3.99}$. [**20M**]

(1.2.13) Biểu diễn thập phân vô hạn tuần hoàn của $\frac{1}{n}$ gồm phần không tuần hoàn (các chữ số đầu tiên) và phần tuần hoàn. Phần không tuần hoàn chỉ xuất hiện nếu mẫu số chứa thừa số 2 hoặc 5.

(1.2.14) Ta xét phần dư của số chính phương theo modulo 12 (chỉ có thể là $0, 1, 4, 9$), sau đó áp dụng nguyên lý Dirichlet để xét các phần dư xuất hiện nhiều lần.

[1] IMO SL 1992 P1.

(1.2.15) Tìm ngưỡng qua việc tính tổng các số $2^n - 2^k$, sau đó dùng quy nạp để chứng minh mọi số lớn hơn ngưỡng này đều biểu diễn được.

(1.2.16) Nếu có quan hệ chia hết giữa các phần tử trong tập M_n điều đó dẫn đến một bất đẳng thức giữa giá trị nhỏ nhất ở bước hiện tại và sai biệt lớn nhất giữa các phần tử của tập trước đó.

(1.2.17) Đặt $b_n = \dfrac{a_n}{\operatorname{lcm}(a_{n-2}, a_{n-3})}$, chứng minh dãy b_n nguyên và giảm dần.

(1.2.18) (JPN 2015 MO1/P1) Hãy phân tích mẫu số $n^3 + n^2 + n + 1$ thành nhân tử, sau đó kiểm tra xem khi nào nó chia hết 10^n. [**10M**]

(1.2.19) Cách 1: Khai thác tính đối xứng trong phần dư modulo và viết lại tổng theo số nhỏ hơn và lớn hơn $\frac{n}{2}$.

Cách 2: Dựa trên bất đẳng thức về tổng trung bình và kiểm tra các cấu hình của n theo modulo 4.

(1.2.20) Đặt $m = kn + r$, rồi phân tích tử số theo $a^n + b^n$. Để phân số là số nguyên, cần $a^r + b^r$ chia hết cho $a^n + b^n$, từ đó tìm điều kiện cho r.

(1.2.21) (ROU 2015 MO/G10/P2) Xem xét những giá trị của $f(i)$ phải chứa đủ các ước nguyên tố của n. Lưu ý nếu một trong số các $f(i)$ luôn chọn được bội của tất cả số nguyên tố $(p_1, p_2, \dots)$ thì tích sẽ chia hết n. [**20M**]

(1.2.22) Sử dụng biểu thức $a^2 = a + t$, rồi phân tích phần thập phân $\varepsilon_n = an - \lfloor an \rfloor$ để suy ra sự phân bố đều của hiệu.

(1.2.23) Sử dụng đẳng thức $\displaystyle\sum_{k=1}^{n} a^{\gcd(k,n)} = \sum_{d|n} \phi(d) a^{n/d}$ và áp dụng định lý Euler cùng với nguyên lý đồng dư Trung Hoa.

(1.2.24) Khai thác tính chất chia hết của lcm và lập mâu thuẫn bằng cách xét cấu trúc của dãy liên tiếp.

(1.2.25) Sử dụng *tổng* và *tích* toàn bộ dãy modulo p, rồi chuyển điều kiện về dạng $AB \equiv -1 \pmod{p}$ với A là tổng và B là tích một tập con.

(1.2.26) Trừ hai công thức liên tiếp rồi khai thác tính nguyên tố của p để dẫn đến mâu thuẫn về chia hết.

(1.2.27) Thử viết n trong cơ số 2 rồi phân tích biểu thức $\left\lfloor \frac{n+2^{k-1}}{2^k} \right\rfloor$. Có thể tách từng chữ số nhị phân và xem cách các số hạng góp phần vào tổng.

2.3 2023

(1.3.1) Một số hướng tiếp cận hiệu quả khi khảo sát cấu trúc các ước của hợp số n:

- Thử các trường hợp $n = p^r$, với p nguyên tố.
- Giả sử phản chứng nếu n có nhiều hơn một thừa số nguyên tố.
- Khai thác đối xứng $d_i d_{k+1-i} = n$.

Phần III

Lời giải

Chương 3

Lý thuyết số

3.1 2014

3.2 2015

1.2.3. [BMO 2015/P4][1] Trong 20 số nguyên liên tiếp luôn tồn tại một số có dạng $20k + 15 = 5(4k + 3)$. Ta sẽ chứng minh rằng $d = 5(4k + 3)$ thỏa mãn yêu cầu bài toán.

Vì $d \equiv -1 \pmod 4$, nên d không phải là một số chính phương. Với mọi $n \in \mathbb{N}$, tồn tại một số nguyên a sao cho:

$$a < n\sqrt{d} < a + 1 \implies a^2 < n^2 d < (a + 1)^2.$$

Ta sẽ chứng minh rằng $n^2 d \geq a^2 + 5$. Thật vậy: ta sử dụng Ước nguyên tố dạng $4k + 3$.

Gọi $p \mid (4k + 3)$ sao cho $p \equiv -1 \pmod 4$. Với dạng này, các số $a^2 + 1$ và $a^2 + 4$ không chia hết cho p. Do $p \mid n^2 d$, suy ra:

$$n^2 d \neq a^2 + 1, \quad n^2 d \neq a^2 + 4.$$

Mặt khác, vì $5 \mid n^2 d$ và $5 \nmid a^2 + 2, \quad 5 \nmid a^2 + 3$, ta có:

$$n^2 d \neq a^2 + 2, \quad n^2 d \neq a^2 + 3, \quad n^2 d > a^2 \implies n^2 d \geq a^2 + 5.$$

Do đó:

$$n\sqrt{d} \cdot \left\{ n\sqrt{d} \right\} = n\sqrt{d}(n\sqrt{d} - a) = n^2 d - an\sqrt{d}.$$

Ta đánh giá:

$$n^2 d \geq a^2 + 5, \quad n\sqrt{d} < a + 1 \implies an\sqrt{d} < a(a + 1).$$

Vì $a^2 + 5 > a(a + 1)$, ta có:

$$n\sqrt{d} \cdot \left\{ n\sqrt{d} \right\} > a^2 + 5 - a(a + 1) = 5 - a.$$

Khi $a \leq 2$, ta có $n\sqrt{d} > a + 1 \geq 3$, và vì $\left\{ n\sqrt{d} \right\} > 0$, nên bất đẳng thức đúng.

Còn khi $a \geq 3$, ta có:

$$n\sqrt{d} \cdot \left\{ n\sqrt{d} \right\} > 5 - a \geq \frac{5}{2},$$

vì biểu thức là số dương tăng theo a.

Kết luận: Trong mọi dãy 20 số nguyên dương liên tiếp luôn tồn tại một số d sao cho với mọi $n \in \mathbb{N}$, ta có:

$$n\sqrt{d} \cdot \left\{ n\sqrt{d} \right\} > \frac{5}{2}.$$

[**20M**]. **Tham chiếu:** Ước nguyên tố dạng $4k + 3$. □

[1] Lời giải chính thức.

1.2.4. [BxMO 2015/P3][2]

Ta xét ba trường hợp dựa trên số lượng chữ số 1:

Trường hợp 1: số lượng chữ số 1 là $3k$.

Xuất phát từ vế trái:

$$38\underbrace{11\ldots1}_{3k\text{ chữ số }1} = 38\cdot 10^{3k} + \frac{10^{3k}-1}{9} = \frac{343\cdot 10^{3k}-1}{9}.$$

Nhận thấy:

$$\frac{343\cdot 10^{3k}-1}{9} = \frac{(7\cdot 10^k-1)(49\cdot 10^{2k}+7\cdot 10^k+1)}{9}.$$

Tiếp tục phân tích:

$$= \frac{7\cdot 10^k-1}{3}\cdot\frac{49\cdot 10^{2k}+7\cdot 10^k+1}{3} = 2\underbrace{33\ldots3}_{k}\times 16\underbrace{33\ldots3}_{k-1\text{ chữ số }3}5\underbrace{66\ldots6}_{k-1\text{ chữ số }6}7.$$

Trường hợp 2: số lượng chữ số 1 là $3k+1$.

Xuất phát từ vế trái:

$$38\underbrace{11\ldots1}_{3k+1\text{ chữ số }1} = 38\cdot 10^{3k+1} + \frac{10^{3k+1}-1}{9} = \frac{343\cdot 10^{3k+1}-1}{9}.$$

Do $343 = 3\times 127 - 38$, ta viết lại thành:

$$= \frac{(381\times 10^{3k+1} - 38\cdot 10^{3k+1})-1}{9} = 127\times\frac{3\cdot 10^{3k+1}-1}{9} = 3\times 127\underbrace{037037\ldots037}_{k\text{ cụm }037}.$$

Trường hợp 3: số lượng chữ số 1 là $3k+2$.

Xuất phát từ vế trái:

$$38\underbrace{11\ldots1}_{3k+2\text{ chữ số }1} = 38\cdot 10^{3k+2} + \frac{10^{3k+2}-1}{9} = \frac{3429\cdot 10^{3k}-1}{9}.$$

Vì $3429 = 37\times 103 - 38$, ta lại viết thành:

$$= \frac{(3811\times 10^{3k} - 38\times 10^{3k})-1}{9} = 37\times\frac{103\times 10^{3k}-1}{9} = 37\times 103\underbrace{003003\ldots003}_{k\text{ cụm }003}.$$

Kết luận: Trong cả ba trường hợp, số ban đầu đều được phân tích thành tích hai số nguyên lớn hơn 1, do đó số đã cho là hợp số.

[**10M**]. **Tham chiếu:** Biểu diễn số có các chữ số 1 Định lý chia có dư. □

[2]Lời giải của **codyj**.

1.2.5. [CAN 2015 TST/P3][3]

Giả sử *abc* là một số *tầm thường*. Sáu hoán vị gồm $\{abc, acb, bac, bca, cab, cba\}$. Tổng của chúng là:

$$222(a+b+c) \implies \frac{222(a+b+c)}{6} = 37(a+b+c).$$

Vì *abc* là *tầm thường*, nên:

$$100a + 10b + c = 37(a+b+c) \implies 63a = 27b + 36c \implies 7a = 3b + 4c. \implies 3(a-b) = 4(c-a).$$

Như vậy $3 \mid c - a$, do đó $c \geq a + 3$. Tương tự $a \geq b + 4$. Nên $c \geq b + 7$. $c \geq 9$ nên $b \leq 2$, vì $b > 0$ nên b chỉ có thể là 1 hoặc 2. Do đó *abc* là 518 hoặc 629.

Kết luận: Số *tầm thường* lớn nhất là $\boxed{629}$.

[**0M**]. **Tham chiếu:** Biểu diễn số có các chữ số 1 Định lý chia có dư. □

[3] Lời giải chính thức.

1.2.6. [CHN 2015 TST1/D1/P2][4]

Giả sử ngược lại: từ một chỉ số K trở đi, các giá trị $\operatorname{lcm}(a_k, a_{k+1})$ đều không vượt quá ck.

Khẳng định — Với mọi $k \geq K$, ta có

$$\frac{1}{a_k} + \frac{1}{a_{k+1}} \geq \frac{3}{ck}.$$

Chứng minh. Do $a_k \neq a_{k+1}$, và vì $\gcd(a_k, a_{k+1})$ chia hết $a_k + a_{k+1}$, cho nên

$$a_k + a_{k+1} > 2\min\{a_k, a_{k+1}\} \geq 2\gcd(a_k, a_{k+1}) \implies a_k + a_{k+1} \geq 3\gcd(a_k, a_{k+1}).$$

Do đó,

$$\frac{1}{a_k} + \frac{1}{a_{k+1}} = \frac{a_k + a_{k+1}}{\gcd(a_k, a_{k+1}) \cdot \operatorname{lcm}(a_k, a_{k+1})} \geq \frac{3}{\operatorname{lcm}(a_k, a_{k+1})} \geq \frac{3}{ck}.$$

■

Lấy tổng từ $k = K$ đến $k = N$, với N tùy ý, ta có

$$\sum_{i=K}^{N} \left(\frac{1}{a_i} + \frac{1}{a_{i+1}} \right) \geq \frac{3}{c} \left(\frac{1}{K} + \cdots + \frac{1}{N} \right) \tag{1}$$

Tuy nhiên, do các số $a_K, \ldots, a_{N+1}$ là đôi một phân biệt, nên trong tổng bên trái, mỗi số hạng $\frac{1}{j}$ chỉ xuất hiện tối đa hai lần với mỗi số nguyên dương j; do đó,

$$\sum_{i=K}^{N} \left(\frac{1}{a_i} + \frac{1}{a_{i+1}} \right) \leq \frac{2}{1} + \cdots + \frac{2}{N} \tag{2}$$

Kết hợp (1) và (2), rồi sắp xếp lại, ta được

$$\frac{2}{1} + \cdots + \frac{2}{K} \geq \left(\frac{3}{c} - 2 \right) \left(\frac{1}{K} + \cdots + \frac{1}{N} \right).$$

Vì $3/c > 2$, nên vế trái là cố định còn vế phải lại không bị chặn khi $N \to \infty$, vô lý.

Kết luận: tồn tại vô hạn số nguyên dương k sao cho: $\operatorname{lcm}(a_k, a_{k+1}) > ck$.

[**10M**]. **Tham chiếu:** Tính phân kỳ của chuỗi điều hoà. Tính chất gcd và lcm. □

[4] Lời giải của **TheUltimate123**.

1.2.7. [CHN 2015 TST1/D2/P2][5]

Xét tập giá trị

$$A = \{ax + by + cz \mid x, y, z \in \mathbb{Z} \cap [-n, n]\}.$$

Ta có

$$|A| \leq (2n \cdot a + 2n \cdot b + 2n \cdot c) + 1 \leq 6n(3n^2 + 4n) + 1 = 6n^3 + 8n^2 + 1.$$

Có tổng cộng $(2n+1)^3$ bộ ba $(x, y, z) \in [-n, n]^3$, mà

$$(2n+1)^3 > 6n^3 + 8n^2 + 1,$$

nên theo Nguyên lý Dirichlet, tồn tại hai bộ ba khác nhau

$$(x, y, z), (x', y', z') \in ([-n, n] \cap \mathbb{Z})^3 \quad \text{với} \quad ax + by + cz = ax' + by' + cz'.$$

Bộ bộ ba tạo thành từ hiệu tương ứng của các thành phần của hai bộ ba này:

$$a(x - x') + b(y - y') + c(z - z') = 0 \implies ax + by + cz = 0,$$

là một bộ ba $x - x', y - y', z - z' \in [-2n, 2n]$, với các thành phần không đồng thời bằng 0.

Kết luận: Tồn tại bộ (x, y, z) thoả mãn yêu cầu đề bài.

[**5M**]. **Tham chiếu:** Nguyên lý Dirichlet. □

[5] Lời giải của **nayel**.

1.2.8. [EGMO 2015/P3][6]

Giả sử không mất tính tổng quát rằng a_1 là số nhỏ nhất trong các số a_i.

Nếu $a_1 \geq n^m$, thì tất cả các số a_i đều bằng nhau, hoặc $a_1 = n^m - 1$ và tồn tại chỉ số j sao cho $a_j = n^m$.

Trong trường hợp đầu tiên, ta có thể chọn (ví dụ) $b_1 = 1$, $b_2 = 2$, và các số b_i còn lại tuỳ ý. Khi đó,

$$\gcd(a_1 + b_1, a_2 + b_2, \ldots, a_m + b_m) \leq \gcd(a_1 + b_1, a_2 + b_2) = 1.$$

Trong trường hợp thứ hai, ta chọn $b_1 = 1$, $b_j = 1$, và các b_i còn lại tuỳ ý, ta lại có

$$\gcd(a_1 + b_1, a_2 + b_2, \ldots, a_m + b_m) \leq \gcd(a_1 + b_1, a_j + b_j) = 1.$$

Vì vậy, từ đây trở đi, ta giả sử rằng $a_1 \leq nm - 2$.

Giả sử rằng không tồn tại bộ số $b_1, \ldots, b_m$ như mong muốn và ta sẽ tìm mâu thuẫn.

Khi này, với mọi bộ số $b_1, \ldots, b_m \in \{1, \ldots, n\}$, ta luôn có

$$\gcd(a_1 + b_1, a_2 + b_2, \ldots, a_m + b_m) \geq n.$$

Mặt khác, ta cũng có

$$\gcd(a_1 + b_1, a_2 + b_2, \ldots, a_m + b_m) \leq a_1 + b_1 \leq n^m + n - 2.$$

Do đó, chỉ có tối đa $n^m - 1$ giá trị khả dĩ cho ước chung lớn nhất. Tuy nhiên, có n^m cách chọn bộ m số $(b_1, \ldots, b_m)$. Khi đó, theo Nguyên lý Dirichlet, tồn tại hai bộ khác nhau cho cùng một giá trị ước chung lớn nhất, gọi là d.

Nhưng vì $d \geq n$, nên với mỗi i, chỉ có nhiều nhất một giá trị $b_i \in \{1, 2, \ldots, n\}$ sao cho $a_i + b_i$ chia hết cho d. Do đó, chỉ có nhiều nhất một bộ m-tuple $(b_1, b_2, \ldots, b_m)$ sao cho ước chung lớn nhất là d. Điều này dẫn đến mâu thuẫn như mong muốn.

Kết luận: Phản chứng sai, do đó tồn tại bộ $(b_1, \ldots, b_m) \in \{1, \ldots, n\}^m$ sao cho

$$\gcd(a_1 + b_1, \ldots, a_m + b_m) < n.$$

[**10M**]. **Tham chiếu:** Nguyên lý phản chứng. Nguyên lý Dirichlet. Tính chất gcd và lcm. □

[6] Lời giải chính thức.

1.2.11. [GER 2015 MO/P2][7]

Xét (mod 4), ta thấy nếu n trơn thì $n \equiv 0$ hoặc 1 (mod 4).

Trường hợp $n = 4k + 1$: Chọn $a_1 = n,\ 2k$ số $-1,\ 2k$ số 1.

Tổng: $n + 2k(-1) + 2k(1) = n$.

Tích: $n \cdot (-1)^{2k} \cdot 1^{2k} = n$.

Trường hợp $n = 8k$ $(k \geq 1)$: Chọn $a_1 = 2,\ a_2 = 4k,\ 6k - 2$ số 1, $2k$ số -1.

Tổng: $2 + 4k + (6k - 2) \cdot 1 + 2k \cdot (-1) = 8k = n$.

Tích: $2 \cdot 4k \cdot 1^{6k-2} \cdot (-1)^{2k} = 8k = n$.

Trường hợp $n = 16k + 12$: Chọn $a_1 = a_2 = 2,\ a_3 = 4k + 3,\ 14k + 7$ số 1, $2k + 2$ số -1.

Tổng: $2 + 2 + (4k + 3) + (14k + 7) - (2k + 2) = 16k + 12 = n$.

Tích: $2 \cdot 2 \cdot (4k + 3) \cdot 1^{14k+7} \cdot (-1)^{2k+2} = 16k + 12$.

Trường hợp $n = 16k + 4$ $(k \geq 1)$: Chọn $a_1 = -2,\ a_2 = 8k + 2,\ 12k + 3$ số 1, $4k - 1$ số -1.

Tổng: $-2 + (8k + 2) + (12k + 3) \cdot 1 + (4k - 1) \cdot (-1) = 16k + 4 = n$.

Tích: $(-2) \cdot (8k + 2) \cdot 1^{12k+3} \cdot (-1)^{4k-1} = 16k + 4$.

Cuối cùng, kiểm tra các giá trị $n < 10$, chỉ $n = 4$ không thoả mãn.

Kết luận: Các n "trơn" là mọi $n \equiv 0$ hoặc 1 (mod 4), trừ $n = 4$.

[**25M**] **Tham chiếu:** Tính chất đại số của phép đồng dư. Đồng dư modulo n. □

[7] Lời giải của **MathGan**.

1.2.13. [IND 2015 MO/P2][8]

Gọi biểu diễn thập phân của $\frac{1}{n}$ là:

$$\frac{1}{n} = 0.a_1a_2\cdots a_{x_n}\overline{b_1b_2\cdots b_{\ell_n}},$$

trong đó x_n: độ dài phần không tuần hoàn, ℓ_n: độ dài phần tuần hoàn.

Ta có:
$$\frac{10^{x_n+\ell_n}-10^{x_n}}{n} \in \mathbb{Z}^+ \implies n \mid \left(10^{x_n+\ell_n}-10^{x_n}\right) \implies n \mid 10^{x_n}(10^{\ell_n}-1).$$

Giả sử $n = 2^a \cdot 5^b \cdot q$, với $\gcd(q, 10) = 1$. Để $\frac{1}{n}$ có phần không tuần hoàn dài x_n, thì:

$$2^a5^b \mid 10^{x_n} \implies x_n = \min\{x :\ 2^a5^b \mid 10^x\} = \max(a, b).$$

Kết luận: Độ dài phần không tuần hoàn trong biểu diễn thập phân vô hạn của $\frac{1}{n}$ là:

$$x_n = \max(a, b) \quad \text{với } n = 2^a \cdot 5^b \cdot q,\ \gcd(q, 10) = 1.$$

[**5M**]. **Tham chiếu:** Biểu diễn số có các chữ số 1. □

[8] Lời giải của **utkarshgupta**.

1.2.14. [IND 2015 MO/P6][9]

Các phần dư khả dĩ của một số chính phương modulo 12 là:

$$x^2 \equiv 0, 1, 4, 9 \pmod{12}.$$

Gọi S là tập gồm 11 số chính phương. Mỗi phần tử của S thuộc một trong 4 lớp dư trên.

Ta cần tìm hai tập rời nhau $A, B \subset S$, mỗi tập gồm 3 phần tử, sao cho

$$\sum_{x\in A} x \equiv \sum_{y\in B} y \pmod{12}.$$

Trường hợp 1: Có ít nhất 6 phần tử trong S có cùng phần dư modulo 12 (giả sử là r). Ta có thể chọn hai bộ ba rời nhau gồm các phần tử đều có phần dư r, nên tổng mỗi bộ ba là

$$3r \pmod{12} \text{ Hai tổng này bằng nhau modulo 12.}$$

Trường hợp 2: Có một phần dư xuất hiện 4 hoặc 5 lần. Vì tổng cộng có 11 phần tử và chỉ 4 phần dư khả dĩ, theo nguyên lý Dirichlet sẽ có ít nhất một phần dư khác xuất hiện từ 2 lần trở lên. Từ đó ta có thể chọn hai bộ ba từ các phần dư khác nhau. Vì số phần dư là hữu hạn, nên số tổng modulo 12 có thể tạo ra từ các bộ ba cũng hữu hạn. Do đó vẫn tồn tại hai bộ ba có tổng bằng nhau modulo 12.

Trường hợp 3: Mỗi phần dư trong $\{0, 1, 4, 9\}$ xuất hiện tối đa 3 lần. Vì $|S| = 11$, trường hợp này tồn tại.

Số bộ ba phân biệt có thể chọn từ S là:

$$\binom{11}{3} = 165.$$

Xét các bộ ba (cho phép trùng lặp phần tử, không phân biệt thứ tự) từ tập $\{0, 1, 4, 9\}$, là số tổ hợp có lặp:

$$\binom{4+3-1}{3} = \binom{6}{3} = 20.$$

Tức là chỉ có tối đa 20 tổng khác nhau modulo 12 có thể thu được từ một bộ ba.

Vì có 165 bộ ba trong S nhưng chỉ có 20 khả năng tổng modulo 12, theo nguyên lý Dirichlet tồn tại hai bộ ba khác nhau có tổng đồng dư modulo 12.

Kết luận: Trong cả ba trường hợp, luôn tồn tại hai tập rời nhau gồm ba số chính phương có tổng bằng nhau modulo 12.

[**15M**]. **Tham chiếu:** Nguyên lý Dirichlet. □

[9] Dựa theo lời giải của **Sahil**.

1.2.15. [IND 2015 TST2/P1][10]

Khẳng định (1) — Mọi số lớn hơn $(n-2)\cdot 2^n+1$ đều biểu diễn được bằng tổng các phần tử trong A_n. Ta chứng minh bằng quy nạp theo n.

Chứng minh. Bước cơ sở: $n=2 \Rightarrow A_2=\{3,2\}$. Mọi số dương $\neq 1$ đều biểu diễn được.

Giả sử đúng với $n-1$. Xét $n>2$, và $m>(n-2)\cdot 2^n+1$.

Trường hợp 1: m chẵn. Khi đó

$$\frac{m}{2}>(n-3)\cdot 2^{n-1}+1.$$

Theo giả thiết quy nạp, $\frac{m}{2}$ biểu diễn được từ A_{n-1}, tức là từ các $2^{n-1}-2^{k_i}$. Nhân hai vế:

$$m=\sum(2^n-2^{k_i+1})\in A_n.$$

Trường hợp 2: m lẻ. Khi đó

$$\frac{m-(2^n-1)}{2}>(n-3)\cdot 2^{n-1}+1,$$

nên $m-(2^n-1)$ biểu diễn được từ A_{n-1}, cộng thêm $2^n-1\in A_n$ để được m. ■

Khẳng định (2) — Số $(n-2)\cdot 2^n+1$ không biểu diễn được.

Chứng minh. Gọi N là số nhỏ nhất $\equiv 1 \pmod{2^n}$ biểu diễn được bằng tổng các phần tử trong A_n. Khi đó:

$$N=\sum(2^n-2^{k_i})=n\cdot 2^n-\sum 2^{k_i}.$$

Nếu có $k_i=k_j$, ta có thể thay $2\cdot(2^n-2^k)\to 2^n-2^{k+1}$, từ đó giảm N đi 2^n, mâu thuẫn với tính nhỏ nhất của N. Vậy các k_i là phân biệt:

$$\sum 2^{k_i}\leq 2^0+\cdots+2^{n-1}=2^n-1.$$

Từ đó:

$$N=n\cdot 2^n-(2^n-1)=(n-1)\cdot 2^n+1.$$

■

Do (1) và (2), suy ra số lớn nhất không biểu diễn được là:

$$(n-2)\cdot 2^n+1.$$

[**25M**]. **Tham chiếu:** Nguyên lý quy nạp toán học. □

[10] IMO SL 2014 N1.

1.2.16. [IRN 2015 MO/N2][11]

Giả sử tại bước n, tồn tại hai phần tử $k, t \in M_{n-1}$ sao cho

$$b_n k + 1 \mid b_n t + 1.$$

Suy ra $b_n k + 1 \mid b_n(t - k) \Rightarrow b_n k + 1 \mid k - t$.

Vậy nếu có quan hệ chia hết, thì

$$\max(M_{n-1}) - \min(M_{n-1}) \geq \min(M_n). \tag{1}$$

Gọi $M = \max(M_1),\ m = \min(M_1)$. Ta có:

$$\max(M_n) - \min(M_n) = b_n b_{n-1} \cdots b_2 (M - m),$$

và

$$\min(M_n) \geq b_n b_{n-1} \cdots b_2 m + b_{n-1} \cdots b_2.$$

Thế vào (1):

$$b_2 \cdots b_{n-1}(M - m - 1) \geq b_2 \cdots b_n m \Rightarrow \frac{M - m - 1}{m} \geq b_n.$$

Mặt khác, vì $b_n \in M_{n-1}$, và các phần tử trong dãy M_n tăng rất nhanh qua mỗi bước (do mỗi phần tử mới có dạng $b_n m + 1$), nên tồn tại một số N sao cho với mọi $n \geq N$, ta có:

$$b_n \geq n - 2.$$

Do đó, nếu

$$\frac{M - m - 1}{m} < n - 2,$$

thì không thể tồn tại quan hệ chia hết trong M_n.

Kết luận: Khi n đủ lớn, bất đẳng thức trên luôn sai, nên tồn tại một bước mà trong M_n, không có phần tử nào chia hết cho phần tử khác.

[**25M**]. **Tham chiếu:** Nguyên lý phản chứng. □

[11] Dựa theo lời giải của **Arefe**.

1.2.17. [IRN 2015 TST/D3-P2][12]

Ta chứng minh điều mạnh hơn: tồn tại $k \le a_3 + 3$ sao cho $a_k \le 0$.

Bước 1: Đặt

$$b_n = \frac{a_n}{\operatorname{lcm}(a_{n-2}, a_{n-3})} \quad \text{với mọi } n \ge 5.$$

Ta chứng minh rằng $b_n \in \mathbb{N}$ và giảm dần.

Với $n \ge 4$, $a_{n-2} \mid a_n$ và $a_{n-3} \mid a_n$, nên $\operatorname{lcm}(a_{n-2}, a_{n-3}) \mid a_n$, suy ra $b_n \in \mathbb{N}$.

Khẳng định — Với mọi $n \ge 5$, ta có $b_{n+1} < b_n$.

Chứng minh. Ta có

$$a_{n+1} = \operatorname{lcm}(a_n, a_{n-1}) - \operatorname{lcm}(a_{n-1}, a_{n-2}).$$

Thay $a_n = b_n \cdot \operatorname{lcm}(a_{n-2}, a_{n-3})$, ta suy ra:

$$a_{n+1} = \operatorname{lcm}(b_n, a_{n-2}, a_{n-3}, a_{n-1}) - \operatorname{lcm}(a_{n-1}, a_{n-2}).$$

Vì $a_{n-3} \mid a_{n-1}$, nên

$$a_{n+1} = \operatorname{lcm}(b_n, a_{n-2}, a_{n-1}) - \operatorname{lcm}(a_{n-1}, a_{n-2}) \implies b_{n+1} < b_n.$$

■

Bước 2: Ước lượng b_5.

Ta có

$$a_4 = \operatorname{lcm}(a_3, a_2) - \operatorname{lcm}(a_2, a_1) = c \cdot a_2, \quad \text{với } c \le a_3 - 1,$$

và

$$a_5 = \operatorname{lcm}(a_4, a_3) - \operatorname{lcm}(a_3, a_2) = \operatorname{lcm}(ca_2, a_3) - \operatorname{lcm}(a_3, a_2).$$

Suy ra:

$$b_5 = \frac{a_5}{\operatorname{lcm}(a_3, a_2)} \le c - 1 \le a_3 - 2.$$

Kết luận: Dãy b_n nguyên, giảm dần, bắt đầu từ $b_5 \le a_3 - 2$, nên sau tối đa $a_3 - 2$ bước sẽ đạt giá trị không dương. Do đó, tồn tại $k \le a_3 + 3$ sao cho $a_k = 0 \le 0$.

[**25M**]. **Tham chiếu:** Tính chất gcd và lcm. Nguyên lý cực hạn. □

[12] Lời giải của **guptaamitu1**.

1.2.19. [KOR 2015 MO/P8][Cách 1][13]

Với các giá trị đặc biệt như $n = p$ nguyên tố, $n = p^2$, hoặc $n = pq$ với p, q là các số nguyên tố, ta có thể kiểm tra trực tiếp. Vì vậy, ta giả sử từ đây rằng n không thuộc các dạng này.

Với mỗi số a sao cho $\gcd(a, n) = 1$, thì $\gcd(n - a, n) = 1$. Trong cặp $(a, n - a)$, một số nhỏ hơn $\frac{n}{2}$, số còn lại lớn hơn.

Giả sử $a < \frac{n}{2}$, ta có:

$$\left|\frac{n}{2} - a\right| + \left|\frac{n}{2} - (n - a)\right| = n - 2a.$$

Suy ra:

$$\sum_{i=1}^{k} \left|a_i - \frac{n}{2}\right| = \frac{n\varphi(n)}{2} - 2S, \tag{1}$$

trong đó S là tổng các số $< \frac{n}{2}$ và nguyên tố cùng nhau với n.

Gọi p là ước nguyên tố nhỏ nhất của n, đặt $m = \frac{n}{p}$. Gọi T là tổng các số $< m$ nguyên tố cùng nhau với m, ta có:

$$T = \frac{m\varphi(m)}{2} \quad \text{và} \quad \varphi(m) \geq 2p \implies S \geq T \geq pm = n. \tag{2}$$

Thay (2) vào (1):

$$\sum_{i=1}^{k} \left|a_i - \frac{n}{2}\right| \leq \frac{n\varphi(n)}{2} - 2n = \frac{n(k-4)}{2}.$$

[**30M**]. **Tham chiếu:** Hàm phi Euler Tổng các số nguyên tố cùng nhau với m. ☐

[13] Lời giải của **andria**.

1.2.19. [KOR 2015 MO/P8][Cách 2][14]

Ta nhận thấy rằng nếu a_i thuộc tập thì $n - a_i$ cũng thuộc tập, tổng hai số là n. Do đó k chẵn và:

$$a_{k/2} < \frac{n}{2} < a_{k/2+1}, \quad \sum_{i=1}^{k} a_i = \frac{nk}{2}. \tag{1}$$

Ta có:

$$\sum_{i=1}^{k} \left| a_i - \frac{n}{2} \right| = \sum_{i=1}^{k/2} \left(\frac{n}{2} - a_i \right) + \sum_{i=k/2+1}^{k} \left(a_i - \frac{n}{2} \right)$$

Kết hợp với (1), bất đẳng thức tương đương:

$$S = \sum_{i=1}^{k/2} a_i > n.$$

Ta cần chứng minh tổng các số $< \frac{n}{2}$ và nguyên tố cùng nhau với n lớn hơn n.

Gọi $f(n) \approx \frac{n}{3}$, được điều chỉnh để tránh chia hết cho 3:

$$f(n) = \begin{cases} \frac{n \pm 1}{3}, & n \equiv \mp 1 \pmod 3 \\ \frac{n}{3} \pm 1, & n \equiv 0 \pmod 3 \end{cases} \implies \frac{n}{3} - 1 \le f(n) \le \frac{n}{3} + 1, \ \gcd(f(n), n) = 1$$

Trường hợp 1: n lẻ. Nếu $n < 30$, kiểm tra trực tiếp. Với $n > 30$, đặt $n = 2^k + m$. Khi đó:

$$S \ge 2^{k-1} - 1 + \frac{n}{3} - 1 + \frac{n-1}{2} = \frac{13n}{12} - \frac{5}{2} > n$$

Trường hợp 2: $n \equiv 0 \mod 4$. Khi đó:

$$S = \frac{1}{2} \cdot \frac{n}{2} \cdot \frac{k}{2} = \frac{nk}{8} > n \quad (\text{vì } k > 8)$$

Trường hợp 3: $n = 4m + 2$. Với $m > 7$, ta có:

$$S \ge 1 + m + \frac{4m+2}{3} - 1 + 2m - 1 = \frac{13m}{3} - \frac{1}{3} > 4m + 2 = n$$

Kết luận: Trong cả ba trường hợp, ta có:

$$\sum_{i=1}^{k/2} a_i > n \implies \sum_{i=1}^{k} \left| a_i - \frac{n}{2} \right| < \frac{n(k-4)}{2}.$$

[**30M**]. **Tham chiếu:** Hàm phi Euler. □

[14]Lời giải của **rkm0959**.

1.2.20. [MEMO 2015/I/P4][15]

Giả sử $\gcd(a, b) = 1$, $a, b > 1$, và phân số:

$$\frac{a^m + b^m}{a^n + b^n}$$

là một số nguyên.

Ta có $a^n + b^n \mid a^m + b^m$, nên $m \geq n$. Đặt $m = kn + r$, với $k \geq 1$, $0 \leq r < n$.

Ta phân tích:

$$\frac{a^m + b^m}{a^n + b^n} = \frac{(a^n)^k a^r + (b^n)^k b^r}{a^n + b^n}$$

Tử số là tổ hợp của $a^n + b^n$ nhân với hệ số nào đó cộng với phần dư. Quá trình này lặp lại đến khi còn lại:

$$\frac{a^r + b^r}{a^n + b^n}$$

Nếu $r > 0$, thì $a^r + b^r < a^n + b^n$, nên không thể chia hết, mâu thuẫn. Vậy $r = 0 \implies m = kn$.

Ta kiểm tra điều kiện cần. Nếu k lẻ:

$$a^m + b^m = (a^n)^k + (b^n)^k \equiv -(a^n + b^n) \pmod{a^n + b^n} \implies \text{chia hết.}$$

Nếu k chẵn, thử với $a = -b$, thì:

$$a^m + b^m = 0, \quad a^n + b^n = 0 \implies \text{phân số không xác định.}$$

Kết luận: Tất cả các cặp thỏa mãn là:

$$\boxed{(m, n) = (kn, n) \quad \text{với } k \text{ lẻ}}.$$

[**10M**]. **Tham chiếu:** Định lý chia có dư. □

[15] Lời giải chính thức.

1.2.22. [ROU 2015 TST/D1/P4][16]

Đặt $a = \frac{1+\sqrt{k}}{2}$, với $k \equiv 1 \pmod 4$ và k không phải là số chính phương. Khi đó

$$a^2 = a + \frac{k-1}{4} = a + t, \quad \text{với } t \in \mathbb{Z}_{>0}.$$

Đặt $\varepsilon_n = an - \lfloor an \rfloor \in (0,1)$. Khi đó

$$a^2 n = an + tn = \lfloor an \rfloor + \varepsilon_n + tn.$$

Vậy

$$\lfloor a^2 n \rfloor = \lfloor an \rfloor + tn + \delta_n, \quad \delta_n \in \{0,1\}.$$

Đặt $m_n = \lfloor an \rfloor$. Khi đó

$$\lfloor am_n \rfloor = \lfloor a(\lfloor an \rfloor) \rfloor.$$

Vậy

$$\lfloor a^2 n \rfloor \; - \; \lfloor a \lfloor an \rfloor \rfloor = tn + \lfloor an \rfloor - \lfloor am_n \rfloor + \delta_n.$$

Vì a là vô tỷ, ε_n phân bố đều trong khoảng $(0,1)$, và $(a-1)\varepsilon_n$ cũng phân bố đều trong $(0, a-1)$. Do đó

$$\left\{ \lfloor a^2 n \rfloor - \lfloor a \lfloor an \rfloor \rfloor \; : \; n \in \mathbb{N}_{>0} \right\}$$

là tập hợp chính xác $\{1, 2, \ldots, \lfloor a \rfloor\}$, vì mỗi giá trị nguyên như vậy xuất hiện chính xác một lần nhờ vào sự phân bố đồng đều của các phần thập phân.

[**25M**]. **Tham chiếu:** Phân bố đều của phần thập phân số vô tỉ. □

1.2.23. [ROU 2015 TST/D2/P1][17]

Ta chứng minh khẳng định sau:

Khẳng định — Nếu p là số nguyên tố và $\gcd(a,p)=1$, thì:

$$a^{p^k} \equiv a^{p^{k-1}} \pmod{p^k}.$$

Chứng minh. Theo định lý Euler, $a^{\phi(p^k)} \equiv 1 \pmod{p^k}$, với $\phi(p^k) = p^{k-1}(p-1)$. Suy ra:

$$a^{p^k} = a^{p \cdot p^{k-1}} \equiv a^{p^{k-1}} \pmod{p^k}.$$

■

Trường hợp 1: $n = p^s$ là lũy thừa của số nguyên tố.

Theo GCD Power Sum Identity:

$$\sum_{k=1}^{p^s} a^{\gcd(k,p^s)} = \sum_{d \mid p^s} \varphi(d) \cdot a^{p^s/d}.$$

Các ước d là $p^0, p^1, \ldots, p^s$, do đó:

$$S = a^{p^s} + (p-1) \cdot a^{p^{s-1}} + (p^2 - p) \cdot a^{p^{s-2}} + \cdots + (p^s - p^{s-1}) \cdot a.$$

Ta chứng minh $p^s \mid S$ bằng quy nạp theo s:

- Cơ sở $s=1$: $a^p + (p-1)a = pa \equiv 0 \pmod{p}$.
- Bước quy nạp: Áp dụng bổ đề trên cho từng số hạng, suy ra $p^s \mid S$.

Trường hợp 2: n có ít nhất hai thừa số nguyên tố.

Giả sử $n = p^s m$ với $\gcd(p,m) = 1$. Khi đó:

$$\sum_{k=1}^{n} a^{\gcd(k,n)} = \sum_{d \mid n} \varphi(d) \cdot a^{n/d} = \sum_{\substack{d \mid n \\ p \nmid d}} \varphi(d) \cdot a^{n/d} + \sum_{\substack{d \mid n \\ p \mid d}} \varphi(d) \cdot a^{n/d}.$$

- Phần đầu chia hết cho m nhờ giả thiết quy nạp.
- Phần sau chia hết cho p^s theo kết quả ở Trường hợp 1.

Vì $\gcd(m, p^s) = 1$, theo Định lý số dư Trung Hoa, tổng chia hết cho $n = p^s m$.

$$\boxed{n \mid \sum_{k=1}^{n} a^{\gcd(k,n)}}$$

[25M] **Tham chiếu:** GCD Power Sum Identity. Định lý Euler. Định lý số dư Trung Hoa. □

[17] Dựa theo lời giải của **andria**.

1.2.24. [ROU 2015 TST/D3/P3][18]

Phần (a): Giả sử ngược lại rằng $f(n) \geq 3\sqrt{n}$. Đặt $s = \lfloor \sqrt{n} \rfloor$, và $a = s(s-1)$. Khi đó:

$$a = s(s-1) < s(s+1) \leq n \implies a < n.$$

Xét tập các số nguyên $\{a+1, a+2, \ldots, n\}$. Tập này chứa cả:

$$s^2 = s \cdot s > s(s-1) = a \Rightarrow s^2 \in [a+1, n],$$

và

$$(s+1)(s-1) = s^2 - 1 \Rightarrow s^2 - 1 \in [a+1, n].$$

Do đó, $M(n, n-a) = \text{lcm}(n, n-1, \ldots, a+1)$ chia hết cho s^2 và $s^2 - 1$, nên cũng chia hết cho $a = s(s-1)$.
Suy ra:

$$M(n, n-a+1) = \text{lcm}(M(n, n-a), a) = M(n, n-a),$$

mâu thuẫn với giả thiết rằng chuỗi $M(n,1) < M(n,2) < \ldots$. Vậy:

$$\boxed{f(n) < 3\sqrt{n}}.$$

Phần (b): Gọi $N \in \mathbb{N}_{>0}$. Ta chứng minh rằng nếu $n > N! + N$ thì $f(n) > N$.
Giả sử tồn tại $k \leq N$ sao cho:

$$M(n,k) = M(n,k+1).$$

Khi đó:

$$M(n,k+1) = \text{lcm}(M(n,k), n-k) = M(n,k) \Rightarrow (n-k) \mid M(n,k).$$

Mà $M(n,k) \mid n(n-1)\cdots(n-k+1)$, nên:

$$(n-k) \mid k!.$$

Tuy nhiên, nếu $n - k > N! \geq k!$, thì mâu thuẫn xảy ra.
Vậy với mọi $k \leq N$, ta đều có $M(n,k) < M(n,k+1) \Rightarrow f(n) > N$.
Từ đó suy ra:

$$\boxed{\text{Chỉ có hữu hạn } n \text{ sao cho } f(n) \leq N.}$$

[**30M**] **Tham chiếu:** Hàm số ước số dương. Hàm tổng ước số. Tính chất cơ bản của phép chia. □

[18] Dựa theo lời giải của **Aiscrim**.

1.2.25. [RUS 2015 TST/D10/P2][19]

Ta biết rằng:

$$\sum_{i=1}^{p-1} i = \frac{(p-1)p}{2} \equiv 1 \pmod p, \quad \prod_{i=1}^{p-1} i \equiv -1 \pmod p \quad \text{(Định lý Wilson)}$$

Gọi S là một tập con không rỗng của $\{1, 2, \ldots, p-1\}$. Khi đó, phần bù của S là $S^c = \{1, \ldots, p-1\} \setminus S$. Bài toán tương đương với việc tìm S sao cho:

$$\sum_{i \in S} i \equiv \prod_{j \in S^c} j \pmod p.$$

Đặt $A = \sum_{i \in S} i, \quad B = \prod_{i \in S} i$, khi đó:

$$\sum_{i \in S^c} i \equiv 1 - A \pmod p, \quad \prod_{i \in S^c} i \equiv \frac{-1}{B} \pmod p.$$

Ta sẽ xây dựng S thỏa mãn: $A \equiv \dfrac{-1}{B} \pmod p \iff AB \equiv -1 \pmod p$.

Trường hợp 1: Nếu $p \equiv 1 \pmod 4$. Khi đó tồn tại $a \in \mathbb{F}_p$ sao cho $a^2 \equiv -1 \pmod p$. Lấy $S = \{a\}$, ta có:

$$A = a, \quad B = a \Rightarrow AB = a^2 \equiv -1 \pmod p.$$

Trường hợp 2: Nếu $p \equiv 3 \pmod 4$, thì $p - 1 \equiv 2 \pmod 4$, nên tồn tại số nguyên tố lẻ $q \mid (p-1)$ (do $p \geq 5$). Khi đó, tồn tại phần tử sinh $a \in \mathbb{F}_p$ sao cho $\operatorname{ord}_p(a) = q$. Xét tập:

$$S = \left\{a^{\frac{q-1}{2}}, a^{\frac{q-3}{2}}, \ldots, a, a^{-1}, a^{-3}, \ldots, a^{-\frac{q-1}{2}}\right\}, \quad |S| = q - 1.$$

Các phần tử đi thành cặp nghịch đảo, nên tích của S là: $\displaystyle\prod_{i \in S} i \equiv 1 \pmod p$.

Ta nhân cả tổng với $a^{\frac{q-1}{2}}$, thu được:

$$a^{\frac{q-1}{2}} \sum_{i \in S} i = a^{q-1} + a^{q-2} + \cdots + 1 \equiv 0 \pmod p,$$

vì đây là tổng cấp số nhân với công bội a, số hạng q, nên tổng bằng $\frac{a^q - 1}{a - 1} \equiv 0 \pmod p$.

Do đó:

$$\sum_{i \in S} i \equiv -1 \pmod p, \quad \prod_{i \in S} i \equiv 1 \pmod p \Rightarrow AB \equiv -1 \pmod p.$$

[**25M**]. Định lý Wilson. Tổng cấp số nhân modulo p. Tồn tại căn bậc hai của -1. Tồn tại căn nguyên thủy. Cấu trúc nhóm nhân modulo p. Tính chất đồng dư theo bậc. Bậc của lũy thừa. □

[19] Dựa theo lời giải của **IAmTheHazard**.

1.2.26. [THA 2015 MO/P1][20] Từ giả thiết:

$$a_n a_{n+2} = a_{n+1}^2 + p, \quad a_{n+1}a_{n+3} = a_{n+2}^2 + p.$$

Trừ hai vế:

$$a_n a_{n+2} - a_{n+1}^2 = a_{n+1}a_{n+3} - a_{n+2}^2 \implies a_{n+2}(a_n + a_{n+2}) = a_{n+1}(a_{n+1} + a_{n+3}).$$

Giả sử $\gcd(a_{n+1}, a_{n+2}) = d > 1$. Từ:

$$a_n a_{n+2} = a_{n+1}^2 + p \implies d \mid p \implies d = p.$$

Xét tiếp:

$$a_{n+2}a_{n+4} = a_{n+3}^2 + p, \quad a_{n+1}a_{n+3} = a_{n+2}^2 + p.$$

Vì $p \mid a_{n+2}$, thì:

$$a_{n+2} \equiv 0 \pmod{p} \implies a_{n+2}^2 \equiv 0 \pmod{p^2} \implies a_{n+1}a_{n+3} \equiv p \pmod{p^2}.$$

Nhưng:

$$a_{n+1}, a_{n+3} \equiv 0 \pmod{p} \implies a_{n+1}a_{n+3} \equiv 0 \pmod{p^2} \implies p \equiv 0 \pmod{p^2}$$

là mâu thuẫn. Vậy $\gcd(a_{n+1}, a_{n+2}) = 1$.

Từ:

$$a_{n+2}(a_n + a_{n+2}) = a_{n+1}(a_{n+1} + a_{n+3})$$

và $\gcd(a_{n+1}, a_{n+2}) = 1 \implies a_{n+1} \mid a_n + a_{n+2}$

Kết luận: Ta đã chứng minh:

$$\boxed{a_{n+1} \mid a_n + a_{n+2} \quad \text{với mọi } n}$$

[**25M**]. **Tham chiếu:** Tính chất số nguyên tố. Chia hết trong tích khi nguyên tố cùng nhau. Nguyên lý phản chứng. □

[20] Lời giải của **rstenetbg**.

3.3 2023

1.3.1. [IMO 2023/P1](Cách 1)[21]

Trường hợp 1: Giả sử $n = p^r$. Khi đó $d_i = p^{i-1}$, và

$$d_i \mid d_{i+1} + d_{i+2} \Leftrightarrow p^{i-1} \mid p^i + p^{i+1} = p^i(1+p),$$

luôn đúng với mọi i. Vậy mọi lũy thừa của số nguyên tố đều thỏa mãn.

Trường hợp 2: Giả sử n có ít nhất hai thừa số nguyên tố. Gọi $p < q$ là hai thừa số nguyên tố nhỏ nhất. Khi đó tồn tại các ước số liên tiếp:

$$d_j = p^{j-1}, \quad d_{j+1} = p^j, \quad d_{j+2} = q.$$

Suy ra các ước số đối xứng:

$$d_{k-j-1} = \frac{n}{q}, \quad d_{k-j} = \frac{n}{p^j}, \quad d_{k-j+1} = \frac{n}{p^{j-1}}.$$

Từ giả thiết $d_{k-j-1} \mid d_{k-j} + d_{k-j+1}$, ta có:

$$\frac{n}{q} \,\Bigg|\, \left(\frac{n}{p^j} + \frac{n}{p^{j-1}}\right) \implies p^j \mid q(p+1) \implies p \mid q, \quad \text{mâu thuẫn vì } p \neq q.$$

Kết luận: n phải là lũy thừa của một số nguyên tố.

[**5M**]. **Tham chiếu:** Tính chất số nguyên tố. □

[21] Shortlist 2023 with solutions.

1.3.1. [IMO 2023/P1](Cách 2)[22]

Khẳng định — $d_i \mid d_{i+1}$ với mọi $1 \leq i \leq k-1$.

Chứng minh. Chứng minh bằng quy nạp.

Bước cơ sở: $d_1 = 1 \Rightarrow d_1 \mid d_2$.

Bước quy nạp: Giả sử $d_{i-1} \mid d_i$. Từ giả thiết:

$$d_{i-1} \mid d_i + d_{i+1} \implies d_{i-1} \mid d_{i+1}. \tag{1}$$

Xét các ước đối xứng:

$$\frac{d_{k-i} + d_{k-i+1}}{d_{k-i-1}} = \frac{\frac{n}{d_i} + \frac{n}{d_{i-1}}}{\frac{n}{d_{i+1}}} = \frac{d_{i+1}}{d_i} + \frac{d_{i+1}}{d_{i-1}}. \tag{2}$$

Do (2) là số nguyên, nên từ (1) suy ra $d_i \mid d_{i+1}$. ■

Do mọi ước d_i là bội của d_2 – ước nguyên tố nhỏ nhất của n – suy ra n là lũy thừa của một số nguyên tố.

[**5M**]. **Tham chiếu:** Tính chất số nguyên tố Nguyên lý quy nạp toán học. □

[22] Shortlist 2023 with solutions.

1.3.1. [IMO 2023/P1](Cách 3)[23]

Sử dụng đối xứng $d_i d_{k+1-i} = n$. Từ giả thiết:

$$d_{k-i-1} \mid d_{k-i} + d_{k-i+1} \implies \frac{n}{d_{i+2}} \,\Bigg|\, \left(\frac{n}{d_{i+1}} + \frac{n}{d_i}\right).$$

Nhân hai vế với $d_i d_{i+1} d_{i+2}$, ta có:

$$d_i d_{i+1} \mid d_i d_{i+2} + d_{i+1} d_{i+2} \implies d_i \mid d_{i+1} d_{i+2}. \tag{1}$$

Mặt khác, từ đề bài:

$$d_i \mid d_{i+1} + d_{i+2} \implies d_i \mid d_{i+1}^2 + d_{i+1} d_{i+2}. \tag{2}$$

Kết hợp (1) và (2) suy ra $d_i \mid d_{i+1}^2$.

Gọi $p = d_2$ là ước nguyên tố nhỏ nhất. Dùng quy nạp dễ dàng chứng minh được $p \mid d_i$ với mọi $i \geq 2$. Nếu tồn tại ước nguyên tố khác $q \neq p$, thì $p \mid q$, mâu thuẫn.

Kết luận: n là lũy thừa của một số nguyên tố.

[**5M**]. **Tham chiếu:** Tính chất số nguyên tố Nguyên lý quy nạp toán học. □

[23] Shortlist 2023 with solutions.

Phần IV

Công cụ

Chương 4

Định lý, bổ đề, và hằng đẳng thức

4.1 Các nguyên lý và chiến lược giải toán

Định lý 4.1.1 (Nguyên lý quy nạp toán học)

Giả sử $P(n)$ là một mệnh đề toán học xác định với mọi số nguyên $n \geq n_0$, trong đó n_0 là một số nguyên cố định. Nếu thỏa mãn:

- (Cơ sở quy nạp) $P(n_0)$ đúng;
- (Bước quy nạp) Với mọi $k \geq n_0$, nếu $P(k)$ đúng thì $P(k+1)$ cũng đúng,

thì $P(n)$ đúng với mọi $n \geq n_0$.

Định lý 4.1.2 (Nguyên lý Dirichlet)

Nếu có nhiều hơn n đối tượng được phân vào n ngăn, thì tồn tại ít nhất một ngăn chứa từ hai đối tượng trở lên.

Định lý 4.1.3 (Nguyên lý cực hạn)

Trong một tập hợp hữu hạn các đối tượng, nếu mỗi đối tượng được gán một giá trị theo tiêu chí nhất định, thì tồn tại phần tử đạt giá trị lớn nhất hoặc nhỏ nhất (gọi là phần tử cực đại hoặc cực tiểu).

Việc chọn phần tử như vậy (cực đại hoặc cực tiểu) thường giúp đơn giản hóa bài toán hoặc dẫn đến mâu thuẫn khi giả sử ngược.

Định lý 4.1.4 (Nguyên lý bất biến)

Trong một quá trình gồm nhiều bước biến đổi, nếu tồn tại một đại lượng không thay đổi qua mỗi bước (gọi là bất biến), thì có thể dùng bất biến đó để suy ra tính chất hoặc kết thúc của quá trình.

Nguyên lý này đặc biệt hữu ích để chứng minh rằng một trạng thái nào đó là không thể đạt được, hoặc rằng quá trình phải dừng sau hữu hạn bước.

Định lý 4.1.5 (Nguyên lý đổi biến đơn điệu)

Giả sử trong một quá trình, có một đại lượng luôn tăng hoặc luôn giảm qua mỗi bước (gọi là biến đơn điệu, hay monovariant), và đại lượng đó bị chặn, thì quá trình phải kết thúc sau hữu hạn bước.

Nguyên lý này thường dùng để chứng minh một quá trình không thể tiếp diễn vô hạn.

Định lý 4.1.6 (Nguyên lý phản chứng)

Để chứng minh một mệnh đề P là đúng, ta có thể giả sử rằng P sai và từ đó suy ra một mâu thuẫn logic. Khi đó, kết luận rằng P là đúng.

Đây là một trong những phương pháp chứng minh phổ biến và hiệu quả nhất trong toán học.

Định lý 4.1.7 (Chiến lược xét chẵn/lẻ)

Trong các bài toán liên quan đến số nguyên, việc phân tích tính chẵn/lẻ (parity) của các đại lượng có thể giúp phát hiện các mâu thuẫn hoặc bất biến, từ đó giải được bài toán.

Tính chẵn/lẻ là một dạng đặc biệt của bất biến hoặc monovariant.

4.2 Các định lý giải tích

Bổ đề 4.2.1 (Tính phân kỳ của chuỗi điều hoà)
Chuỗi điều hoà $H_n = \sum_{k=1}^{n} \frac{1}{k}$ tăng mà không bị chặn, tức là:

$$\lim_{n\to\infty} H_n = \infty.$$

Ngoài ra, với mọi $n \geq 1$, ta có đánh giá gần đúng:

$$\log n < H_n < 1 + \log n.$$

4.3 Số nguyên tố và phép chia hết

Định nghĩa 4.3.1 (Số nguyên tố)**.** Một số nguyên $p > 1$ được gọi là **số nguyên tố** nếu p chỉ có đúng hai ước dương là 1 và p (tức là không chia hết cho số nguyên dương nào khác ngoài 1 và chính nó).

Định nghĩa 4.3.2 (Hợp số)**.** Một số nguyên $n > 1$ được gọi là **hợp số** nếu tồn tại một số nguyên dương d sao cho $1 < d < n$ và $d \mid n$ (tức là n có ước khác ngoài 1 và chính nó).

Định lý 4.3.3 (Định lý cơ bản của số học)
Mọi số tự nhiên lớn hơn 1 có thể viết một cách duy nhất (không kể sự sai khác về thứ tự các thừa số) thành tích các thừa số nguyên tố:
$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$
với p_i là các số nguyên tố khác nhau và $\alpha_i \in \mathbb{Z}^+$.

Định lý 4.3.4 (Định lý Euclid)
Có vô số số nguyên tố. Cụ thể, với bất kỳ tập hữu hạn các số nguyên tố $p_1, p_2, \dots, p_k$, tồn tại số nguyên tố p không thuộc tập đó.

Định lý 4.3.5 (Định lý Bertrand)
Với mọi số nguyên $n > 1$, tồn tại số nguyên tố p sao cho:
$$n < p < 2n.$$

Định lý 4.3.6 (Định lý số nguyên tố — dạng yếu)
Hàm đếm số nguyên tố $\pi(n)$ thỏa mãn:
$$\pi(n) \sim \frac{n}{\log n}, \quad \text{và } \pi(n) < \frac{1.25506n}{\log n}.$$

Định lý 4.3.7 (Tính chất cơ bản của phép chia)
Với các số nguyên x, y, z, ta có:

- $x \mid x$, $1 \mid x$, $x \mid 0$
- Nếu $x \mid y$ và $y \mid z$ thì $x \mid z$
- Nếu $x \mid y$ thì tồn tại $k \in \mathbb{Z}$ sao cho $y = kx$
- Nếu $x \mid y$ thì $x \mid yz$ với mọi z
- Nếu $x \mid y$ và $x \mid z$ thì $x \mid (ay + bz)$ với mọi $a, b \in \mathbb{Z}$
- Nếu $x \mid y$ và $y \mid x$ thì $x = \pm y$

Định lý 4.3.8 (Tính chất gcd và lcm)

Với $a, b \in \mathbb{Z}^+$, ta có:

$$\gcd(a, b) \cdot \text{lcm}(a, b) = ab.$$

Ngoài ra:

- $\gcd(a, b) \mid a$ và $\gcd(a, b) \mid b$
- $\text{lcm}(a, b)$ là bội chung nhỏ nhất

Định lý 4.3.9 (Định lý chia có dư)

Với $a \in \mathbb{Z}$ và $b \in \mathbb{Z}^+$, tồn tại duy nhất $q, r \in \mathbb{Z}$ sao cho:

$$a = bq + r, \quad 0 \le r < b.$$

Định lý 4.3.10 (Thuật toán Euclid)

Thuật toán tìm $\gcd(a, b)$ dựa vào lặp lại định lý chia:

$$\gcd(a, b) = \gcd(b, a \bmod b).$$

Định lý 4.3.11 (Định lý Bézout)

Với $a, b \in \mathbb{Z}$, tồn tại $x, y \in \mathbb{Z}$ sao cho:

$$ax + by = \gcd(a, b).$$

Định lý 4.3.12 (Tính chất số nguyên tố)

Nếu p là số nguyên tố và $p \mid ab$, thì $p \mid a$ hoặc $p \mid b$.

Định lý (Chia hết trong tích khi nguyên tố cùng nhau)

Nếu $a \mid bc$ và $\gcd(a, b) = 1$, thì $a \mid c$.

Bổ đề 4.3.13 (Biểu diễn số có các chữ số 1)

Với mọi số nguyên dương n, ta có:

$$\underbrace{11\ldots1}_{n \text{ chữ số } 1} = \frac{10^n - 1}{9}.$$

4.4 Số học đồng dư cơ bản

Định nghĩa 4.4.1 (Đồng dư modulo n). Với $a, b, n \in \mathbb{Z}$, ta nói $a \equiv b \pmod{n}$ khi $n \mid (a-b)$.

Định lý 4.4.2 (Tính chất đại số của phép đồng dư)
Với $a \equiv r \pmod{n}$ và $b \equiv s \pmod{n}$, ta có:

- $a + b \equiv r + s \pmod{n}$
- $ab \equiv rs \pmod{n}$
- $ka \equiv kr \pmod{n}$ với mọi $k \in \mathbb{Z}$

Định lý 4.4.3 (Ước nguyên tố dạng $4k+3$)
Mỗi số nguyên dương có dạng $4s+3$ đều có ít nhất một ước nguyên tố cũng có dạng đó, tức là $\equiv -1 \pmod{4}$ (see Định lý Dirichlet về cấp số cộng nguyên tố).

Định lý 4.4.4 (Định lý nhỏ Fermat)
Nếu p là số nguyên tố và $\gcd(a, p) = 1$, thì:

$$a^{p-1} \equiv 1 \pmod{p}.$$

Hệ quả: $a^p \equiv a \pmod{p}$ với mọi $a \in \mathbb{Z}$.

Định lý 4.4.5 (Định lý số dư Trung Hoa)
Cho các số nguyên $n_1, \ldots, n_k$ đôi một nguyên tố cùng nhau và các số nguyên $a_1, \ldots, a_k$, tồn tại duy nhất $x \mod N = n_1 n_2 \cdots n_k$ sao cho:

$$x \equiv a_i \pmod{n_i}, \quad \forall i.$$

Định lý 4.4.6 (Định lý Euler)
Với $\gcd(a, n) = 1$, ta có:

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Định lý 4.4.7 (Định lý Wilson)
Với số nguyên tố p, ta có:

$$(p-1)! \equiv -1 \pmod{p}.$$

Định lý 4.4.8 (Hủy nhân trong đồng dư)

Nếu $ad \equiv bd \pmod{n}$, thì:

$$a \equiv b \pmod{\frac{n}{\gcd(d, n)}}.$$

Định lý 4.4.9 (Định lý Dirichlet về cấp số cộng nguyên tố)

Cho hai số nguyên dương a và d sao cho $\gcd(a, d) = 1$. Khi đó, cấp số cộng $a, a+d, a+2d, a+3d, \ldots$ chứa vô hạn số nguyên tố.

4.5 Các hàm số học

Định nghĩa 4.5.1 (Hàm số ước số dương)**.** Với $n = p_1^{a_1} \cdots p_k^{a_k}$, ta có:

$$\tau(n) = (1 + a_1)(1 + a_2) \cdots (1 + a_k).$$

Hàm này đếm số ước dương của n. Cũng được ký hiệu là $d(n)$.

Định nghĩa 4.5.2 (Hàm tổng ước số)**.** Với $n = p_1^{a_1} \cdots p_k^{a_k}$, ta có:

$$\sigma(n) = (1 + p_1 + \cdots + p_1^{a_1}) \cdots (1 + p_k + \cdots + p_k^{a_k}).$$

Đây là tổng các ước dương của n.

Định nghĩa 4.5.3 (Hàm phi Euler)**.** Với $n = p_1^{a_1} \cdots p_k^{a_k}$, ta có:

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

Hàm này đếm số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n.

Định nghĩa 4.5.4 (Hàm Möbius)**.** Với $n \in \mathbb{Z}^+$, định nghĩa:

$$\mu(n) = \begin{cases} 1 & \text{nếu } n = 1, \\ (-1)^k & \text{nếu } n \text{ là tích của } k \text{ số nguyên tố phân biệt}, \\ 0 & \text{nếu } n \text{ chia hết bình phương của số nguyên tố.} \end{cases}$$

Định lý 4.5.5 (GCD Power Sum Identity)

For any positive integer n and any real or complex number a, we have

$$\sum_{k=1}^{n} a^{\gcd(k,n)} = \sum_{d|n} \phi(d)\, a^{n/d}.$$

Định nghĩa 4.5.6 (Phép nhân Dirichlet)**.** Với hai hàm số số học $f, g\colon \mathbb{Z}^+ \to \mathbb{R}$, định nghĩa:

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d).$$

Định lý 4.5.7 (Đẳng thức $\tau = 1 * 1$)

Hàm $\tau(n)$ là tích Dirichlet của hai hàm hằng:

$$\tau(n) = \sum_{d|n} 1 = (1 * 1)(n).$$

Định lý 4.5.8 (Đẳng thức $\sigma = \mathrm{id} * 1$)
Hàm tổng ước $\sigma(n)$ là tích Dirichlet của hàm đồng nhất và hàm hằng:

$$\sigma(n) = \sum_{d|n} d = (\mathrm{id} * 1)(n).$$

Định lý 4.5.9 (Tổng $\mu(d)$ trên các ước)
Với mọi $n \in \mathbb{Z}^+$, ta có:

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{nếu } n = 1, \\ 0 & \text{nếu } n > 1. \end{cases}$$

Định lý 4.5.10 (Nghịch đảo Möbius tổng quát)
Nếu $f(n) = \sum_{d|n} g(d)$, thì:

$$g(n) = \sum_{d|n} \mu(d) f(n/d).$$

Định lý 4.5.11 (Bất đẳng thức cho $\varphi(n)$)
Với $n \geq 3$, ta có:

$$\frac{n}{\log \log n} < \varphi(n) < n.$$

Định lý 4.5.12 (Tổng các giá trị $\varphi(n)$)
Khi $x \to \infty$, ta có:

$$\sum_{n \leq x} \varphi(n) \sim \frac{3}{\pi^2} x^2.$$

Định lý (Tổng các số nguyên tố cùng nhau với m)
Gọi T là tổng các số nguyên dương nhỏ hơn m và nguyên tố cùng nhau với m, thì ta có:

$$T = \frac{m\varphi(m)}{2}.$$

4.6 Phương trình nghiệm nguyên

Định lý 4.6.1 (Đẳng thức Simon yêu thích)
Với các biểu thức như $xy + ax + by + c$, ta có:

$$xy + ax + by + c = (x + a)(y + b) + (c - ab).$$

Được dùng để đưa phương trình hai biến về dạng tích.

Bổ đề 4.6.2 (Nguyên lý hạ vô hạn (Infinite Descent))
Nếu tồn tại dãy vô hạn các số nguyên dương $x_0 > x_1 > x_2 > \cdots$ mà mỗi x_i thỏa mãn tính chất P, thì có mâu thuẫn. Do đó, giả thiết ban đầu là sai.

Định lý 4.6.3 (Monovariant $S = |x| + |y| + |z|$)
Nếu một quá trình biến đổi bộ số nguyên luôn làm giảm hoặc giữ nguyên $S = |x| + |y| + |z|$ và $S \in \mathbb{Z}_{\geq 0}$, thì quá trình phải kết thúc sau hữu hạn bước.

Định lý 4.6.4 (Kỹ thuật Vieta Jumping)
Với phương trình đối xứng $P(x, y) = 0$, nếu (a, b) là nghiệm nguyên và $x^2 - (a+b)x + ab = 0$, thì nghiệm còn lại x' cũng là nghiệm. Nếu $x' < a$, ta có thể sử dụng Vieta Jumping để tìm nghiệm nhỏ hơn — dẫn đến mâu thuẫn.

Bổ đề 4.6.5 (Mâu thuẫn đồng dư)
Nếu giả sử $a \equiv b \pmod{p}$ nhưng rút ra $a \equiv c \not\equiv b \pmod{p}$, thì mâu thuẫn xảy ra. Kỹ thuật dùng để loại nghiệm.

Định lý 4.6.6 (Định lý Fermat Giáng Sinh)
Phương trình:

$$x^4 + y^4 = z^2$$

không có nghiệm nguyên dương khác 0.

4.7 Phân bố đều và số vô tỉ

Bổ đề 4.7.1 (Phân bố đều của phần thập phân số vô tỉ)
Cho $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Khi đó dãy $\{n\alpha\}$ phân bố đều trên khoảng $(0, 1)$, tức là với mọi $0 \leq a < b \leq 1$, ta có:

$$\lim_{N\to\infty} \frac{1}{N} \left|\{1 \leq n \leq N : \{n\alpha\} \in [a, b)\}\right| = b - a.$$

Ở đây $\{x\} = x - \lfloor x \rfloor$ là phần thập phân của x.

4.8 Căn nguyên thủy và đẳng thức cổ điển

Định nghĩa 4.8.1 (Bậc modulo n)**.** Với $a \in \mathbb{Z}$, $\gcd(a,n) = 1$, bậc của a modulo n, ký hiệu $\mathrm{ord}_n(a)$, là số nguyên dương nhỏ nhất d sao cho:

$$a^d \equiv 1 \pmod{n}.$$

Định lý 4.8.2 (Tính chia hết của bậc)
Nếu $a^k \equiv 1 \pmod{n}$, thì $\mathrm{ord}_n(a) \mid k$.

Bổ đề 4.8.3 (Tính chất đồng dư theo bậc)
Nếu $\mathrm{ord}_n(a) = d$, thì:

$$a^i \equiv a^j \pmod{n} \iff i \equiv j \pmod{d}.$$

Bổ đề 4.8.4 (Tổng Euler lũy thừa theo modulo)
Với mọi số nguyên tố p và số nguyên $j \geq 1$, và với mọi $x \in \mathbb{Z}$, ta có:

$$\sum_{k=0}^{j} \phi\left(p^k\right) x^{p^{j-k}} \equiv 0 \pmod{p^j}.$$

Định nghĩa 4.8.5 (Căn nguyên thủy)**.** Một số $g \in \mathbb{Z}$ được gọi là căn nguyên thủy modulo n nếu:

$$\mathrm{ord}_n(g) = \varphi(n).$$

Khi đó g sinh ra nhóm $(\mathbb{Z}/n\mathbb{Z})^\times$.

Định lý 4.8.6 (Tồn tại căn nguyên thủy)
Căn nguyên thủy tồn tại nếu và chỉ nếu:

$$n = 1,\ 2,\ 4,\ p^k,\ 2p^k \text{ với } p \text{ là số nguyên tố lẻ.}$$

Bổ đề 4.8.7 (Bậc của lũy thừa)
Nếu $\mathrm{ord}_n(a) = d$, thì:

$$\mathrm{ord}_n(a^k) = \frac{d}{\gcd(k,d)}.$$

Định lý 4.8.8 (Đẳng thức Sophie Germain)

Với mọi $a, b \in \mathbb{Z}$, ta có:

$$a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab).$$

4.9 Chuẩn p-adic và định lý LTE

Định nghĩa 4.9.1 (Chuẩn p-adic)**.** Với p là số nguyên tố và $n \in \mathbb{Z}$, định nghĩa:

$$\nu_p(n) = \begin{cases} \max\{k \in \mathbb{N}_0 : p^k \mid n\} & \text{nếu } n \neq 0, \\ \infty & \text{nếu } n = 0. \end{cases}$$

Định lý 4.9.2 (Tính chất cơ bản của ν_p)

Với $a, b \in \mathbb{Z}$, ta có:

- $\nu_p(ab) = \nu_p(a) + \nu_p(b)$
- $\nu_p(a^k) = k\nu_p(a)$
- $\nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b)$
- $\nu_p(a+b) \geq \min\{\nu_p(a), \nu_p(b)\}$

Dấu bằng xảy ra nếu $\nu_p(a) \neq \nu_p(b)$.

Định lý 4.9.3 (Định lý LTE cho hiệu — $p \mid x - y$)

Cho $x, y \in \mathbb{Z}$, p là số nguyên tố lẻ, $n \in \mathbb{Z}^+$, nếu $p \mid x - y$ và $p \nmid xy$, thì:

$$\nu_p(x^n - y^n) = \nu_p(x - y) + \nu_p(n).$$

Định lý 4.9.4 (Định lý LTE cho tổng — $p \mid x + y$)

Cho $p > 2$ là số nguyên tố, $x, y \in \mathbb{Z}$, $p \mid x + y$, và $p \nmid xy$. Khi đó với n lẻ:

$$\nu_p(x^n + y^n) = \nu_p(x + y) + \nu_p(n).$$

Định lý 4.9.5 (Định lý LTE cho $\nu_2(x^n - 1)$)

Với $x \in \mathbb{Z}$ lẻ và $n \in \mathbb{Z}^+$, ta có:

$$\nu_2(x^n - 1) = \nu_2(x - 1) + \nu_2(x + 1) + \nu_2(n) - 1.$$

Định lý 4.9.6 (Định lý Zsigmondy)

Nếu $a > b > 0$, $\gcd(a, b) = 1$, và $n > 1$, thì tồn tại ước nguyên tố của $a^n - b^n$ không chia $a^k - b^k$ với $k < n$, trừ các ngoại lệ:

$$(a, b, n) = (2, 1, 6), \text{ hoặc } a + b \text{ là lũy thừa của 2 và } n = 2.$$

4.10 Đa thức

Định lý 4.10.1 (Định lý nghiệm hữu tỉ)
Nếu $P(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ có nghiệm hữu tỉ $\frac{r}{s}$ với $\gcd(r, s) = 1$, thì:

$$r \mid a_0, \quad s \mid a_n.$$

Định lý 4.10.2 (Định lý chia đa thức)
Với $F(x), G(x) \in \mathbb{Z}[x]$, tồn tại duy nhất $Q(x), R(x) \in \mathbb{Z}[x]$ sao cho:

$$F(x) = G(x)Q(x) + R(x), \quad \deg R < \deg G.$$

Định lý 4.10.3 (Nội suy Lagrange)
Cho $n+1$ điểm phân biệt $(x_0, y_0), \ldots, (x_n, y_n) \in \mathbb{R}^2$, tồn tại một đa thức $P(x) \in \mathbb{R}[x]$, bậc không vượt quá n, sao cho $P(x_i) = y_i$ với mọi i. Cụ thể:

$$P(x) = \sum_{i=0}^{n} y_i \prod_{\substack{0 \le j \le n \\ j \ne i}} \frac{x - x_j}{x_i - x_j}.$$

Bổ đề 4.10.4 (Đồng dư đa thức theo hiệu)
Nếu $a \equiv b \pmod{a-b}$, thì với mọi đa thức $P(x) \in \mathbb{Z}[x]$, ta có:

$$P(a) \equiv P(b) \pmod{a-b}.$$

Định lý 4.10.5 (Định lý cơ bản của đại số — dạng thực)
Mọi đa thức hệ số thực bậc ít nhất 1 có thể phân tích thành tích của các đa thức bậc nhất hoặc bậc hai không khả quy trong $\mathbb{R}[x]$.

Định lý 4.10.6 (Định lý Lucas)
Cho số nguyên tố p và $m, n \in \mathbb{Z}_{\ge 0}$, viết:

$$m = m_0 + m_1 p + \cdots + m_k p^k, \quad n = n_0 + n_1 p + \cdots + n_k p^k,$$

thì:

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p}.$$

Định lý 4.10.7 (Đẳng thức Vandermonde)

Với $m, n, r \in \mathbb{Z}^+$, ta có:

$$\sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k} = \binom{m+n}{r}.$$

4.11 Số dư bậc hai và ký hiệu Legendre

Định nghĩa 4.11.1 (Ký hiệu Legendre)**.** Với số nguyên tố lẻ p và $a \in \mathbb{Z}$, định nghĩa:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{nếu } p \mid a, \\ 1 & \text{nếu } a \not\equiv 0 \pmod p \text{ và } \exists x \in \mathbb{Z} : x^2 \equiv a \pmod p, \\ -1 & \text{nếu } a \text{ không là bình phương chính phương modulo } p. \end{cases}$$

Định lý 4.11.2 (Tính chất của ký hiệu Legendre)
Với $a, b \in \mathbb{Z}$ và số nguyên tố lẻ p, ta có:

- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
- $\left(\frac{a^2}{p}\right) = 1$ nếu $p \nmid a$
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Định lý 4.11.3 (Tổng cấp số nhân modulo p)
Cho số nguyên tố p, và $a \in \mathbb{Z} \setminus \{1\}$ sao cho $a^k \equiv 1 \pmod p$, ta có:

$$\sum_{i=0}^{k-1} a^i \equiv 0 \pmod p.$$

Đây là tổng của một cấp số nhân bậc k với công bội $a \not\equiv 1 \pmod p$ trong $\mathbb{F}_p$.

Định lý 4.11.4 (Tồn tại căn bậc hai của -1)
Với số nguyên tố lẻ p, ta có:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{nếu } p \equiv 1 \pmod 4, \\ -1 & \text{nếu } p \equiv 3 \pmod 4. \end{cases}$$

Do đó, -1 là số chính phương modulo p khi và chỉ khi $p \equiv 1 \pmod 4$.

Định lý 4.11.5 (Định luật tương hỗ bậc hai)
Với hai số nguyên tố lẻ phân biệt p, q, ta có:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Hệ quả (Tổng Legendre bằng 0)
Với số nguyên tố lẻ p, ta có:
$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0.$$

Định lý 4.11.6 (Ước lượng số dư bậc hai nhỏ nhất)
Với số nguyên tố $p > 3$, tồn tại số nguyên $r \in \{2, 3, \dots, \lfloor\sqrt{p}\rfloor + 1\}$ sao cho r không là số dư bậc hai modulo p. Do đó:
$$r < \sqrt{p} + 1.$$

4.12 Căn nguyên thủy và bậc lũy thừa (phần nâng cao)

Bổ đề 4.12.1 (Tồn tại phần tử bậc d)
Nếu $d \mid p-1$, thì tồn tại $a \in \mathbb{Z}$ sao cho:

$$\mathrm{ord}_p(a) = d.$$

Có chính xác $\varphi(d)$ phần tử như vậy trong $(\mathbb{Z}/p\mathbb{Z})^\times$.

Định lý 4.12.2 (Tập các phần tử bậc d)
Nếu $d \mid p-1$, thì tập các phần tử bậc d trong $(\mathbb{Z}/p\mathbb{Z})^\times$ có đúng $\varphi(d)$ phần tử. Hợp của các tập này (khi $d \mid p-1$) chính là toàn bộ nhóm $(\mathbb{Z}/p\mathbb{Z})^\times$.

Định lý 4.12.3 (Các nghiệm của $x^d \equiv 1 \pmod p$)
Với $d \mid p-1$, phương trình $x^d \equiv 1 \pmod p$ có đúng d nghiệm phân biệt modulo p, tạo thành một nhóm con cyclic của $(\mathbb{Z}/p\mathbb{Z})^\times$.

Bổ đề 4.12.4 (Tính chia hết qua bậc)
Nếu $a^k \equiv 1 \pmod p$, thì $\mathrm{ord}_p(a) \mid k$.

Định lý 4.12.5 (Cấu trúc nhóm nhân modulo p)
Với số nguyên tố p, nhóm $(\mathbb{Z}/p\mathbb{Z})^\times$ là cyclic cấp $p-1$, tức là tồn tại $g \in \mathbb{Z}$ sao cho:

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{g^1, g^2, \ldots, g^{p-1}\}.$$

Bổ đề 4.12.6 (Rút gọn đồng dư theo mũ)
Nếu $a^k \equiv b^k \pmod p$ và $\gcd(k, p-1) = 1$, thì:

$$a \equiv b \pmod p.$$

4.13 Bậc lũy thừa theo hợp số

Định nghĩa 4.13.1 (Hàm Carmichael)**.** Hàm Carmichael $\lambda(n)$ là số nguyên dương nhỏ nhất sao cho:

$$a^{\lambda(n)} \equiv 1 \pmod{n} \quad \text{với mọi } a \in \mathbb{Z} \text{ sao cho } \gcd(a, n) = 1.$$

Nếu $n = \operatorname{lcm}(m_1, \ldots, m_k)$, thì:

$$\lambda(n) = \operatorname{lcm}(\lambda(m_1), \ldots, \lambda(m_k)).$$

Với số nguyên tố p, ta có:

$$\lambda(p^e) = \begin{cases} \varphi(p^e) & \text{nếu } p \text{ lẻ, hoặc } p = 2, e \leq 2, \\ \frac{1}{2}\varphi(p^e) & \text{nếu } p = 2, e \geq 3. \end{cases}$$

Định lý 4.13.2 (Bậc modulo hợp số)

Với $a \in \mathbb{Z}$, $\gcd(a, n) = 1$, ta có:

$$\operatorname{ord}_n(a) \mid \lambda(n), \quad \text{và } a^{\operatorname{ord}_n(a)} \equiv 1 \pmod{n}.$$

Bổ đề 4.13.3 (Bậc modulo tích các lũy thừa số nguyên tố)

Nếu $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, và $\gcd(a, n) = 1$, thì:

$$\operatorname{ord}_n(a) = \operatorname{lcm}\big(\operatorname{ord}_{p_1^{e_1}}(a),\ \operatorname{ord}_{p_2^{e_2}}(a),\ \ldots,\ \operatorname{ord}_{p_k^{e_k}}(a)\big).$$

4.14 Thủ thuật, kỹ thuật và công cụ hiếm gặp

Định lý 4.14.1 (Trung bình số ước)
Gọi $d(k)$ là số ước dương của k. Khi đó:

$$\log n - 1 \leq \frac{1}{n}\sum_{k=1}^{n} d(k) \leq \log n + 1.$$

Tức là trung bình số ước thỏa $\Theta(\log n)$.

Định lý 4.14.2 (Tổng tất cả các ước từ 1 đến n)
Ta có:

$$\sum_{i=1}^{n} \sigma(i) = \sum_{i=1}^{n} i \left\lfloor \frac{n}{i} \right\rfloor.$$

Đây là tổng các ước dương của tất cả các số từ 1 đến n.

Định lý 4.14.3 (Ma trận ước số $D_{i,j}$)
Xét bảng D cấp $n \times n$ với phần tử:

$$D_{i,j} = \begin{cases} 1 & \text{nếu } j \mid i, \\ 0 & \text{ngược lại.} \end{cases}$$

Tổng theo hàng thứ i là $\tau(i)$, tổng theo cột thứ j là $\left\lfloor \frac{n}{j} \right\rfloor$.

Định lý 4.14.4 (Tổng nghịch đảo ước số)
Với mọi $n \geq 1$, ta có:

$$\sum_{d|n} \frac{1}{d} \leq \log n + 1.$$

Chương 5

Xếp hạng

Thang độ khó MOHS

Trong tài liệu này, Evan Chen cung cấp xếp hạng độ khó cá nhân cho các bài toán từ một số kỳ thi gần đây. Điều này đòi hỏi phải xác định một tiêu chí đánh giá độ khó một cách cẩn thận. Evan Chen gọi hệ thống này là **thang độ khó MOHS** (phát âm là "moez"); đôi khi anh cũng sử dụng đơn vị "M" (viết tắt của "Mohs").

Thang đo này tiến hành theo bước nhảy 5M, với mức thấp nhất là 0M và mức cao nhất là 60M. Tuy nhiên, trên thực tế, rất ít bài toán được xếp hạng cao hơn 50M, nên có thể coi nó chủ yếu là một thang đo từ 0M đến 50M, với một số bài toán thuộc dạng "vượt mức thông thường".

Bên dưới là bản dịch tiếng Việt từ tài liêu trên.

Xếp hạng dựa theo ý kiến cá nhân của Evan Chen

Mặc dù có rất nhiều điều đã được viết ra ở đây, nhưng cuối cùng, những xếp hạng này vẫn chỉ là ý kiến cá nhân của Evan Chen. Evan Chen không khẳng định rằng các xếp hạng này là khách quan hoặc phản ánh một sự thật tuyệt đối nào đó.

Lưu ý hài hước (Bảo hành xếp hạng). Các xếp hạng được cung cấp "nguyên trạng", không có bất kỳ bảo hành nào, dù rõ ràng hay ngụ ý, bao gồm nhưng không giới hạn ở các bảo hành về khả năng thương mại, sự phù hợp với một mục đích cụ thể, và việc không vi phạm quyền sở hữu trí tuệ. Trong mọi trường hợp, Evan không chịu trách nhiệm đối với bất kỳ khiếu nại, thiệt hại hoặc trách nhiệm pháp lý nào phát sinh từ, liên quan đến, hoặc có liên quan đến những xếp hạng này.

Hướng dẫn sử dụng

Cảnh báo quan trọng: Lạm dụng các xếp hạng này có thể gây hại cho bạn.

Ví dụ, nếu bạn quyết định không nghiêm túc thử sức với một số bài toán chỉ vì chúng được xếp hạng 40M trở lên, bạn có thể tự làm khó mình bằng cách tước đi cơ hội tiếp xúc với những bài toán khó. Nếu bạn không thường xuyên thử sức với các bài toán cấp độ IMO3 một cách nghiêm túc, bạn sẽ không bao giờ đạt đến mức độ có thể thực sự giải được chúng.

Vì lý do này, nghịch lý thay, đôi khi việc không biết bài toán khó đến mức nào lại tốt hơn, để bạn không vô thức có thái độ bỏ cuộc ngay từ đầu.

Các xếp hạng này được thiết kế để làm tài liệu tham khảo. Một cách sử dụng hợp lý là không xem xếp hạng bài toán cho đến khi bạn đã giải xong; điều này mô phỏng tốt nhất điều kiện thi đấu thực tế, khi bạn không biết độ khó của bài toán cho đến khi bạn giải được nó hoặc hết giờ và thấy những ai khác đã giải được. Bạn đã được cảnh báo. Chúc may mắn!

Ý nghĩa của các mức xếp hạng bài toán

Dưới đây là ý nghĩa của từng mức độ xếp hạng bài toán theo thang đo MOHS.

Định nghĩa (0M)**.** Bài toán có mức 0M quá dễ để xuất hiện trong IMO. Thông thường, một học sinh giỏi trong lớp toán nâng cao có thể giải được bài toán này mà không cần đào tạo chuyên sâu về toán olympic.

Định nghĩa (5M)**.** Đây là mức dễ nhất có thể xuất hiện trong IMO nhưng vẫn đáp ứng tiêu chuẩn của kỳ thi. Những bài toán này có thể được giải quyết rất nhanh.

Ví dụ:

- IMO 2019/1 về phương trình $f(2a) + 2f(b) = f(f(a + b))$
- IMO 2017/1 về căn bậc hai $\sqrt{a_n}$ hoặc $a_n + 3$

Định nghĩa (10M)**.** Đây là mức độ dành cho các bài toán IMO số 1 hoặc 4 mà hầu hết các thí sinh không gặp khó khăn khi giải. Tuy nhiên, vẫn cần có một số công việc để hoàn thành lời giải.

Ví dụ:

- IMO 2019/4 về $k! = (2^n - 1) \dots$
- IMO 2018/1 về $DE \parallel FG$

Định nghĩa (15M)**.** Đây là mức thấp nhất của các bài toán có thể xuất hiện dưới dạng bài số 2 hoặc 5 của IMO, nhưng thường phù hợp hơn với bài số 1 hoặc 4. Những bài toán này thường có thể được giải quyết dễ dàng bởi các đội tuyển thuộc top 10 thế giới.

Ví dụ:

- IMO 2019/5 về bài toán "Ngân hàng Bath"
- IMO 2018/4 về "Amy/Ben và lưới 20×20"
- IMO 2017/4 về tiếp tuyến KT của Γ

Định nghĩa (20M)**.** Những bài toán ở mức này có thể quá khó để xuất hiện dưới dạng IMO 1/4 nhưng vẫn chưa đạt đến độ khó trung bình của IMO 2/5.

Ví dụ:

- IMO 2018/5 về $a_1, a_2, \dots, a_n$ sao cho $\frac{a_1}{a_2} + \dots + \frac{a_n}{a_1} \in \mathbb{Z}$

Định nghĩa (25M)**.** Đây là mức độ phù hợp nhất với các bài toán IMO 2/5. Những bài toán này là thử thách thực sự ngay cả với các đội tuyển hàng đầu.

Ví dụ:

- IMO 2019/2 về "P_1, Q_1, P, Q đồng viên"

Định nghĩa (30M)**.** Những bài toán ở mức này khó hơn một chút so với mức trung bình của IMO 2/5, nhưng vẫn chưa đủ khó để được sử dụng làm bài số 3 hoặc 6.

Ví dụ:

- IMO 2018/2 về phương trình $a_i a_{i+1} + 1 = a_{i+2}$

Định nghĩa (35M)**.** Đây là mức độ khó cao nhất dành cho các bài toán IMO 2/5 và cũng là mức độ dễ nhất của các bài toán IMO 3/6.

Ví dụ:

- IMO 2019/6 về "$DI \cap PQ$ trên phân giác góc ngoài $\angle A$"
- IMO 2017/5 về "Ngài Alex và các cầu thủ bóng đá"

Định nghĩa (40M). Những bài toán ở mức này quá khó để xuất hiện ở IMO 2/5. Ngay cả các đội tuyển hàng đầu cũng không thể đạt điểm tuyệt đối với bài toán ở mức này.

Ví dụ:

- IMO 2019/3 về "mạng xã hội và xor tam giác"
- IMO 2017/2 về phương trình $f(f(x)f(y)) + f(x + y) = f(xy)$
- IMO 2017/3 về "thợ săn và con thỏ"
- IMO 2017/6 về "nội suy đa thức thuần nhất"

Định nghĩa (45M). Bài toán thuộc hạng này thường chỉ có một số ít thí sinh giải được. Đây là mức độ của những bài toán IMO 3/6 khó hơn mức trung bình.

Ví dụ:

- IMO 2018/3 về "tam giác phản Pascal"
- IMO 2018/6 về "$\angle BXA + \angle DXC = 180°$"

Định nghĩa (50M). Đây là mức khó nhất mà một bài toán vẫn có thể xuất hiện trong kỳ thi IMO hoặc bài kiểm tra chọn đội tuyển của các quốc gia hàng đầu.

Định nghĩa (55M). Bài toán ở mức này quá dài dòng hoặc tốn nhiều thời gian để giải quyết trong một kỳ thi có giới hạn thời gian.

Định nghĩa (60M). Bài toán ở mức này không thể giải trong vòng 4,5 giờ bởi học sinh trung học, nhưng vẫn có thể được giải quyết trong điều kiện không giới hạn thời gian. Ví dụ, một kết quả từ một nghiên cứu tổ hợp với chứng minh dài 15 trang có thể rơi vào hạng này.

Lưu ý: Evan Chen sử dụng bội số của 5 để tránh nhầm lẫn giữa số bài toán (ví dụ: bài toán số 6) với mức độ khó (ví dụ: 30M).

Chương 6

Tiêu chuẩn Xếp hạng MOHS

Thang độ khó MOHS

Trong tài liệu này, Evan Chen cung cấp xếp hạng độ khó cá nhân cho các bài toán từ một số kỳ thi gần đây. Điều này đòi hỏi phải xác định một tiêu chí đánh giá độ khó một cách cẩn thận. Evan Chen gọi hệ thống này là **thang độ khó MOHS** (phát âm là "moez"); đôi khi anh cũng sử dụng đơn vị "M" (viết tắt của "Mohs").

Thang đo này tiến hành theo bước nhảy 5M, với mức thấp nhất là 0M và mức cao nhất là 60M. Tuy nhiên, trên thực tế, rất ít bài toán được xếp hạng cao hơn 50M, nên có thể coi nó chủ yếu là một thang đo từ 0M đến 50M, với một số bài toán thuộc dạng "vượt mức thông thường".

Bên dưới là bản dịch tiếng Việt từ tài liêu trên.

Xếp hạng dựa theo ý kiến cá nhân của Evan Chen

Mặc dù có rất nhiều điều đã được viết ra ở đây, nhưng cuối cùng, những xếp hạng này vẫn chỉ là ý kiến cá nhân của Evan Chen. Evan Chen không khẳng định rằng các xếp hạng này là khách quan hoặc phản ánh một sự thật tuyệt đối nào đó.

Lưu ý hài hước (Bảo hành xếp hạng). Các xếp hạng được cung cấp "nguyên trạng", không có bất kỳ bảo hành nào, dù rõ ràng hay ngụ ý, bao gồm nhưng không giới hạn ở các bảo hành về khả năng thương mại, sự phù hợp với một mục đích cụ thể, và việc không vi phạm quyền sở hữu trí tuệ. Trong mọi trường hợp, Evan không chịu trách nhiệm đối với bất kỳ khiếu nại, thiệt hại hoặc trách nhiệm pháp lý nào phát sinh từ, liên quan đến, hoặc có liên quan đến những xếp hạng này.

Hướng dẫn sử dụng

Cảnh báo quan trọng: Lạm dụng các xếp hạng này có thể gây hại cho bạn.

Ví dụ, nếu bạn quyết định không nghiêm túc thử sức với một số bài toán chỉ vì chúng được xếp hạng 40M trở lên, bạn có thể tự làm khó mình bằng cách tước đi cơ hội tiếp xúc với những bài toán khó. Nếu bạn không thường xuyên thử sức với các bài toán cấp độ IMO3 một cách nghiêm túc, bạn sẽ không bao giờ đạt đến mức độ có thể thực sự giải được chúng.

Vì lý do này, nghịch lý thay, đôi khi việc không biết bài toán khó đến mức nào lại tốt hơn, để bạn không vô thức có thái độ bỏ cuộc ngay từ đầu.

Các xếp hạng này được thiết kế để làm tài liệu tham khảo. Một cách sử dụng hợp lý là không xem xếp hạng bài toán cho đến khi bạn đã giải xong; điều này mô phỏng tốt nhất điều kiện thi đấu thực tế, khi bạn không biết độ khó của bài toán cho đến khi bạn giải được nó hoặc hết giờ và thấy những ai khác đã giải được. Bạn đã được cảnh báo. Chúc may mắn!

Ý nghĩa của các mức xếp hạng bài toán

Dưới đây là ý nghĩa của từng mức độ xếp hạng bài toán theo thang đo MOHS.

Định nghĩa (0M)**.** Bài toán có mức 0M quá dễ để xuất hiện trong IMO. Thông thường, một học sinh giỏi trong lớp toán nâng cao có thể giải được bài toán này mà không cần đào tạo chuyên sâu về toán olympic.

Định nghĩa (5M)**.** Đây là mức dễ nhất có thể xuất hiện trong IMO nhưng vẫn đáp ứng tiêu chuẩn của kỳ thi. Những bài toán này có thể được giải quyết rất nhanh.

Ví dụ:

- IMO 2019/1 về phương trình $f(2a) + 2f(b) = f(f(a + b))$
- IMO 2017/1 về căn bậc hai $\sqrt{a_n}$ hoặc $a_n + 3$

Định nghĩa (10M)**.** Đây là mức độ dành cho các bài toán IMO số 1 hoặc 4 mà hầu hết các thí sinh không gặp khó khăn khi giải. Tuy nhiên, vẫn cần có một số công việc để hoàn thành lời giải.

Ví dụ:

- IMO 2019/4 về $k! = (2^n - 1) \dots$
- IMO 2018/1 về $DE \parallel FG$

Định nghĩa (15M)**.** Đây là mức thấp nhất của các bài toán có thể xuất hiện dưới dạng bài số 2 hoặc 5 của IMO, nhưng thường phù hợp hơn với bài số 1 hoặc 4. Những bài toán này thường có thể được giải quyết dễ dàng bởi các đội tuyển thuộc top 10 thế giới.

Ví dụ:

- IMO 2019/5 về bài toán "Ngân hàng Bath"
- IMO 2018/4 về "Amy/Ben và lưới 20×20"
- IMO 2017/4 về tiếp tuyến KT của Γ

Định nghĩa (20M)**.** Những bài toán ở mức này có thể quá khó để xuất hiện dưới dạng IMO 1/4 nhưng vẫn chưa đạt đến độ khó trung bình của IMO 2/5.

Ví dụ:

- IMO 2018/5 về $a_1, a_2, \dots, a_n$ sao cho $\frac{a_1}{a_2} + \cdots + \frac{a_n}{a_1} \in \mathbb{Z}$

Định nghĩa (25M)**.** Đây là mức độ phù hợp nhất với các bài toán IMO 2/5. Những bài toán này là thử thách thực sự ngay cả với các đội tuyển hàng đầu.

Ví dụ:

- IMO 2019/2 về "P_1, Q_1, P, Q đồng viên"

Định nghĩa (30M)**.** Những bài toán ở mức này khó hơn một chút so với mức trung bình của IMO 2/5, nhưng vẫn chưa đủ khó để được sử dụng làm bài số 3 hoặc 6.

Ví dụ:

- IMO 2018/2 về phương trình $a_i a_{i+1} + 1 = a_{i+2}$

Định nghĩa (35M)**.** Đây là mức độ khó cao nhất dành cho các bài toán IMO 2/5 và cũng là mức độ dễ nhất của các bài toán IMO 3/6.

Ví dụ:

- IMO 2019/6 về "$DI \cap PQ$ trên phân giác góc ngoài $\angle A$"
- IMO 2017/5 về "Ngài Alex và các cầu thủ bóng đá"

Định nghĩa (40M)**.** Những bài toán ở mức này quá khó để xuất hiện ở IMO 2/5. Ngay cả các đội tuyển hàng đầu cũng không thể đạt điểm tuyệt đối với bài toán ở mức này.

Ví dụ:

- IMO 2019/3 về "mạng xã hội và xor tam giác"
- IMO 2017/2 về phương trình $f(f(x)f(y)) + f(x+y) = f(xy)$
- IMO 2017/3 về "thợ săn và con thỏ"
- IMO 2017/6 về "nội suy đa thức thuần nhất"

Định nghĩa (45M)**.** Bài toán thuộc hạng này thường chỉ có một số ít thí sinh giải được. Đây là mức độ của những bài toán IMO 3/6 khó hơn mức trung bình.

Ví dụ:

- IMO 2018/3 về "tam giác phản Pascal"
- IMO 2018/6 về "$\angle BXA + \angle DXC = 180°$"

Định nghĩa (50M)**.** Đây là mức khó nhất mà một bài toán vẫn có thể xuất hiện trong kỳ thi IMO hoặc bài kiểm tra chọn đội tuyển của các quốc gia hàng đầu.

Định nghĩa (55M)**.** Bài toán ở mức này quá dài dòng hoặc tốn nhiều thời gian để giải quyết trong một kỳ thi có giới hạn thời gian.

Định nghĩa (60M)**.** Bài toán ở mức này không thể giải trong vòng 4,5 giờ bởi học sinh trung học, nhưng vẫn có thể được giải quyết trong điều kiện không giới hạn thời gian. Ví dụ, một kết quả từ một nghiên cứu tổ hợp với chứng minh dài 15 trang có thể rơi vào hạng này.

Lưu ý: Evan Chen sử dụng bội số của 5 để tránh nhầm lẫn giữa số bài toán (ví dụ: bài toán số 6) với mức độ khó (ví dụ: 30M).

Từ điển chú giải

Chỉ mục MOHS