Các bài toán thi Olympic Quốc Gia và Thế Giới

Ban biên soạn

Tạp chí Pi
Hội toán học Việt Nam

Ngày 22 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

Lý thuyết chung

Chương 1

Khái niệm và Định nghĩa

Định nghĩa (Quan hệ thứ tự)**.** Một quan hệ thứ tự trên một tập hợp là một quan hệ $\leq$ thỏa mãn ba tính chất:

1. $a \leq a$.
2. Nếu $a \leq b$ và $b \leq a$ thì $a = b$.
3. Nếu $a \leq b$ và $b \leq c$ thì $a \leq c$.

Định nghĩa (Quan hệ thứ tự toàn phần)**.** Một quan hệ thứ tự được gọi là *toàn phần* nếu mọi cặp phần tử đều có thể so sánh được, tức là với mọi a và b, ta luôn có hoặc $a \leq b$ hoặc $b \leq a$.

Định nghĩa (Dãy số)**.** Một **dãy số** là một hàm được xác định cho mọi số nguyên không âm n, với $x_n = f(n)$. Số hạng thứ n, x_n, thường có thể được tính từ các số hạng trước đó theo một công thức xác đijnh bởi một hàm số F:

$$x_n = F(x_{n-1}, x_{n-2}, \ldots)$$

Định nghĩa (Dãy đơn điệu)**.** Một dãy số $\{a_n\}_{n=1}^{\infty}$ được gọi là:

1. **tăng đơn điệu** nếu $a_k \leq a_{k+1}$ với mọi $k \geq 1$.
2. **giảm đơn điệu** nếu $a_k \geq a_{k+1}$ với mọi $k \geq 1$.
3. **tăng nghiêm ngặt** nếu $a_k < a_{k+1}$ với mọi $k \geq 1$.
4. **giảm nghiêm ngặt** nếu $a_k > a_{k+1}$ với mọi $k \geq 1$.

Trong bất kỳ trường hợp nào ở trên, dãy số $\{a_n\}$ được gọi là **đơn điệu**.

Định nghĩa (Chuẩn p-adic)**.** Trong số học, chuẩn p-adic (hoặc bậc p-adic) của một số nguyên n là số mũ của lũy thừa lớn nhất của số nguyên tố p mà n chia hết.

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

Nói một cách khác, chuẩn p-adic là số mũ của p trong phân tích thừa số nguyên tố của n:

$$n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \ldots {p_k}^{\alpha_k} \implies \nu_{p_i}(n) = \alpha_i, \ \forall\ i = 1, 2, \ldots, k.$$

trong đó $p_1, p_2, \ldots, p_k$ là các số nguyên tố và $\alpha_1, \alpha_2, \ldots, \alpha_k$ là các số nguyên dương.

Định nghĩa (Hàm số tự nghịch đảo)**.** Trong toán học, một **hàm số tự nghịch đảo** là một hàm số f sao cho:

$$f(f(x)) = x$$

với mọi x thuộc tập xác định của f. Nói cách khác, f là hàm ngược của chính nó.

Chương 2

Định lý và bổ đề

Định lý (Nguyên lý Chuồng Bồ Câu)

Nguyên lý Chuồng Bồ Câu (còn được gọi là nguyên lý hộp Dirichlet, nguyên lý Dirichlet hoặc nguyên lý hộp) phát biểu rằng nếu có nhiều hơn n con bồ câu được đặt vào n chuồng, thì ít nhất một chuồng phải chứa hai con bồ câu trở lên.

Một cách phát biểu khác là: trong một tập hợp gồm n số nguyên bất kỳ, luôn tồn tại hai số có cùng phần dư khi chia cho $n-1$.

Phiên bản mở rộng của nguyên lý Chuồng Bồ Câu phát biểu rằng nếu k đối tượng được đặt vào n hộp, thì ít nhất một hộp phải chứa tối thiểu $\lceil \frac{k}{n} \rceil$ đối tượng. Ở đây, $\lceil \cdot \rceil$ ký hiệu cho hàm trần.

Định lý (Nguyên lý Bất biến)

Xét một tập hợp trạng thái $S = (s_1, s_2, \ldots, s_n)$ và một tập hợp các phép chuyển đổi $T \subseteq S \times S$. Một **bất biến** đối với T là một hàm $f : S \mapsto \mathbb{R}$ sao cho nếu $(s_i, s_j) \in T$ thì $f(s_i) = f(s_j)$.

Định lý (Nguyên lý Quy nạp)

Cho a là một số nguyên, và cho $P(n)$ là một mệnh đề (hoặc phát biểu) về n với mọi số nguyên $n \geq a$. **Nguyên lý quy nạp** là một phương pháp chứng minh rằng $P(n)$ đúng với mọi số nguyên $n \geq a$ thông qua hai bước:

1. *Cơ sở quy nạp:* Chứng minh rằng $P(a)$ đúng.
2. *Bước quy nạp:* Giả sử rằng $P(k)$ đúng với một số nguyên $k \geq a$, và sử dụng giả thiết này để chứng minh rằng $P(k+1)$ cũng đúng.

Khi đó, ta có thể kết luận rằng $P(n)$ đúng với mọi số nguyên $n \geq a$.

Định lý (Nguyên lý sắp thứ tự tốt trên tập hữu hạn)

Nguyên lý sắp thứ tự tốt phát biểu rằng mọi tập hợp có thứ tự toàn phần, hữu hạn và khác rỗng đều chứa *một phần tử lớn nhất* và *một phần tử nhỏ nhất*.

Định lý (Nguyên lý sắp thứ tự tốt trên tập hợp số nguyên dương)

Nguyên lý sắp thứ tự tốt phát biểu rằng mọi tập hợp khác rỗng của các số nguyên dương đều chứa *một phần tử nhỏ nhất*.

Định lý (Nguyên lý cực hạn)

Chúng ta sử dụng thuật ngữ *Nguyên lý cực hạn* để chỉ sự tồn tại của một phần tử nhỏ nhất hoặc lớn nhất trong một tập hợp.

Chúng ta thường kết hợp

1. *Nguyên lý cực hạn* với *Chứng minh phản chứng* để chứng minh sự tồn tại hoặc không tồn tại của một đối tượng, hoặc
2. *Nguyên lý cực hạn* với *Nguyên lý Chuồng Bồ Câu* để thiết lập điều kiện tồn tại hoặc để tăng hoặc giảm một đại lượng, ngoài ra
3. *Nguyên lý cực hạn* có thể được kết hợp với *Nguyên lý Quy nạp* để đơn giản hóa một chứng minh.

Định lý 2.0.1 (Bất đẳng thức Chuỗi Xen Kẽ)

Cho một dãy số giảm dần a_n với $a_n > 0$ và giới hạn $\lim_{n\to\infty} a_n = 0$, chuỗi xen kẽ:

$$S = a_1 - a_2 + a_3 - a_4 + \dots$$

hội tụ và sai số của tổng vô hạn được ước lượng bởi:

$$\left| S - \sum_{k=1}^{N} (-1)^{k+1} a_k \right| \leq a_{N+1}.$$

Chương 3

Hằng đẳng thức

Phần II

Lý thuyết số

Chương 4

Tính chia hết

4.1 Lý thuyết

Định lý (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.

Mọi số tự nhiên n lớn hơn 1, có thể viết duy nhất dưới dạng:

$$n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \ldots {p_k}^{\alpha_k}$$

trong đó $p_1, p_2, \ldots, p_k$ là các số nguyên tố và $\alpha_1, \alpha_2, \ldots, \alpha_k$ là các số nguyên dương.

4.2 Các ví dụ

Ví dụ (CHN 2015 TST1/D1/P2)

[**unrated**] Cho $a_1, a_2, a_3, \ldots$ là các số nguyên dương phân biệt, và $0 < c < \frac{3}{2}$. Chứng minh rằng: Tồn tại vô hạn số nguyên dương k sao cho

$$[a_k, a_{k+1}] > ck.$$

Lời giải. (Cách 1)[1]Giả sử phản chứng rằng tồn tại một số nguyên dương K sao cho

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

với mọi số nguyên $k \ge K$.

Khẳng định — Với mọi $k \ge K$, ta có

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

Chứng minh. Do $a_k \ne a_{k+1}$, ta quan sát thấy rằng

$$a_k + a_{k+1} \ge 3\gcd(a_k, a_{k+1})$$

vì $\gcd(a_k, a_{k+1})$ chia hết cho $a_k + a_{k+1}$ và

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

Do đó,

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

■

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

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

Do $a_K, \ldots, a_{N+1}$ đều là các số khác nhau, nên trong tổng bên trái, mỗi số hạng $\frac{1}{j}$ xuất hiện nhiều nhất hai lần. Từ đó, ta suy ra:

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

Kết hợp hai bất đẳng thức trên và biến đổi lại, ta có:

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

Vì $\frac{3}{c} > 2$, vế trái là một giá trị cố định nhưng vế phải không bị chặn khi $N \to \infty$, dẫn đến mâu thuẫn. □

[1]Lời giải của TheUltimate123.

Ví dụ (CHN 2015 TST1/D2/P2)

[**unrated**] Cho trước một số nguyên dương n. 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

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

Lời giải. (Cách 1)[2]Gọi

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

Khi đó,

$$\min A = -3n^3 - 4n^2, \quad \max A = 3n^3 + 4n^2.$$

Do đó, khoảng $[\min A, \max A]$ chứa

$$3n^3 + 4n^2 - (-3n^3 - 4n^2) + 1 = 6n^3 + 8n^2 + 1 < (2n + 1)^3 \text{ số nguyên.}$$

Theo Nguyên lý Chuồng Bồ Câu, phải tồn tại hai bộ giá trị khác biệt

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

tức là

$$a(x - x') + b(y - y') + c(z - z') = 0.$$

Vì $x - x', y - y', z - z' \in [-2n, 2n]$ và không đồng thời bằng 0, ta có điều phải chứng minh. □

[2]Lời giải của TheUltimate123.

Ví dụ (CHN 2015 TST1/D2/P5)

[**unrated**] Cho trước một số nguyên dương n. 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

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

Lời giải. (Cách 1)[3]Gọi

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

Khi đó,

$$\min A = -3n^3 - 4n^2, \quad \max A = 3n^3 + 4n^2.$$

Do đó, khoảng $[\min A, \max A]$ chứa

$$3n^3 + 4n^2 - (-3n^3 - 4n^2) + 1 = 6n^3 + 8n^2 + 1 < (2n + 1)^3 \text{ số nguyên.}$$

Theo Nguyên lý Chuồng Bồ Câu, phải tồn tại hai bộ giá trị khác biệt

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

tức là

$$a(x - x') + b(y - y') + c(z - z') = 0.$$

Vì $x - x', y - y', z - z' \in [-2n, 2n]$ và không đồng thời bằng 0, ta có điều phải chứng minh. □

[3]Lời giải của nayel.

Ví dụ (IMO 2023/P1)

[5M] Xác định tất cả các số nguyên hợp 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 $1 \le i \le k-2$.

Lời giải. (Cách 1)[4]Theo Định lý cơ bản của số học, dễ thấy rằng $n = p^r$ với $r \ge 2$ thỏa mãn điều kiện vì

$$d_i = p^{i-1}, \text{ với } 1 \le i \le k = r+1 \text{ và rõ ràng } p^{i-1} \mid (p^i + p^{i+1}).$$

Bây giờ, giả sử tồn tại một số nguyên n thỏa mãn điều kiện đã cho và có ít nhất hai thừa số nguyên tố phân biệt, gọi là p và q, với $p < q$ là hai thừa số nguyên tố nhỏ nhất của n.

Tồn tại số nguyên j sao cho:

$$d_1 = 1, d_2 = p, \ldots, d_j = p^{j-1}, d_{j+1} = p^j, d_{j+2} = q.$$

Ta cũng có:

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

Từ điều kiện đề bài:

$$d_{k-j-1} \mid (d_{k-i} + d_{k-j+1}) \implies \frac{n}{q} \mid \left(\frac{n}{p^j} + \frac{n}{p^{j-1}}\right) \quad (1)$$

Suy ra $p^j \mid q(p+1)$ dẫn đến $p \mid q$, mâu thuẫn với $p \ne q$. Vậy n phải là lũy thừa của một số nguyên tố. □

Lời giải. (Cách 2)[4] Vì $d_i d_{k+1-i} = n$, ta có:

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

Nhân hai vế với $d_i d_{i+1} d_{i+2}$ và đơn giản hóa:

$$d_i d_{i+1} \mid d_i d_{i+2} + d_{i+1} d_{i+2} \implies d_i \mid d_{i+1} d_{i+2} \quad (2)$$

Áp dụng điều kiện đề bài, ta có:

$$d_i \mid d_{i+1}(d_{i+1} + d_{i+2}) = d_{i+1}^2 + d_{i+1} d_{i+2}.$$

Kết hợp với (2), suy ra $d_i \mid d_{i+1}^2$ với mọi $1 \le i \le k-2$.

Giả sử rằng $d_2 = p$ là ước số nguyên tố nhỏ nhất của n. Ta chứng minh bằng Nguyên lý Quy nạp:

Khẳng định — $p \mid d_i, \ \forall\ 2 \le i \le k-1$.

Chứng minh. Thật vậy, trường hợp $d_2 = p$ là hiển nhiên. Giả sử $p \mid d_j$ với $2 \le j \le k-2$, khi đó:

$$p \mid d_j \mid {d_{j+1}}^2 \implies p \mid d_{j+1} \text{ (vì } p \text{ nguyên tố).}$$

■

Từ đó suy ra n là lũy thừa của một số nguyên tố vì nếu tồn tại một số nguyên tố $q \ne p$ mà cũng là ước số của n thì $p \mid q$ và đó là điều vô lý. □

Lời giải. (Cách 3)[4]

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

Chứng minh. Ta dùng Nguyên lý Quy nạp để chứng minh.

Bướcc cơ sở: $d_1 = 1$ là hiển nhiên. Giả sử $d_{i-1} \mid d_i$. Từ điều kiện đề bài:

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

Ta xét:

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

Ta suy ra:

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

suy ra $d_i \mid d_{i+1}$, hoàn thành chứng minh. ■

Dựa vào Mệnh đề đã chứng minh, n không thể có hai thừa số nguyên tố khác nhau vì thừa số nhỏ nhất sẽ chia hết thừa số còn lại. Do đó, n phải là lũy thừa của một số nguyên tố, và các lũy thừa của số nguyên tố đều thỏa mãn điều kiện của bài toán. □

[4] Shortlist 2023 with solutions.

Ví dụ (IND 2015 MO/P2)

[**unrated**] Với mọi số tự nhiên $n > 1$, viết phân số $\frac{1}{n}$ dưới dạng thập phân vô hạn (không viết dạng rút gọn hữu hạn, ví dụ: $\frac{1}{2} = 0.4\overline{9}$, chứ không phải 0.5). Hãy xác định độ dài phần **không tuần hoàn** trong biểu diễn thập phân vô hạn của $\frac{1}{n}$.

Lời giải. (Cách 1)[5]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.

Khi đó:

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

Giả sử $n = 2^a \cdot 5^b \cdot q$, với q nguyên tố cùng nhau với 10 (tức $\gcd(q, 10) = 1$).

Để $\frac{1}{n}$ có biểu diễn thập phân vô hạn tuần hoàn với phần không tuần hoàn dài x_n, thì:

$$2^a5^b \mid 10^{x_n} \implies x_n \text{ là số nhỏ nhất sao cho } 2^a5^b \mid 10^{x_n} \implies x_n = \max(a, b)$$

Vì 10^{x_n} chia hết cho cả 2^a và 5^b khi $x_n \geq \max(a, b)$, và đây là giá trị nhỏ nhất như vậy.

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

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

□

[5]Lời giải của utkarshgupta.

Ví dụ (IND 2015 MO/P6)

[**unrated**] 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:

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

Lời giải. Xét các giá trị khả dĩ của một số chính phương modulo 12. Ta có:

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

Giả sử tập S gồm 11 số chính phương. Xét tập S_r là đa tập các phần dư modulo 12 của các phần tử trong S. Tức là mỗi phần tử trong S_r thuộc $\{0, 1, 4, 9\}$.

Ta cần chứng minh rằng tồn tại hai tập con rời nhau $A, B \subset S$, mỗi tập có đúng 3 phần tử, sao cho:

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

Xét ba trường hợp.

Trường hợp 1: Trong S_r tồn tại ít nhất 6 phần tử có cùng phần dư. Lúc này, ta có thể chia 6 phần tử đó thành hai tập con A, B có ba phần tử bằng nhau, suy ra tổng của mỗi tập bằng nhau, nên đương nhiên đồng dư modulo 12.

Trường hợp 2: Có một phần dư xuất hiện 4 hoặc 5 lần. Do S có 11 phần tử, nên ít nhất phải có một phần dư khác xuất hiện ít nhất 2 lần (theo nguyên lý Dirichlet). Lúc này, ta có thể chọn ba phần tử từ nhóm 4–5 phần tử đó cho một tập, và ba phần tử còn lại (từ phần dư khác) cho tập còn lại. Tổng của mỗi tập là tổ hợp của các phần dư đã biết, nên tồn tại hai tổ hợp có cùng tổng modulo 12.

Trường hợp 3: Mỗi phần dư xuất hiện tối đa 3 lần. Vì chỉ có 4 loại phần dư $\{0, 1, 4, 9\}$, nên tổng số lượng phần tử tối đa nếu chỉ có hai loại phần dư với ít nhất 2 lần xuất hiện là:

$$3 + 3 + 1 + 1 = 8 < 11, \text{ mâu thuẫn.}$$

Do đó, phải có ít nhất 3 loại phần dư khác nhau với ít nhất 2 lần xuất hiện. Khi đó, ta dễ dàng chọn hai tổ hợp ba phần tử có tổng bằng nhau modulo 12 từ ba nhóm đó.

Trong mọi trường hợp, luôn tồn tại hai tập con rời nhau gồm ba số chính phương sao cho tổng của chúng đồng dư modulo 12. □

[5] Dựa theo lời giải của Sahil.

Ví dụ (IND 2015 TST2/P1)

[**unrated**][6]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.

Lời giải. (Cách 1) Trước hết, ta chứng minh rằng mọi số nguyên lớn hơn $(n-2)\cdot 2^n + 1$ đều có thể biểu diễn dưới dạng tổng như yêu cầu. Ta sẽ sử dụng quy nạp theo n.

Với $n = 2$, ta có $A_2 = \{2^2 - 2^0, 2^2 - 2^1\} = \{3, 2\}$. Khi đó, mọi số nguyên dương $m \neq 1$ đều có thể viết dưới dạng tổng các phần tử của A_2: nếu m chẵn thì $m = 2 + 2 + \cdots + 2$; nếu m lẻ thì $m = 3 + 2 + \cdots + 2$.

Giả sử mệnh đề đúng với mọi số nhỏ hơn n, ta xét $n > 2$, và một số nguyên $m > (n-2)\cdot 2^n + 1$.

Nếu m là chẵn, xét:

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

Theo giả thiết quy nạp, tồn tại cách biểu diễn:

$$\frac{m}{2} = (2^{n-1} - 2^{k_1}) + (2^{n-1} - 2^{k_2}) + \cdots + (2^{n-1} - 2^{k_r})$$

với $0 \leq k_i < n-1$. Suy ra:

$$m = (2^n - 2^{k_1+1}) + (2^n - 2^{k_2+1}) + \cdots + (2^n - 2^{k_r+1}),$$

tức là tổng các phần tử trong A_n.

Nếu m là lẻ, xét:

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

Theo giả thiết quy nạp, tồn tại biểu diễn:

$$\frac{m - (2^n - 1)}{2} = (2^{n-1} - 2^{k_1}) + \cdots + (2^{n-1} - 2^{k_r}),$$

với $k_i < n-1$. Suy ra:

$$m = (2^n - 2^{k_1+1}) + \cdots + (2^n - 2^{k_r+1}) + (2^n - 1),$$

là tổng các phần tử thuộc A_n.

Bây giờ ta chứng minh rằng số $(n-2)\cdot 2^n + 1$ không thể biểu diễn được.

Gọi N là số nguyên dương nhỏ nhất sao cho $N \equiv 1 \pmod{2^n}$ và N có thể biểu diễn được thành tổng các phần tử từ A_n. Xét biểu diễn:

$$N = (2^n - 2^{k_1}) + (2^n - 2^{k_2}) + \cdots + (2^n - 2^{k_r}) \tag{1}$$

với $0 \leq k_i < n$.

Giả sử tồn tại hai chỉ số i, j sao cho $k_i = k_j$.

Nếu $k_i = k_j = n-1$, thì:

$$N - 2\cdot(2^n - 2^{n-1}) = N - 2^n$$

cũng có thể biểu diễn được, mâu thuẫn với tính nhỏ nhất của N.

Nếu $k_i = k_j = k < n-1$, thì:

$$N - 2 \cdot (2^n - 2^k) + (2^n - 2^{k+1}) = N - 2^n$$

cũng mâu thuẫn.

Vậy các k_i đều phân biệt, nên:

$$2^{k_1} + \cdots + 2^{k_r} \leq 2^0 + 2^1 + \cdots + 2^{n-1} = 2^n - 1$$

Mặt khác, từ (1) xét modulo 2^n, ta có:

$$2^{k_1} + \cdots + 2^{k_r} \equiv -N \equiv -1 \pmod{2^n} \implies 2^{k_1} + \cdots + 2^{k_r} = 2^n - 1$$

Điều này xảy ra khi $\{k_1, \ldots, k_r\} = \{0, 1, \ldots, n-1\}$, và khi đó:

$$N = n \cdot 2^n - (2^0 + \cdots + 2^{n-1}) = (n-1) \cdot 2^n + 1.$$

Do đó, số $(n-2) \cdot 2^n + 1$ không thể biểu diễn được như yêu cầu. □

[6] IMO SL 2014 N1.

Ví dụ (IRN 2015 MO/N2)

[**unrated**] Gọi $M_0 \subset \mathbb{N}$ là một tập hợp hữu hạn, không rỗng các 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.

Lời giải. (Cách 1)[7]Giả sử tại bước n, tồn tại hai phần tử $k, t \in M_{n-1}$ sao cho phần tử tương ứng trong M_n có quan hệ chia hết:

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

Điều này dẫn đến:

$$b_n k + 1 \mid b_n(t - k) \implies b_n k + 1 \mid k - t$$

Vì vậy, nếu có tồn tại một phần tử trong M_n chia hết cho một phần tử khác, thì hiệu giữa phần tử lớn nhất và nhỏ nhất trong M_{n-1} phải lớn hơn hoặc bằng phần tử nhỏ nhất của M_n:

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

Giờ ta đánh giá khoảng cách giữa phần tử lớn nhất và nhỏ nhất trong M_n. Gọi $M = \max(M_1)$, $m = \min(M_1)$. Dễ thấy rằng các phần tử trong M_n là:

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

Do đó:

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

và:

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

Thế vào bất đẳng thức (1), ta có:

$$b_2 b_3 \cdots b_{n-1}(M - m - 1) \geq b_2 b_3 \cdots b_n m$$

Rút gọn vế trái và vế phải (chia cả hai vế cho $b_2 \cdots b_{n-1}$), ta được:

$$\frac{M - m - 1}{m} \geq b_n$$

Tuy nhiên, theo quá trình xây dựng, vì $b_n \in M_{n-1}$, và các phần tử trong chuỗi tăng nhanh, ta có:

$$b_n \geq n - 2$$

Vậy nếu bất đẳng thức:

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

xảy ra, thì không thể tồn tại hai phần tử chia hết cho nhau trong M_n. Tức là tại bước đó, không có phần tử nào chia hết cho phần tử nào khác trong cùng tập.

Do đó, khi n đủ lớn, điều này chắc chắn xảy ra, và bài toán được chứng minh. □

[7]Dựa theo lời giải của Arefe.

Ví dụ (IRN 2015 TST/D3-P2)

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

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

(Ở đây, $[a, b]$ 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 $a_k \leq 0$.

Lời giải. (Cách 1)[8]Ta sẽ chứng minh điều mạnh hơn: Tồn tại $k \leq a_3 + 3$ sao cho $a_k \leq 0$. Đặt

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

Ta có ngay rằng:

$$a_{n-2} \mid a_n \quad \forall n \geq 4$$

Điều này kéo theo $a_{n-3} \mid a_n$ với mọi $n \geq 5$, do đó $b_n \in \mathbb{N}$, tức là b_n nguyên.

Khẳng định — Với mọi $n \geq 5$, ta có:

$$b_{n+1} < b_n$$

Chứng minh. Cố định $n \geq 5$. Khi đó,

$$\begin{aligned} a_{n+1} &= \text{lcm}[a_n, a_{n-1}] - \text{lcm}[a_{n-1}, a_{n-2}] = \text{lcm}[b_n \cdot \text{lcm}(a_{n-2}, a_{n-3}), a_{n-1}] - \text{lcm}[a_{n-1}, a_{n-2}] \\ &= \text{lcm}[b_n, a_{n-2}, a_{n-3}, a_{n-1}] - \text{lcm}[a_{n-1}, a_{n-2}] \end{aligned}$$

Mà $a_{n-3} \mid a_{n-1}$, nên:

$$a_{n+1} = \text{lcm}[b_n, a_{n-2}, a_{n-1}] - \text{lcm}[a_{n-1}, a_{n-2}] \implies b_{n+1} = \frac{a_{n+1}}{\text{lcm}[a_{n-1}, a_{n-2}]} < b_n.$$

■

Để hoàn tất chứng minh, ta chỉ cần chỉ ra rằng $b_5 \leq a_3 - 2$, bởi nếu vậy thì dãy b_n giảm dần, nên sẽ đến lúc $b_k = 0$ với $k \leq a_3 + 3$, suy ra $a_k = 0$.

Ta tính:

$$a_4 = \text{lcm}(a_3, a_2) - \text{lcm}(a_2, a_1) = ca_2 \quad \text{với } c \leq a_3 - 1$$

Tiếp theo:

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

Suy ra:

$$b_5 = \frac{a_5}{\text{lcm}(a_3, a_2)} \leq c - 1 \leq a_3 - 2$$

Vậy ta đã chứng minh được rằng $a_k = 0$ với $k \leq a_3 + 3$. ■

Chú ý: Giới hạn trên là chặt. Chẳng hạn, chọn $a_1 = 1, a_2 = 2, a_3 = 3$, ta có:

$$\begin{aligned} a_4 &= \text{lcm}(3, 2) - \text{lcm}(2, 1) = 6 - 2 = 4 \\ a_5 &= \text{lcm}(4, 3) - \text{lcm}(3, 2) = 12 - 6 = 6 \\ a_6 &= \text{lcm}(6, 4) - \text{lcm}(4, 3) = 12 - 12 = 0 \end{aligned}$$

Vậy giá trị nhỏ nhất thỏa mãn $a_k \leq 0$ là $k = 6 = a_3 + 3$. □

[8]Lời giải của guptaamitu1.

Ví dụ (KOR 2015 MO/P8)

[**unrated**] 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:

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

Lời giải. (Cách 1)[9]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. ($\bigstar$)

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 $\frac{n}{2}$ và số còn lại lớn hơn. Giả sử $a < \frac{n}{2}$, ta có:

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

Vậy nên:

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

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

Gọi p là ước nguyên tố nhỏ nhất của n, và đặt $m = \frac{n}{p}$. Gọi T là tổng các số nguyên dương nhỏ hơn m và nguyên tố cùng nhau với m. Khi đó:

$$T = \sum_{\substack{1 \le a < m \\ \gcd(a,m)=1}} a = \frac{m\varphi(m)}{2}.$$

Theo giả thiết ($\bigstar$), nên $\varphi(m) \ge 2p$. Từ đó, ta suy ra:

$$S \ge T = \frac{m\varphi(m)}{2} \ge pm = n, \tag{2}$$

Thay (2) vào (1), ta được:

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

Vì $\varphi(n) = k > 8$, ta có:

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

□

[9]Lời giải của andria.

Lời giải. (Cách 2)[10]Ta dễ dàng nhận thấy rằng nếu a_i là một phần tử, thì $n - a_i$ cũng thuộc tập và tổng của hai số này là n. Do đó k chẵn và

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

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 ban đầu tương đương với:

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

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

Gọi $f(n)$ là một số nguyên gần nhất với $\frac{n}{3}$, nhưng không chia hết cho 3:

$$f(n) = \begin{cases} \frac{n\pm1}{3}, & n \equiv \mp 1 \pmod 3 \\ \frac{n}{3} \pm 1, & n \equiv 0 \pmod 3 \end{cases} \implies \begin{cases} \frac{n}{3} - 1 \le f(n) \le \frac{n}{3} + 1, \text{ và} \\ \gcd(f(n), n) = 1. \end{cases}$$

Trường hợp 1: n lẻ. Với $n < 30$, ta kiểm tra bằng tính toán trực tiếp. Giả sử $n > 30$. Đặt $n = 2^k + m$, với $1 \le m \le 2^k - 1$. Khi đó:

$$2^{k-2} < f(n) < 2^k, \quad f(n) < \frac{n-1}{2} \text{ với } n > 9.$$

Suy ra:

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

Trường hợp 2: $n \equiv 0 \mod 4$. Nếu $\gcd(x, n) = 1$, thì $\gcd\left(\frac{n}{2} - x, n\right)$. Do đó:

$$S = \frac{1}{2} \cdot \frac{n}{2} \cdot \frac{k}{2} = \frac{nk}{8} > n, \text{ vì } k > 8.$$

Trường hợp 3: $n = 4m + 2$. Với $m \le 7$, ta kiểm tra bằng tính toán trực tiếp. Với $m > 7$, ta có:

$$\gcd(2m - 1, 4m + 2) = 1, \quad m + 1 \le f(n) \le 2m - 1.$$

Một trong hai số m hoặc $m + 1$ là lẻ, và nguyên tố cùng nhau với n. Gọi số đó là t. Khi đó:

$$S \ge 1 + t + f(n) + 2m - 1 \ge 1 + m + \frac{4m+2}{3} - 1 + 2m - 1 = \frac{13}{3}m - \frac{1}{3} > 4m + 2 = n.$$

Kết luận. Sau khi xét đầy đủ các trường hợp, ta có:

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

□

[10]Lời giải của rkm0959.

Ví dụ (RUS 2015 TST/D9/P1)

[**unrated**] Tìm tất cả các cặp số tự nhiên (a, b) sao cho:

- $b-1$ chia hết cho $a+1$, và
- a^2+a+2 chia hết cho b.

Lời giải. (Cách 1)[11]Đặt $c = a+1 \geq 2$, khi đó các điều kiện tương đương:

- $c \mid b-1$,
- $b \mid c^2-c+2$.

Điều này cho thấy b và c là hai số nguyên tố cùng nhau và đều chia hết cho biểu thức

$$c^2-c+2-2b \implies bc \mid c^2-c+2-2b.$$

Dễ thấy rằng $\boxed{(a,1)}$ là nghiệm với mọi $a \in \mathbb{N}$. Bây giờ ta xét trường hợp $b \geq 2$. Khi đó:

$$c < b \implies bc > b^2 > c^2 \implies c^2-c+2-2b < bc.$$

Đồng thời:

$$c^2-c+2-2b > -2b \geq -bc \implies -bc < c^2-c+2-2b < bc \implies \text{giá trị này phải bằng } 0.$$

Khi đó:

$$c^2-c+2 = 2b \implies a^2+a+2 = 2b.$$

Vậy điều kiện thứ hai trở thành:

$$b \mid 2b \implies \text{luôn đúng.}$$

Kiểm tra lại điều kiện thứ nhất:

$$b = \frac{a^2+a+2}{2} \implies b-1 = \frac{a^2+a}{2}+1.$$

Ta cần:

$$a+1 \mid \frac{a^2+a}{2}+1.$$

Biểu thức này chỉ là một số nguyên khi a chẵn. Đặt $a = 2k$ thì:

$$b = \frac{(2k)^2+2k+2}{2} = \frac{4k^2+2k+2}{2} = 2k^2+k+1.$$

Do đó, thu được họ nghiệm thứ hai:

$$\boxed{(a,b) = (2k, 2k^2+k+1), \quad k \in \mathbb{N}}.$$

□

[11]Dựa theo lời giải của Tintam.

Lời giải. (Cách 2)[12]Đặt $t = a + 1$ ($\implies a = t - 1$). Điều kiện thứ nhất trở thành:

$$t \mid b - 1 \implies b = tk + 1 \text{ với } k \in \mathbb{N}.$$

Điều kiện thứ hai trở thành:

$$b \mid a^2 + a + 2 = (t-1)^2 + (t-1) + 2 = t^2 - t + 2.$$

Do đó:

$$tk + 1 \mid t^2 - t + 2.$$

Vì $tk + 1 \mid t^2 - t + 2$, và $tk + 1 \mid 2tk + 2$, suy ra:

$$tk + 1 \mid (t^2 - t + 2) - (2tk + 2) = t^2 - t - 2tk = t(t - 2k - 1).$$

Mặt khác, vì $\gcd(t, tk + 1) = 1$, nên:

$$tk + 1 \mid t - 2k - 1.$$

Trường hợp 1: $k = 0$. Khi đó:

$$b = 1, \quad a^2 + a + 2 \mid 1 \implies 1 \mid a^2 + a + 2 \text{ luôn đúng.}$$

Vậy mọi $a \in \mathbb{N}$ đều thỏa mãn. Tập nghiệm:

$$\boxed{(a, 1) \text{ với } a \in \mathbb{N}}.$$

Trường hợp 2: $k \geq 1$. Từ điều kiện $tk + 1 \mid t - 2k - 1$, giả sử $t > 2k + 1$. Khi đó:

$$t - 2k - 1 \geq tk + 1 \implies t \geq tk + 2k + 2 > t, \text{ mâu thuẫn.}$$

Nếu $t < 2k + 1$, thì:

$$2k + 1 \geq tk + t + 1 \implies t \leq 1, \text{ điều này vô lý vì } t = a + 1 \geq 2.$$

Do đó, chỉ còn lại:

$$t = 2k + 1 \implies a = t - 1 = 2k, \quad b = tk + 1 = (2k + 1)k + 1 = 2k^2 + 2k + 1.$$

Vậy ta thu được họ nghiệm thứ hai:

$$\boxed{(a, b) = (2k, 2k^2 + 2k + 1), \quad k \in \mathbb{N}}.$$

□

[12]Dựa theo lời giải của grupyorum.

4.3 Bài tập

Bài tập (JPN 2015 MO1/P1)**.** [**unrated**] Tìm tất cả các số nguyên dương n sao cho

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

là một số nguyên.

Chương 5

Cơ bản về số học đồng dư

5.1 Lý thuyết

5.2 Các ví dụ

Ví dụ (IMO 2015/N1)

[**unrated**] Xác định tất cả các số nguyên dương M sao cho dãy số $a_0, a_1, a_2, \ldots$ được xác định bởi

$$a_0 = M + \frac{1}{2} \quad \text{and} \quad a_{k+1} = a_k \lfloor a_k \rfloor \quad \text{với } k = 0, 1, 2, \ldots$$

chứa ít nhất một số nguyên.

Lời giải. [1](Cách 1) Xét $b_k = 2a_k$ với mọi $k \geq 0$. Khi đó,

$$b_{k+1} = 2a_{k+1} = 2a_k \lfloor a_k \rfloor = b_k \lfloor \frac{b_k}{2} \rfloor.$$

Vì b_0 là một số nguyên, suy ra b_k là một số nguyên với mọi $k \geq 0$.

Giả sử rằng dãy $a_0, a_1, a_2, \ldots$ không chứa số nguyên nào. Khi đó, b_k phải là số nguyên lẻ với mọi $k \geq 0$, do đó

$$b_{k+1} = b_k \lfloor b_k/2 \rfloor = \frac{b_k(b_k - 1)}{2}. \tag{1}$$

Chúng ta cung cấp một cách khác để chứng minh rằng $M = 1$ một khi đã đạt đến phương trình (1). Chúng ta khẳng định rằng

Khẳng định — $b_k \equiv 3 \pmod{2^m}$ với mọi $k \geq 0$ và $m \geq 1$.

Chứng minh. Ta chứng minh bằng Nguyên lý Quy nạp theo m.

Bước cơ sở: $b_k \equiv 3 \pmod 2$ đúng với mọi $k \geq 0$ vì b_k là số lẻ.

Bước quy nạp: Giả sử rằng $b_k \equiv 3 \pmod{2^m}$ với mọi $k \geq 0$. Do đó, tồn tại một số nguyên d_k sao cho

$$b_k = 2^m d_k + 3.$$

Khi đó, ta có

$$3 \equiv b_{k+1} \equiv (2^m d_k + 3)(2^{m-1} d_k + 1) \equiv 3 \cdot 2^{m-1} d_k + 3 \pmod{2^{m+1}},$$

suy ra d_k phải là số chẵn. Điều này dẫn đến $b_k \equiv 3 \pmod{2^{m+1}}$, như yêu cầu. ■

Từ khẳng định trên, ta có $b_k = 3$ với mọi $k \geq 0$, suy ra $M = 1$. □

[1] Shortlist 2015 with solutions.

Ví dụ (IMO 2015/P2)

[**30M**] Hãy tìm tất cả các bộ số nguyên dương (a, b, c) sao cho mỗi số trong các số:

$$ab - c, bc - a, ca - b$$

là lũy thừa của 2.

Lời giải. [2](Cách 1) Các nghiệm của (a, b, c) là $(2, 2, 2)$, $(2, 2, 3)$, $(2, 6, 11)$, $(3, 5, 7)$ và các hoán vị của chúng.

Trong toàn bộ chứng minh, giả sử rằng $a \le b \le c$, do đó ta có

$$ab - c = 2^m, \quad ca - b = 2^n, \quad bc - a = 2^p,$$

với $m \le n \le p$. Lưu ý rằng $a > 1$, bởi nếu không thì $b - c = 2^m$, điều này là không thể. Do đó,

$$2^n = ac - b \ge (a - 1)c \ge 2,$$

nghĩa là n và p là các số dương.

Quan sát rằng nếu $a = b \ge 3$, ta có $a(c - 1) = 2^n$, do đó a và $c - 1$ đều là (số chẵn và) lũy thừa của 2. Khi đó c là số lẻ và $a^2 - c = 2^m = 1$. Suy ra $c + 1 = a^2$ cũng là một lũy thừa của 2, điều này dẫn đến $c = 3$. Tuy nhiên, $a = b = c = 3$ không phải là một nghiệm; do đó, trường hợp $a = b \ge 3$ là không khả thi.

Ta xét các trường hợp còn lại như sau.

Trường hợp 1: $a = 2$ Ta có

$$2b - c = 2^m, \quad 2c - b = 2^n, \quad bc - 2 = 2^p.$$

Từ phương trình thứ hai, b là số chẵn. Từ phương trình thứ ba, nếu $p = 1$, thì $b = c = 2$; nếu $p > 1$, thì c là số lẻ, điều này dẫn đến $m = 0$.

Khi đó, ta có

$$3b = 2^n + 2 \quad (\text{nên } n \ge 2), \quad 3c = 2^{n+1} + 1,$$

và

$$(2^{n-1} + 1)(2^{n+1} + 1) = 9(2^{p-1} + 1).$$

Từ đó suy ra

$$1 \equiv 9 \pmod{2^{n-1}} \implies n \le 4.$$

Suy ra $n = 2$ hoặc $n = 4$, và (b, c) có thể là $(2, 3)$ hoặc $(6, 11)$. Do đó, các nghiệm của (a, b, c) là $(2, 2, 2)$, $(2, 2, 3)$ hoặc $(2, 6, 11)$.

Trường hợp 2: $3 \le a < b \le c$ Vì $(a - 1)c \le 2^n$, ta có $c \le 2^{n-1}$. Do đó,

$$b + a < 2c \le \frac{2^{n+1}}{a - 1} \le 2^n, \ b - a < c \le 2^{n-1}.$$

Từ đó suy ra $b - a$ không chia hết cho 2^{n-1}, và $b + a$ không chia hết cho 2^{n-1} khi $a \ge 5$.

Cộng và trừ $ac - b = 2^n$ và $bc - a = 2^p$, ta thu được

$$(c - 1)(b + a) = 2^p + 2^n, \ (c + 1)(b - a) = 2^p - 2^n.$$

Từ phương trình thứ hai, $c + 1$ chia hết cho 4. Do đó, $c - 1$ không chia hết cho 4, điều này dẫn đến $b + a < 2^n$ là một bội của 2^{n-1}. Do đó, $a \le 4$ và $b + a = 2^{n-1}$.

Trường hợp 2a: Xét $a = 3$ Khi đó ta có

$$3b - c = 2^m, \quad 3c - b = 2^n, \quad b = 2^{n-1} - 3.$$

Suy ra

$$2^{n-1} - 3 = 3 \cdot 2^{m-3} + 2^{n-3} \implies 2^{n-3} = 2^{m-3} + 1.$$

Từ đó, ta suy ra $m = 3$, $n = 4$, $b = 5$ và $c = 7$.

Trường hợp 2b: Xét $a = 4$ Ta có $4c - b = 2^n$ và $b = 2^{n-1} - 4$, từ đó

$$c = 3 \cdot 2^{n-3} - 1.$$

Tuy nhiên, điều kiện $b \leq c$ dẫn đến $2^{n-3} \leq 3$, và $a < b$ dẫn đến $2^{n-3} > 2$. Điều này là không thể, do đó không tồn tại nghiệm với $a = 4$.

Vậy ta thu được $(a, b, c) = (3, 5, 7)$ là nghiệm duy nhất với $3 \leq a < b \leq c$. □

[2] Lời giải chính thức.

Ví dụ (IND 2015 TST3/P2)

[**unrated**][3]Tìm tất cả các bộ ba (p, x, y) bao gồm một số nguyên tố p và hai số nguyên dương x và y sao cho $x^{p-1} + y$ và $x + y^{p-1}$ đều là lũy thừa của p.

Lời giải. (Cách 1) Với $p = 2$, rõ ràng mọi cặp số nguyên dương x, y sao cho tổng của chúng là một lũy thừa của 2 đều thỏa mãn điều kiện bài toán.

Do đó, từ đây giả sử $p > 2$, và ta đặt a, b là các số nguyên dương sao cho:

$$x^{p-1} + y = p^a, \quad x + y^{p-1} = p^b$$

Giả sử không mất tính tổng quát rằng $x \le y$, do đó:

$$p^a = x^{p-1} + y \le x + y^{p-1} = p^b \implies a \le b \implies p^a \mid p^b$$

Xét:

$$p^b = y^{p-1} + x = (p^a - x^{p-1})^{p-1} + x$$

Lấy đồng dư theo modulo p^a, và lưu ý rằng $p - 1$ chẵn, ta được:

$$0 \equiv x^{(p-1)^2} + x \pmod{p^a}$$

Nếu $p \mid x$, thì $p^a \mid x$, vì $x^{(p-1)^2-1} + 1$ không chia hết cho p. Tuy nhiên điều này là không thể vì $x \le x^{p-1} < p^a$. Vậy $p \nmid x$, do đó:

$$p^a \mid x^{(p-1)^2-1} + 1 = x^{pp-2} + 1.$$

Áp dụng định lý Fermat nhỏ, ta có $x^{(p-1)^2} \equiv 1 \pmod{p}$, dẫn đến $p \mid x + 1$.

Gọi p^r là lũy thừa cao nhất của p chia hết $x + 1$. Sử dụng khai triển nhị thức, ta viết:

$$x^{p(p-2)} = \sum_{k=0}^{p(p-2)} \binom{p(p-2)}{k} (-1)^{p(p-2)-k} (x+1)^k$$

Tất cả các hạng tử trong tổng đều chia hết cho p^{3r} nên chia hết cho p^{r+2}, ngoại trừ:

- Hạng tử với $k = 2$: giá trị là $-\frac{p(p-2)(p^2-2p-1)}{2}(x+1)^2$, chia hết cho p^{2r+1} nên chia hết cho p^{r+2}
- Hạng tử với $k = 1$: giá trị là $p(p-2)(x+1)$, chia hết cho p^{r+1} nhưng không chia hết cho p^{r+2}
- Hạng tử với $k = 0$: giá trị là -1,

Vậy lũy thừa lớn nhất của p chia hết $x^{p(p-2)} + 1$ là p^{r+1}.

Nhưng ta đã biết $p^a \mid x^{p(p-2)} + 1$, nên suy ra $a \le r + 1$.

Mặt khác, $p^r \le x + 1 \le x^{p-1} + y = p^a$, do đó $a = r$ hoặc $a = r + 1$.

Nếu $a = r$, thì bất đẳng thức chỉ xảy ra khi $x = y = 1$, điều này mâu thuẫn với $p > 2$. Vậy $a = r + 1$, và do $p^r \le x + 1$, nên:

$$x = \frac{x^2 + x}{x + 1} \le \frac{x^{p-1} + y}{x + 1} = \frac{p^a}{x + 1} \le \frac{p^a}{p^r} = p \implies x = p - 1$$

Do đó $r = 1$, $a = 2$. Nếu $p \ge 5$, thì:

$$p^a = x^{p-1} + y > (p-1)^4 = (p^2 - 2p + 1)^2 > (3p)^2 > p^2 = p^a, \text{ mâu thuẫn.}$$

Vậy trường hợp duy nhất là $p = 3$, và $x = 2$, $y = p^a - x^{p-1} = 9 - 4 = 5$, là lời giải. □

[3]IMO SL 2014 N5.

Ví dụ (IND 2015 TST4/P3)

[**unrated**][4]Cho $n > 1$ là một số nguyên. Chứng minh rằng có vô hạn phần tử của dãy $(a_k)_{k\geq 1}$, được xác định bởi

$$a_k = \left\lfloor \frac{n^k}{k} \right\rfloor,$$

là số lẻ. (Với số thực x, ký hiệu $\lfloor x \rfloor$ là phần nguyên của x.)

Lời giải. (Cách 1) Nếu n là số lẻ, lấy $k = n^m$ với $m = 1, 2, \ldots$. Khi đó:

$$a_k = n^{n^m - m} \text{ là số lẻ với mọi } m.$$

Bây giờ giả sử n là số chẵn, viết $n = 2t$ với $t \geq 1$ là số nguyên. Với mỗi $m \geq 2$, xét số nguyên:

$$n^{2^m} - 2^m = 2^m \cdot \left(2^{2^m - m} \cdot t^{2^m} - 1\right),$$

vì $2^m - m > 1$, nên biểu thức trong ngoặc có ước nguyên tố lẻ p.

Khi đó, đặt $k = p \cdot 2^m$, ta có:

$$n^k = (n^{2^m})^p \equiv (2^m)^p = (2^p)^m \equiv 2^m \pmod{p},$$

(vì $2^p \equiv 2 \pmod{p}$, theo định lý Fermat nhỏ).

Mặt khác, từ bất đẳng thức:

$$n^k - 2^m < n^k < n^k + 2^m(p-1),$$

ta suy ra phân số $\frac{n^k}{k}$ nằm giữa hai số nguyên liên tiếp:

$$\frac{n^k - 2^m}{p \cdot 2^m} \quad \text{và} \quad \frac{n^k + 2^m(p-1)}{p \cdot 2^m}.$$

Do đó:

$$a_k = \left\lfloor \frac{n^k}{k} \right\rfloor = \frac{n^k - 2^m}{p \cdot 2^m}.$$

Ta thấy:

$$\frac{n^k - 2^m}{p \cdot 2^m} = \frac{\frac{n^k}{2^m} - 1}{p},$$

và vì $\frac{n^k}{2^m} - 1$ là số nguyên lẻ (do $k > m$), nên a_k là số lẻ.

Với mỗi m khác nhau ta thu được các k khác nhau vì số mũ của 2 trong phân tích thừa số nguyên tố của k khác nhau. Vậy có vô hạn giá trị k sao cho a_k là số lẻ. □

[4]IMO SL 2014 N4.

Ví dụ (IRN 2015 MO/N4)

[**unrated**] Cho các số nguyên dương a, b, c, d, k, ℓ sao cho với mọi số tự nhiên n, tập các thừa số nguyên tố của hai số

$$n^k + a^n + c \quad \text{và} \quad n^\ell + b^n + d$$

là giống nhau. Chứng minh rằng $a = b$, $c = d$, và $k = \ell$.

Lời giải. (Cách 1)[5]Giả sử tồn tại các số nguyên dương a, b, c, d, k, l thỏa mãn điều kiện đề bài, nhưng (a, b, c, d, k, l) không giống nhau.

Ta xét số n có dạng:

$$n = (kp - t)(p - 1) + s$$

với p là một số nguyên tố đủ lớn, $t, s \in \mathbb{N}$ cố định.

Với cách chọn này, ta có:

$$\begin{aligned} n \equiv s \pmod{p-1} &\implies a^n \equiv a^s \pmod{p}, \quad b^n \equiv b^s \pmod{p} \\ n \equiv t + s \pmod{p} &\implies n^k \equiv (t+s)^k \pmod{p}, \quad n^l \equiv (t+s)^l \pmod{p} \end{aligned}$$

Vậy:

$$n^k + a^n + c \equiv (t+s)^k + a^s + c \pmod{p}, \; n^l + b^n + d \equiv (t+s)^l + b^s + d \pmod{p}$$

Nếu $p \mid n^k + a^n + c$, thì:

$$(t+s)^k \equiv -a^s - c \pmod{p}, \; (t+s)^l \equiv -b^s - d \pmod{p}$$

Nâng hai vế lên lũy thừa bội chung:

$$\begin{aligned} &((t+s)^k)^l = (-(a^s + c))^l, \; ((t+s)^l)^k = (-(b^s + d))^k \\ &\implies (-(a^s + c))^l \equiv (-(b^s + d))^k \pmod{p} \implies p \mid (a^s + c)^l - (b^s + d)^k. \end{aligned}$$

Giả sử:

$$P(s) := (a^s + c)^l - (b^s + d)^k$$

là đa thức khác hằng số. Thế thì $P(s)$ có vô hạn giá trị khác 0 khi s thay đổi, và do đó có vô hạn thừa số nguyên tố.

Nhưng mặt khác, với mỗi s, ta có thể chọn t và p sao cho $p \mid n^k + a^n + c$, nên $p \mid P(s)$. Điều này chỉ có thể xảy ra nếu $P(s) = 0$ với mọi $s \in \mathbb{N}$, tức là:

$$(a^s + c)^l = (b^s + d)^k \quad \text{với mọi } s \in \mathbb{N}.$$

Đặt $j = \gcd(k, l)$, và viết $k = j \cdot k', l = j \cdot l'$. Khi đó:

$$(a^s + c)^{l'} = (b^s + d)^{k'} \implies a^s + c \text{ là } k'\text{-th power}, \quad b^s + d \text{ là } l'\text{-th power}$$

Bây giờ, giả sử $k' > 1$. Với s đủ lớn, a^s sẽ chiếm ưu thế lớn hơn c, nên $a^s + c$ không thể là lũy thừa đúng của k' (do chênh lệch giữa hai số lũy thừa kề nhau rất lớn). Mâu thuẫn.

Tương tự, giả sử $l' > 1$ cũng dẫn đến mâu thuẫn. Vì vậy, để phương trình đúng với mọi s, ta phải có $k = l$ và:

$$a^s + c = b^s + d \implies a^s - b^s = d - c$$

Nhưng với s đủ lớn và $a \neq b$, hiệu $a^s - b^s$ thay đổi và không thể cố định, mâu thuẫn với $d - c$ cố định. Do đó, $a = b$, suy ra $c = d$. □

[5]Lời giải của mojyla222.

Ví dụ (RUS 2015 TST/D7/P5)

[unrated] Cho số nguyên tố $p \geq 5$. Chứng minh rằng tồn tại số nguyên dương $a < p-1$ sao cho cả hai số $a^{p-1}-1$ và $(a+1)^{p-1}-1$ đều không chia hết cho p^2.

Lời giải. [6](Cách 1) Giả sử tồn tại a sao cho $p^2 \mid a^{p-1}-1$. Khi đó

Khẳng định — $p^2 \nmid (p-a)^{p-1}$.

Chứng minh. Thật vậy:

$$(p-a)^{p-1} = \sum_{i=0}^{p-1} \binom{p-1}{i} p^{p-1-i}(-a)^i \equiv a^{p-1} - 1 - (p-1)pa^{p-2} \equiv a^{p-1} - 1 + pa^{p-2} \pmod{p^2},$$

do đó:

$$(p-a)^{p-1} \equiv pa^{p-2} \not\equiv 0 \pmod{p^2}.$$

■

Giả sử phản chứng: *với mọi* $1 \leq a \leq p-2$, ta luôn có:

$$p^2 \mid a^{p-1}-1 \quad \text{hoặc} \quad p^2 \mid (a+1)^{p-1}-1.$$

Vì $p^2 \mid 1^{p-1}-1=0$, nên $a=1$ thỏa mãn giả sử phản chứng. Do đó, theo khẳng định $p^2 \nmid (p-1)^{p-1}-1$, từ đó theo giả sử phản chứng $p^2 \mid (p-2)^{p-1}-1$.

Áp dụng khai triển nhị thức:

$$(p-2)^{p-1} \equiv 2^{p-1} - p(p-1)2^{p-2} \pmod{p^2}$$

Vì $p^2 \mid (p-2)^{p-1}-1$, suy ra:

$$p^2 \mid 2^{p-1} - 1 + p2^{p-2}.$$

Nhân hai vế với $2^{p-1}+1$, ta được:

$$p^2 \mid (2^{p-1}+1)(2^{p-1}-1+p2^{p-2}) = 4^{p-1} - 1 + p2^{p-2}(2^{p-1}+1). \tag{1}$$

Mặt khác, lần lượt theo giả sử phản chứng và khẳng định:

$$p^2 \nmid 2^{p-1}-1 \implies p^2 \mid 3^{p-1}-1 \implies p^2 \nmid (p-3)^{p-1}-1 \implies p^2 \mid (p-4)^{p-1}-1.$$

Suy ra:

$$p^2 \mid 4^{p-1} - 1 + p4^{p-2}. \tag{2}$$

So sánh (1) và (2), ta có:

$$p \mid 4^{p-2} + 2^{p-2}.$$

Nhưng, theo định lý Fermat nhỏ:

$$4(4^{p-2}+2^{p-2}) = 4^{p-1} + 2 \cdot 2^{p-1} \equiv 3 \pmod{p}, \text{ mâu thuẫn!}$$

Vì vậy, giả thiết phản chứng sai.

Vậy tồn tại ít nhất một số $a < p-1$ sao cho cả $a^{p-1}-1$ và $(a+1)^{p-1}-1$ đều không chia hết cho p^2. □

[6]Lời giải của HoshimiyaMukuro.

5.3 Bài tập

Bài tập (JPN 2015 MO1/P3). [**unrated**] Một dãy số nguyên dương $\{a_n\}_{n=1}^{\infty}$ được gọi là *tăng mạnh* nếu với mọi số nguyên dương n, ta có:

$$a_n < a_{n+1} < a_n + a_{n+1} < a_{n+2}.$$

(a) Chứng minh rằng nếu $\{a_n\}$ là dãy tăng mạnh thì các số nguyên tố lớn hơn a_1 chỉ xuất hiện hữu hạn lần trong dãy.

(b) Chứng minh rằng tồn tại dãy $\{a_n\}$ tăng mạnh sao cho không có số nào chia hết cho bất kỳ số nguyên tố nào đã xuất hiện trong dãy.

Chương 6

Các hàm số học

6.1 Lý thuyết

Định nghĩa (Hàm số học)**.** $f:\ \mathbb{N}\to\mathbb{C}$ là một hàm số học.

Định nghĩa (Phần nguyên)**.** $\lfloor\circ\rfloor:\ \mathbb{R}\to\mathbb{Z}$ là một hàm thỏa mãn điều kiện $\lfloor x\rfloor=n$, trong đó $n\in\mathbb{Z},\ n\le x<n+1$. $\lfloor x\rfloor$ được gọi là phần nguyên, hàm sàn, hoặc sàn của x.

Định nghĩa (Hàm Trần)**.** $\lceil\circ\rceil:\ \mathbb{R}\to\mathbb{Z}$ là một hàm thỏa mãn điều kiện $\lceil x\rceil=n$, trong đó $n\in\mathbb{Z},\ n-1\le x\le n$. $\lceil x\rceil$ được gọi là hàm trần, hoặc trần của x.

Định nghĩa (Phần thập phân)**.** $\{x\}:\ \mathbb{R}\to[0,1)$ là một hàm thỏa mãn điều kiện $\{x\}=x-\lfloor x\rfloor$. $\{x\}$ được gọi là phần thập phân của x.

Định nghĩa (Hàm cộng tính)**.** Một hàm số học $f:\ \mathbb{N}\to\mathbb{C}$ được gọi là **cộng tính** nếu thỏa mãn:

$$f(mn)=f(m)+f(n),\quad \forall m,n\in\mathbb{N},\ (m,n)=1.$$

Định nghĩa (Hàm nhân tính)**.** Một hàm số học $f:\ \mathbb{N}\to\mathbb{C}$ được gọi là **nhân tính** nếu thỏa mãn:

$$f(mn)=f(m)f(n),\quad \forall m,n\in\mathbb{N},\ (m,n)=1.$$

Định nghĩa (Hàm số ước số dương)**.** Với $n\in\mathbb{Z}^+,\ n=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$, $\tau(n)=(1+a_1)(1+a_2)\cdots(1+a_k)$. $d(n)$ cũng được dùng thay cho $\tau(n)$.

Định nghĩa (Hàm tổng lũy thừa ước số dương)**.** Với $n\in\mathbb{N}$, σ_k là tổng các k^{h} lũy thừa của các ước số dương của n.

$$\sigma_k(n)=\sum_{d\mid n}d^k.$$

$d(n)$ hoặc $\tau(n)$ ký hiệu cho $\sigma_0(n)$, tức số ước của n, và $\sigma(n)$ ký hiệu cho $\sigma_1(n)$, tức tổng các ước số của n.

Định lý (Công thức cho $\sigma(n)$)
Với $n\in\mathbb{Z}^+$, $n=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$, thì

$$\sigma(n)=\frac{p_1^{a_1+1}-1}{p_1-1}\cdot\frac{p_2^{a_2+1}-1}{p_2-1}\cdots\frac{p_k^{a_k+1}-1}{p_k-1}.$$

Định nghĩa (Hàm Euler's Totient)**.** Với $n \in \mathbb{Z}^+$, $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, thì $\varphi(n)$ là số các số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n.

Định lý (Công Thức Cho $\varphi(n)$)
Với $n \in \mathbb{Z}^+$, $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, thì

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right),$$
$$\varphi(n) = p_1^{a_1-1} p_2^{a_2-1} \cdots p_k^{a_k-1}(p_1 - 1)(p_2 - 1)\cdots(p_k - 1).$$

Bổ đề (Các hàm nhân tính cơ bản)
Các hàm $d(n)$, $\sigma(n)$ và $\varphi(n)$ là các hàm nhân.

Định lý 6.1.1 (Bổ đề Bertrand)
Với mọi số nguyên $n \geq 1$, luôn tồn tại một số nguyên tố p thỏa mãn:

$$n < p < 2n.$$

6.2 Các ví dụ

Ví dụ (CHN 2015 TST3/D2/P3)

[**unrated**] Với mọi số tự nhiên n, định nghĩa:

$$f(n) = \tau(n!) - \tau((n-1)!),$$

trong đó $\tau(a)$ là số ước số dương của a.

Chứng minh rằng tồn tại vô hạn số n là hợp số sao cho với mọi số tự nhiên $m < n$, ta có:

$$f(m) < f(n).$$

Lời giải. (Cách 1)[1]Cho p là một số nguyên tố lẻ. Theo Bổ đề Bertrand, tồn tại số nguyên tố giữa p và $2p$. Giả sử q là số nguyên tố lớn nhất trong các số nguyên tố giữa p và $2p$. Ta chứng minh khẳng định sau

Khẳng định — $f(2p) > f(q)$.

Chứng minh. Ta có:

$$\begin{aligned} f(2p) &= \tau((2p)!) - \tau((2p-1)!) = \frac{3}{2} \cdot \tau(2(2p-1)!) - \tau((2p-1)!) \\ &= 3\tau\left(\frac{2(2p-1)!}{q}\right) - 2\tau\left(\frac{(2p-1)!}{q}\right) > \tau\left(\frac{(2p-1)!}{q}\right) \geq \tau((q-1)!) = f(q). \end{aligned}$$

■

Gọi n là số nguyên dương nhỏ nhất thỏa mãn $n \leq 2p$ và $f(n)$ đạt giá trị lớn nhất trong dãy $f(1), f(2), \ldots, f(2p)$.

Nếu $n \leq q$, thì $f(n) \leq \tau((q-1)!) = f(q) < f(2p)$, mâu thuẫn. Do đó, $n > q$, và từ định nghĩa của q, ta suy ra n là hợp số và $f(n) > f(m)$ với mọi $m < n$.

Hơn nữa, vì $n \in [p+1, 2p+1]$, ta có vô hạn giá trị n khi p chạy qua tất cả các số nguyên tố lẻ. □

[1]Lời giải của chirita.andrei.

Ví dụ (IMO 2015/N1)

[**unrated**] Xác định tất cả các số nguyên dương M sao cho dãy số $a_0, a_1, a_2, \ldots$ được xác định bởi

$$a_0 = M + \frac{1}{2} \quad \text{and} \quad a_{k+1} = a_k \lfloor a_k \rfloor \quad \text{với } k = 0, 1, 2, \ldots$$

chứa ít nhất một số nguyên.

Lời giải. [2](Cách 2) Xét $b_k = 2a_k$ với mọi $k \geq 0$. Khi đó,

$$b_{k+1} = 2a_{k+1} = 2a_k \lfloor a_k \rfloor = b_k \lfloor \frac{b_k}{2} \rfloor.$$

Vì b_0 là một số nguyên, suy ra b_k là một số nguyên với mọi $k \geq 0$.

Giả sử rằng dãy $a_0, a_1, a_2, \ldots$ không chứa số nguyên nào. Khi đó, b_k phải là số nguyên lẻ với mọi $k \geq 0$, do đó

$$b_{k+1} = b_k \lfloor b_k/2 \rfloor = \frac{b_k(b_k - 1)}{2}. \tag{1}$$

Từ đó, ta có

$$b_{k+1} - 3 = \frac{b_k(b_k - 1)}{2} - 3 = \frac{(b_k - 3)(b_k + 2)}{2}, \text{ với mọi } k \geq 0. \tag{2}$$

Giả sử rằng $b_0 - 3 \neq 0$. Khi đó, phương trình (2) cho ta $b_k - 3 \neq 0$ với mọi $k \geq 0$.

Với mỗi $k \geq 0$, định nghĩa c_k là lũy thừa lớn nhất của 2 chia hết cho $b_k - 3$. Vì $b_k - 3$ là số chẵn với mọi $k \geq 0$, số c_k luôn dương.

Lưu ý rằng $b_k + 2$ là một số nguyên lẻ. Do đó, từ phương trình (2), ta có

$$c_{k+1} = c_k - 1.$$

Như vậy, dãy $c_0, c_1, c_2, \ldots$ của các số nguyên dương là một dãy **giảm nghiêm ngặt**, mâu thuẫn với Nguyên lý cực hạn cho tập hợp các số nguyên dương.

Vậy, ta phải có $b_0 - 3 \leq 0$, suy ra $M = 1$.

Với $M = 1$, có thể kiểm tra rằng dãy số là hằng với $a_k = \frac{3}{2}$ với mọi $k \geq 0$. Do đó, đáp án là $M \geq 2$. □

[2]Shortlist 2015 with solutions.

6.3 Bài tập

Chương 7

Phương trình Diophantine

7.1 Lý thuyết

7.2 Các ví dụ

Ví dụ (KOR 2015 MO/P1)

[unrated] Với mỗi số nguyên dương m, (x, y) là một cặp số nguyên dương thỏa mãn hai điều kiện:

(i) $x^2 - 3y^2 + 2 = 16m$,

(ii) $2y \leq x - 1$.

Chứng minh rằng số lượng các cặp như vậy là số chẵn hoặc bằng 0.

Lời giải. (Cách 1)[1]Nếu không tồn tại nghiệm nào, ta có số nghiệm là 0, thỏa yêu cầu. Giả sử tồn tại một nghiệm $(u, v) \in \mathbb{Z}^2_{>0}$ thỏa mãn hai điều kiện.

Định nghĩa ánh xạ:

$$(u, v) \longmapsto (u', v') = (2u - 3v,\ u - 2v).$$

Bước 1. $(u', v') \in \mathbb{Z}^2_{>0}$. Từ điều kiện $u - 1 \geq 2v \implies u \geq 2v + 1$, ta có:

$$u' = 2u - 3v \geq 2(2v + 1) - 3v = v + 2 \geq 3, \quad v' = u - 2v \geq 1.$$

Bước 2. Ánh xạ bảo toàn phương trình:

$$(u')^2 - 3(v')^2 + 2 = (2u - 3v)^2 - 3(u - 2v)^2 + 2 \qquad = u^2 - 3v^2 + 2 = 16m.$$

Bước 3. Ánh xạ bảo toàn bất đẳng thức:

$$2v' \leq u' - 1 \Leftrightarrow 2(u - 2v) \leq (2u - 3v) - 1 \Leftrightarrow v \geq 1.$$

Bước 4. Ánh xạ là một Hàm số tự nghịch đảo:

$$T(T(u, v)) = (u, v).$$

Bước 5. Không có điểm bất biến (tức nghiệm cố định). Nếu $(u, v) = (2u - 3v,\ u - 2v) \implies u = 3v$, thay vào:

$$x = 3v \implies x^2 - 3y^2 + 2 = 6v^2 + 2 = 16m \implies v^2 = \frac{16m - 2}{6} \implies v^2 \equiv 5 \pmod 8, \text{ vô lý.}$$

Do đó, ánh xạ chia tập nghiệm thành các cặp phân biệt, nên số nghiệm là số chẵn hoặc 0. □

[1]Lời giải chính thức.

Ví dụ (USA 2015 MO/P1)
[**15M**] Giải trong tập số nguyên phương trình

$$x^2 + xy + y^2 = \left(\frac{x+y}{3} + 1\right)^3.$$

Lời giải. (Cách 1)[2]Trước tiên ta nhận thấy cả hai vế đều phải là số nguyên, do đó $\frac{x+y}{3}$ phải là số nguyên.

Do đó ta đặt $x + y = 3t$ với t là một số nguyên.

Khi đó:

$$(3t)^2 - xy = (t+1)^3 \implies 9t^2 + x(x-3t) = t^3 + 3t^2 + 3t + 1$$
$$4x^2 - 12xt + 9t^2 = 4t^3 - 15t^2 + 12t + 4 \implies (2x-3t)^2 = (t-2)^2(4t+1)$$

$4t + 1$ là bình phương của một số lẻ và có thể thay bằng $(2n+1)^2$. Thay $t = n^2 + n$ ta được:

$$(2x - 3n^2 - 3n)^2 = [(n^2 + n - 2)(2n+1)]^2 \implies 2x - 3n^2 - 3n = \pm(2n^3 + 3n^2 - 3n - 2)$$
$$x = n^3 + 3n^2 - 1 \quad \text{hoặc} \quad x = -n^3 + 3n + 1$$

Thay ngược lại ta được các nghiệm:

$$(n^3 + 3n^2 - 1,\ -n^3 + 3n + 1) \cup (-n^3 + 3n + 1,\ n^3 + 3n^2 - 1).$$

□

[2]Lời giải chính thức.

Ví dụ (USA 2015 MO/P5)

[**30M**] Cho các số nguyên dương phân biệt a, b, c, d, e sao cho

$$a^4 + b^4 = c^4 + d^4 = e^5.$$

Chứng minh rằng $ac + bd$ là một hợp số.

Lời giải. (Cách 1)[3]Giả sử ngược lại rằng $ac + bd$ là một số nguyên tố.

Không mất tính tổng quát, giả sử $a > d$. Vì $a^4 + b^4 = c^4 + d^4$, nên suy ra $b < c$.

Xét biểu thức:

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

Vì $a^4 + b^4 = c^4 + d^4 = e^5$, ta có:

$$e^5(cd - ab)(cd + ab) = (ac - bd)(ac + bd)(ad - bc)(ad + bc).$$

Nếu $ac - bd = 0$ hoặc $ad - bc = 0$, thì ta sẽ có $\frac{a}{b} = \frac{c}{d}$ hoặc $\frac{a}{b} = \frac{d}{c}$. Điều này mâu thuẫn với giả thiết rằng $a^4 + b^4 = c^4 + d^4$ và các số a, b, c, d đều phân biệt.

Do đó, tất cả các thừa số ở vế phải đều khác 0, nên $ac + bd$ phải chia hết vế trái:

$$ac + bd \mid e^5(cd - ab)(cd + ab).$$

Giả sử $ac + bd$ là một số nguyên tố. Xét hiệu:

$$(ac + bd) - (cd + ab) = (a - d)(c - b) > 0,$$

suy ra $ac + bd > cd + ab > cd - ab$, nên không thể $ac + bd$ chia hết $cd + ab$ hoặc $cd - ab$. Do đó, $ac + bd$ phải chia hết e^5.

Suy ra tồn tại $k \in \mathbb{Z}^+$ sao cho:

$$e = k(ac + bd)^{1/5}.$$

Nhưng điều này là vô lý vì khi đó:

$$(k(ac + bd))^5 > a^4 + b^4 = e^5.$$

Mâu thuẫn.

Vậy giả thiết ban đầu sai. Suy ra $ac + bd$ không thể là số nguyên tố. Do đó, $ac + bd$ là một hợp số. □

[3]Lời giải chính thức.

7.3 Bài tập

Bài tập (RUS 2015 TST/D10/P3)**.** [**unrated**] Tìm tất cả các số nguyên k sao cho tồn tại vô số bộ ba số nguyên (a, b, c) thỏa mãn:

$$(a^2 - k)(b^2 - k) = c^2 - k.$$

Chương 8

Số học đồng dư nâng cao

8.1 Lý thuyết

8.2 Các ví dụ

8.3 Bài tập

Chương 9

Luỹ thừa lớn nhất

9.1 Lý thuyết

Định nghĩa (Chuẩn p-adic)**.** Trong số học, chuẩn p-adic (hoặc bậc p-adic) của một số nguyên n là số mũ của lũy thừa lớn nhất của số nguyên tố p mà n chia hết.

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

Nói một cách khác, chuẩn p-adic là số mũ của p trong phân tích thừa số nguyên tố của n:

$$n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \ldots {p_k}^{\alpha_k} \implies \nu_{p_i}(n) = \alpha_i, \ \forall\, i = 1, 2, \ldots, k.$$

trong đó $p_1, p_2, \ldots, p_k$ là các số nguyên tố và $\alpha_1, \alpha_2, \ldots, \alpha_k$ là các số nguyên dương.

Định lý (Định lý Kummer)

Cho p là một số nguyên tố và m, n là hai số nguyên dương. Khi đó, số mũ của p trong ước số nguyên tố của hệ số nhị thức $\binom{m}{n}$ được xác định bởi:

$$v_p\left(\binom{m}{n}\right) = \frac{S_p(m) - S_p(n) - S_p(m-n)}{p-1},$$

trong đó $S_p(x)$ là tổng các chữ số trong biểu diễn cơ số p của x.

9.2 Các ví dụ

Ví dụ (CHN 2015 MO/P4)

[**unrated**] Xác định tất cả các số nguyên k sao cho tồn tại vô hạn số nguyên dương n không thỏa mãn:

$$n+k \mid \binom{2n}{n}.$$

Lời giải. (Cách 1)[1]

Ta xét ba trường hợp sau.

Trường hợp 1: Nếu $k=0$, ta có thể chọn $n=2^\alpha$ với mọi số nguyên dương $\alpha \geq 2$. Theo định lý Kummer, ta có

$$v_2\left(\binom{2n}{n}\right) = 1 < \alpha = v_2(2^\alpha) = v_2(n+k).$$

Trường hợp 2: Nếu $k \neq 0, 1$, với mọi số nguyên dương $\alpha \geq 3 + \log_2 |k|$, ta có thể chọn $n = 2^\alpha - k$. Trong hệ cơ số p, n có nhiều nhất α chữ số, với chữ số ít quan trọng nhất bằng 0. Do đó, có nhiều nhất $\alpha - 1$ lần nhớ khi cộng n vào chính nó[2], và do đó theo định lý Kummer, ta có

$$v_2\left(\binom{2n}{n}\right) \leq \alpha - 1 < \alpha = v_2(n+k).$$

Trường hợp 3: Nếu $k=1$, ta có

$$\frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \frac{n}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n+1}$$

là một số nguyên, do đó $(n+1) \mid \binom{2n}{n}$ với mọi n.

Vậy, tất cả các số nguyên $k \neq 1$ đều thỏa mãn điều kiện.

(*Lưu ý rằng:* $\frac{1}{n+1}\binom{2n}{n}$ *là một số Catalan.*) □

[1] Lời giải của yunxiu.
[2] Divisors of the middle binomial coefficient.

Ví dụ (CHN 2015 TST3/D1/P3)

[**unrated**] Cho a, b là hai số nguyên sao cho ước chung lớn nhất của chúng có ít nhất hai thừa số nguyên tố. Đặt

$$S = \{x \mid x \in \mathbb{N}, x \equiv a \pmod{b}\}$$

và gọi $y \in S$ là *không thể phân tích* nếu nó không thể được biểu diễn dưới dạng tích của hai hoặc nhiều phần tử của S (không nhất thiết phải khác nhau). Chứng minh rằng tồn tại một số t sao cho mọi phần tử của S có thể được biểu diễn dưới dạng tích của nhiều nhất t phần tử không thể phân tích.

Lời giải. (Cách 1)[3]Gọi $g = \gcd(a, b)$, khi đó ta có:

$$a = ga', \quad b = gb'.$$

Xét hai trường hợp:

Trường hợp 1: $\gcd(b', g) > 1$ Chọn một số nguyên tố p sao cho $p \mid b'$ và $p \mid g$. Khi đó, $p \nmid a'$, suy ra:

$$\nu_p(a) = \nu_p(g) < \nu_p(b).$$

Với mọi $x \in S$, ta có $\nu_p(x) = \nu_p(a)$, tức là mọi x đều có cùng số mũ tại p. Do đó, không thể phân tích thành tích của hai số khác trong S, nên mọi x trong trường hợp này là không thể phân tích. Trường hợp này là hiển nhiên.

Trường hợp 2: $\gcd(b', g) = 1$ Chọn hai số nguyên tố p, q sao cho $p, q \mid g$. Xét một phần tử $x \in S$:

- Nếu x không thể phân tích, ta hoàn thành chứng minh.
- Nếu x có thể phân tích, viết $x = uv$ với $u, v \in S$.

Ta sử dụng phép biến đổi:

$$(u, v) \to \left(p^{\varphi(b')}u, \frac{v}{p^{\varphi(b')}}\right).$$

Lý do phép biến đổi hợp lệ là do:

1. Không thay đổi phần dư modulo b': Vì $p^{\varphi(b')} \equiv 1 \pmod{b'}$.
2. Không thay đổi phần dư modulo b: Vì chỉ làm tăng số mũ của thừa số nguyên tố trong g, không ảnh hưởng đến $\pmod{b}$.

Lặp lại quá trình này đến khi:

$$\nu_p(v) \le \varphi(b') + \nu_p(g), \quad \nu_q(u) \le \varphi(b') + \nu_q(g).$$

Vì mọi phép phân tích tiếp theo của u, v yêu cầu mỗi thừa số phải chia hết cho $p^{\nu_p(g)}$ và $q^{\nu_q(g)}$, số thừa số bị chặn bởi:

$$t = \frac{\varphi(b') + \nu_p(g)}{\nu_p(g)} + \frac{\varphi(b') + \nu_q(g)}{\nu_q(g)}.$$

Do t là số hữu hạn, mọi phần tử của S có thể được phân tích thành nhiều nhất t phần tử không thể phân tích, chứng minh được hoàn tất. □

[3]Lời giải của MarkBcc168.

Ví dụ (IMO 2015/P2)

[**30M**] Hãy tìm tất cả các bộ số nguyên dương (a, b, c) sao cho mỗi số trong các số:

$$ab - c, bc - a, ca - b$$

là lũy thừa của 2.

Lời giải. [4](Cách 2) Chúng ta sẽ chứng minh rằng các nghiệm duy nhất là $(2, 2, 2)$, $(2, 2, 3)$, $(2, 6, 11)$ và $(3, 5, 7)$, cùng với các hoán vị của chúng.

Không mất tính tổng quát, giả sử rằng $a \geq b \geq c > 1$, khi đó

$$ab - c \geq ca - b \geq bc - a.$$

Ta xét các trường hợp sau:

Trường hợp 1: Nếu a là số chẵn, thì

$$ca - b = \gcd(ab - c, ca - b) \leq \gcd(ab - c, a(ca - b) + ab - c) = \gcd\left(ab - c, c(a^2 - 1)\right).$$

Vì $a^2 - 1$ là số lẻ, ta suy ra $ca - b \leq c$. Điều này dẫn đến $a = b = c = 2$.

Trường hợp 2: Nếu a, b, c đều là số lẻ, thì $a > b > c > 1$. Khi đó, cũng như trên:

$$ca - b \leq \gcd(ab - c, c(a^2 - 1)) \leq 2^{\nu_2(a^2-1)} \leq 2a + 2 \leq 3a - b.$$

Do đó, $c = 3$ và $a = b + 2$. Vì $3a - b = ca - b \geq 2(bc - a) = 6b - 2a$, ta suy ra $a = 7$ và $b = 5$.

Trường hợp 3: Nếu a là số lẻ và b, c là số chẵn, thì

$$\begin{aligned}
&bc - a = 1 \implies bc^2 - b - c = ca - b, \\
\implies\ & c^3 - b - c = (1 - c^2)(ab - c) + a(\underbrace{bc^2 - b - c}_{=ca-b}) + (ca - b), \\
\implies\ & \gcd(ab - c, ca - b) = \gcd(ab - c, c^3 - b - c,) \\
\implies\ & bc^2 - b - c = ca - b = \gcd(ab - c, ca - b) = \gcd(ab - c, c^3 - b - c).
\end{aligned}$$

Khi đó, ta xét hai trường hợp con sau:

Trường hợp 3a: $c^3 - b - c \neq 0$, thì biểu thức trên dẫn đến

$$|c^3 - b - c| \geq bc^2 - b - c,\ b \geq c > 1 \implies b = c \implies a = c^2 - 1.$$

Cuối cùng, $ab - c = c(c^2 - 2)$ là một lũy thừa của 2, dẫn đến $b = c = 2$, nên $a = 3$.

Trường hợp 3b: $c^3 - b - c = 0$, tức là $c^3 = c$. Từ

$$bc - a = 1 \implies a = c^4 - c^2 - 1 \implies ca - b = c^5 - 2c^3 = c^3(c^2 - 2).$$

Vì đây là một lũy thừa của 2, ta suy ra $c = 2$. Khi đó, $a = 11$ và $b = 6$.

Vậy ta đã xét hết tất cả các trường hợp, hoàn tất chứng minh. □

[4]Lời giải của TelvCohl.

Ví dụ (IMO 2023/P1)

[**5M**] Xác định tất cả các số nguyên hợp 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 $1 \leq i \leq k-2$.

Lời giải. (Cách 4)[5]Dễ thấy rằng $n = p^r$ với $r \geq 2$ thỏa mãn điều kiện vì

$$d_i = p^{i-1}, \text{ với } 1 \leq i \leq k = r+1 \text{ và rõ ràng } p^{i-1} \mid (p^i + p^{i+1}).$$

Bây giờ, giả sử tồn tại một số nguyên n thỏa mãn điều kiện đã cho và có ít nhất hai thừa số nguyên tố phân biệt, gọi là p và q, với $p < q$ là hai thừa số nguyên tố nhỏ nhất của n.

Tồn tại số nguyên j sao cho:

$$d_1 = 1, d_2 = p, \ldots, d_j = p^{j-1}, d_{j+1} = p^j, d_{j+2} = q.$$

Ta cũng có:

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

Từ điều kiện đề bài:

$$d_{k-j-1} \mid (d_{k-i} + d_{k-j+1}) \implies \frac{n}{q} \mid \left(\frac{n}{p^j} + \frac{n}{p^{j-1}}\right) \quad (1)$$

Ta sử dụng $v_p(m)$ để biểu diễn Chuẩn p-adic của m. Lưu ý rằng:

$$v_p\left(\frac{n}{q}\right) = v_p(n) \text{ do } \gcd(p,q) = 1.$$

và

$$v_p\left(\frac{n}{p^j}(p+1)\right) = v_p(n) - j \text{ do } \gcd(p, p+1) = 1.$$

Từ (1), suy ra:

$$v_p(n) = v_p\left(\frac{n}{q}\right) \leq v_p\left(\frac{n}{p^j}(p+1)\right) = v_p(n) - j,$$

mâu thuẫn. Vậy n chỉ có một ước số nguyên tố, hoàn thành chứng minh. □

[5]Shortlist 2023 with solutions.

Ví dụ (RUS 2015 MO11/P2)

[**unrated**] Cho số tự nhiên $n > 1$. Ta viết ra các phân số

$$\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}$$

và chỉ giữ lại những phân số tối giản. Gọi tổng các tử số (của những phân số tối giản đó) là $f(n)$. Hỏi có những giá trị $n > 1$ nào sao cho một trong hai số $f(n)$ và $f(2015n)$ là số lẻ, còn số kia là số chẵn?

Lời giải. (Cách 1)[6]Rõ ràng với mọi $m < n$, các tử số rút gọn $\frac{m}{\gcd(m,n)}$ và $\frac{m}{\gcd(m,2015n)}$ có cùng tính chẵn lẻ. Do đó, để so sánh tính chẵn lẻ của $f(n)$ và $f(2015n)$, ta chỉ cần xét tổng:

$$\sum_{i=1}^{2015n-1} \frac{i}{\gcd(i, 2015n)}.$$

Xét điều kiện để $\frac{i}{\gcd(i,2015n)}$ là số lẻ:

$$2 \nmid \frac{i}{\gcd(i, 2015n)} \iff v_2\left(\frac{i}{\gcd(i, 2015n)}\right) = 0.$$

Vì $\gcd(i, 2015n)$ chia hết cho $2^{\min(v_2(i), v_2(2015n))}$, nên biểu thức trên tương đương với:

$$v_2(i) \leq v_2(2015n) = v_2(n), \text{ do 2015 là số lẻ.}$$

Suy ra, số lượng chỉ số $i \in [1, 2015n-1]$ sao cho $\frac{i}{\gcd(i,2015n)}$ là số lẻ bằng số lượng i thỏa $v_2(i) \leq v_2(n)$.

Số lượng này lớn hơn một nửa tổng số và cụ thể là lẻ, vì số các i với $v_2(i) = v_2(n)$ là bội của $2^{v_2(n)}$ và tạo thành cấp số cộng cách đều, nên tổng số các giá trị i thỏa mãn điều kiện là lẻ.

Do đó tổng

$$\sum_{i=1}^{2015n-1} \frac{i}{\gcd(i, 2015n)} \text{ là số lẻ,}$$

kéo theo $f(2015n)$ và $f(n)$ có tính chẵn lẻ khác nhau. □

[6]Lời giải của JAnatolGT_00.

Lời giải. (Cách 2)[7]Gọi $v_2(n)$ là chuẩn 2-adic của n.

Phân số $\frac{i}{n}$ có tử số chẵn *nếu và chỉ nếu* $v_2(i) > v_2(n)$. Do đó, số lượng tử số lẻ là:

$$f(n) \equiv n - 1 - \left\lfloor \frac{n}{2^{v_2(n)+1}} \right\rfloor \pmod 2.$$

Tương tự:

$$f(2015n) \equiv 2015n - 1 - \left\lfloor \frac{2015n}{2^{v_2(n)+1}} \right\rfloor \pmod 2.$$

Do đó, khác biệt về chẵn lẻ giữa $f(n)$ và $f(2015n)$ phụ thuộc vào:

$$\left\lfloor \frac{n}{2^{v_2(n)+1}} \right\rfloor \text{ và } \left\lfloor \frac{2015n}{2^{v_2(n)+1}} \right\rfloor.$$

Đặt $n = 2^\alpha \beta$ với β lẻ. Khi đó:

$$\left\lfloor \frac{n}{2^{\alpha+1}} \right\rfloor = \left\lfloor \frac{\beta}{2} \right\rfloor, \left\lfloor \frac{2015n}{2^{\alpha+1}} \right\rfloor = \left\lfloor \frac{2015\beta}{2} \right\rfloor = \left\lfloor 1007\beta + \frac{\beta}{2} \right\rfloor.$$

Vì β lẻ nên 1007β lẻ, và do đó hai phần nguyên này có tính chẵn lẻ khác nhau.

Suy ra $f(n)$ và $f(2015n)$ có tính chẵn lẻ khác nhau với mọi $n > 1$. □

[7]Lời giải của kreegyt.

9.3 Bài tập

Chương 10

Đa thức nguyên

Chương 11

Phần dư bậc hai

11.1 Lý thuyết

Định lý (Định lý Fermat về tổng hai số chính phương)
Một số nguyên tố lẻ p có thể được biểu diễn dưới dạng tổng của hai số chính phương nếu và chỉ nếu $p \equiv 1 \pmod 4$, tức là tồn tại các số nguyên x, y sao cho

$$p = x^2 + y^2.$$

11.2 Các ví dụ

Ví dụ (CHN 2015 TST2/D2/P3)
[**unrated**] Chứng minh rằng tồn tại vô hạn số nguyên n sao cho n^2+1 là số không có ước chính phương.

Lời giải. (Cách 1)[1]Trước hết ta chứng minh khẳng định sau với mọi số nguyên tố p.

Khẳng định — Phương trình $x^2 \equiv -1 \pmod{p^2}$ có không quá 2 nghiệm trong tập $\{0, 1, \ldots, p^2-1\}$.

Chứng minh. Trường hợp $p = 2$ có thể dễ dàng kiểm tra trực tiếp, nên ta giả sử p là số lẻ.

Giả sử phản chứng rằng tồn tại ít nhất ba số nguyên phân biệt a, b, c sao cho:

$$a^2+1 \equiv b^2+1 \equiv c^2+1 \equiv 0 \pmod{p^2} \implies a^2 \equiv b^2 \pmod{p^2} \implies p^2 \mid (a-b)(a+b). \quad (1)$$

Xét hai trường hợp:

Trường hợp 1: $p \mid a-b$. Khi đó, vì $|a-b| < p^2$, ta có $p^2 \nmid a-b$. Từ (1), suy ra $p \mid a+b$. Xét tổng và hiệu:

$$p \mid (a-b)+(a+b) = 2a, \quad p \mid (a+b)-(a-b) = 2b.$$

Do $p \neq 2$, suy ra $p \mid a$, nhưng điều này mâu thuẫn với giả thiết $p^2 \mid a^2+1$.

Trường hợp 2: $p \nmid a-b$. Từ (1), ta suy ra $p^2 \mid a+b$. Tương tự, có thể chứng minh $p^2 \mid a+c$.

Suy ra $p^2 \mid (a+c)-(a+b) = b-c$. Vì $|b-c| < p^2$, ta có $b = c$, mâu thuẫn với giả thiết ban đầu. ■

Gọi $\mathrm{X}(n)$ và $\mathrm{P}_{4,1}(n)$ là hai tập hợp sau:

$$\mathrm{X}(n) = \{x \mid x^2+1 \text{ có ước chính phương}\}.$$
$$\mathrm{P}_{4,1}(n) = \{p \mid p \text{ là số nguyên tố}, \ p \equiv 1 \pmod 4\}.$$

Theo khẳng định trên, $x^2 \equiv -1 \pmod{p^2}$ trong khoảng $[0, n-1]$ có số nghiệm không vượt quá:

$$2 \cdot \frac{n}{p^2} + 2.$$

Do đó tổng số phần tử trong $\mathrm{X}(n)$:

$$|\mathrm{X}(n)| \leq \sum_{p \in \mathrm{P}_{4,1}(n)} \left(2 + \frac{2n}{p^2}\right) \leq 2|\mathrm{P}_{4,1}(n)| + 2n \sum_{p \in \mathrm{P}_{4,1}(n)} \frac{1}{p^2}.$$

Số lượng số nguyên tố $p \leq n$ thỏa mãn $p \equiv 1 \pmod 4$ được ước lượng bởi:

$$|\mathrm{P}_{4,1}(n)| \leq 1 + \frac{n}{4}.$$

Theo Bất đẳng thức Chuỗi Xen Kẽ, ta có:

$$\sum_p \frac{2}{p^2} < \frac{1}{4} \implies 2n \sum_p \frac{1}{p^2} < \frac{n}{6} \implies |\mathrm{X}(n)| \leq 2 + \frac{2n}{3}.$$

Từ đó, số phần tử x nhỏ hơn n sao cho x^2+1 không có ước chính phương ít nhất là:

$$n - |\mathrm{X}(n)| \geq \frac{n}{3} - 2.$$

Vì $\frac{n}{3} - 2$ có thể lớn tùy ý khi n tăng, nên có vô hạn số n sao cho n^2+1 không có ước chính phương. □

[1]Lời giải của rafayaashary1.

Ví dụ (IRN 2015 MO/N3)

[**unrated**] Cho $p > 5$ là một số nguyên tố. Gọi $A = \{b_1, b_2, \ldots, b_{\frac{p-1}{2}}\}$ là tập tất cả các bình phương đồng dư modulo p, loại trừ 0. Chứng minh rằng không tồn tại các số tự nhiên a, c sao cho $\gcd(ac, p) = 1$ và tập

$$B = \{ab_1 + c, ab_2 + c, \ldots, ab_{\frac{p-1}{2}} + c\} \pmod p$$

không giao A, tức là $A \cap B = \emptyset \mod p$.

Lời giải. (Cách 1)[2]Ta làm việc trong trường $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Gọi $\left(\frac{\cdot}{p}\right)$ là ký hiệu Legendre.

Trường hợp 1: $\left(\frac{a}{p}\right) = 1$

Trong trường hợp này, do tính chất nhân của ký hiệu Legendre, ta có:

$$\left(\frac{ab_i}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b_i}{p}\right) = 1 \quad \text{với mọi } i$$

Tức là ab_i vẫn là các bình phương đồng dư. Khi đó, tập $S = \{ab_1, ab_2, \ldots, ab_{\frac{p-1}{2}}\}$ chính là A.

Bây giờ giả sử $B = \{ab_i + c\}$ không giao với A. Ta sẽ chứng minh điều này dẫn đến mâu thuẫn.

Xét một phần tử $r \in \mathbb{F}_p^*$ sao cho $r^2 \not\equiv \pm c \mod p$. Vì $p > 5$, nên tồn tại ít nhất một giá trị như vậy.

Đặt $s = \frac{c}{r}$, và xét hai biểu thức:

$$x_1 = \left(\frac{r+s}{2}\right)^2, \quad x_2 = \left(\frac{r-s}{2}\right)^2 \implies x_1 - x_2 = rs = c.$$

Do đó, $x_2 + c = x_1$, nghĩa là nếu $x_2 \in A$, thì $x_2 + c \in A$, tức là tồn tại phần tử trong B cũng thuộc A, mâu thuẫn với giả thiết rằng $A \cap B = \emptyset$.

Trường hợp 2: $\left(\frac{a}{p}\right) = -1$

Khi đó, do b_i là bình phương, nên ab_i là không bình phương. Tức là tập $S = \{ab_i\}$ chính là tập các phần tử không là bình phương modulo p.

Bây giờ giả sử $B = \{ab_i + c\}$ rời nhau với A, tức là mọi phần tử của B cũng là không bình phương.

Ta xét dãy:

$$S = \{-c, -2c, \ldots, -\tfrac{p-1}{2}c\} \pmod p$$

Đây là một hoán vị (theo hệ số) của các phần tử của $S = aA$. Nếu giả thiết đúng thì dãy này gồm toàn bộ các phần tử không bình phương.

Bây giờ xét tổng các phần tử trong dãy trên. Tổng này là:

$$\sum_{i=1}^{\frac{p-1}{2}}(-ic) = -c \cdot \sum_{i=1}^{\frac{p-1}{2}} i = -c \cdot \frac{(p-1)(p+1)}{8}$$

Gọi s là tổng các phần tử trong B, thì $s \equiv \sum ab_i + \frac{p-1}{2}c \pmod p$. Ta so sánh với tổng của các phần tử trong A. Do A là đối xứng (vì với mỗi $x \in \mathbb{F}_p^*$, $x^2 \in A$), tổng của A là cố định.

Nếu phép dịch $+c$ bảo toàn tập không bình phương, thì tổng của B phải có dạng giống như tổng của S, tức là có giá trị khác tổng của A. Nhưng nếu B không trùng A và vẫn là không bình phương, thì điều này dẫn đến mâu thuẫn về tổng.

Mặt khác, nếu $c^{-1}S = \{-1, -2, \ldots, -\frac{p-1}{2}\}$, thì tập này gồm các phần tử *liên tiếp*. Nhưng tập các phần tử không bình phương modulo p không thể là một cấp số cộng kiểu đó vì nó không đóng dưới phép cộng. Do đó, $c^{-1}S$ phải là tập các bình phương, tức là:

$$\left(\frac{-1}{p}\right) = 1, \quad \text{và} \quad \left(\frac{ic}{p}\right) = 1$$

Nhưng điều này dẫn đến mâu thuẫn vì S là tập không bình phương. Do đó, mâu thuẫn.

Trong cả hai trường hợp $\left(\frac{a}{p}\right) = \pm 1$, giả thiết rằng $A \cap B = \emptyset$ đều dẫn đến mâu thuẫn. Vậy không tồn tại $a, c \in \mathbb{N}$ với $\gcd(ac, p) = 1$ sao cho B hoàn toàn nằm ngoài A modulo p. □

[2] Dựa theo lời giải của Dukejukem và rafayaashary1.

11.3 Bài tập

Chương 12

Chứng minh kiến tạo

12.1 Lý thuyết

Định lý (Định lý phần dư Trung Hoa)

Giả sử các số $n_1, n_2, \ldots, n_k$ đôi một nguyên tố cùng nhau, và $a_1, a_2, \ldots, a_k$ là các số nguyên tùy ý. Khi đó hệ phương trình đồng dư sau:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

luôn có nghiệm.

Hơn nữa, nếu x_1 và x_2 đều là nghiệm của hệ, thì chúng đồng dư modulo

$$N = \prod_{i=1}^{k} n_i, \quad \text{tức là } x_1 \equiv x_2 \pmod{N}.$$

12.2 Các ví dụ

Ví dụ (IRN 2015 MO/N1)

[**unrated**] Chứng minh rằng tồn tại vô hạn số tự nhiên n sao cho n không thể viết được dưới dạng tổng của hai số nguyên dương mà tất cả các thừa số nguyên tố của chúng đều nhỏ hơn 1394.

Lời giải. (Cách 1)[1] Gọi $p_1, p_2, \ldots, p_k$ là tất cả các số nguyên tố nhỏ hơn 1394.

Ký hiệu số tự nhiên *số P-mịn (smooth)* nếu tất cả các ước số nguyên tố đều thuộc tập $\{p_1, \ldots, p_k\}$.

Với m nguyên dương, ta ước lượng số các số nguyên dương không vượt quá m và là số P-mịn như sau:

$$x_m = (\lfloor \log_{p_1} m \rfloor + 1) \cdot (\lfloor \log_{p_2} m \rfloor + 1) \cdots (\lfloor \log_{p_k} m \rfloor + 1)$$

Lý do: Mỗi số P-mịn không vượt quá m có thể biểu diễn dưới dạng:

$$p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \leq m, \ a_i \geq 0 \tag{1}$$

Do đó số lượng tổ hợp các bộ số mũ $(a_1, a_2, \ldots, a_k)$ thỏa mãn (1) bị chặn bởi x_m.

Từ đó, số các cặp (a, b) là hai số nguyên dương P-mịn có tổng không vượt quá m bị chặn trên bởi x_m^2.

Do đó, số lượng các số tự nhiên $\leq m$ **có thể** viết được dưới dạng tổng của hai số P-mịn là không quá x_m^2.

Suy ra, số lượng các số tự nhiên $\leq m$ **không** thể biểu diễn dưới dạng tổng của hai số P-mịn là ít nhất:

$$m - x_m^2.$$

Giờ ta xét giới hạn khi $m \to \infty$. Ta thấy:

$$x_m = \prod_{i=1}^{k} (\log_{p_i} m + 1) = O((\log m)^k) \implies x_m^2 = O((\log m)^{2k}) \implies \lim_{m \to \infty} m - x_m^2 \to \infty.$$

Vì vậy, tồn tại vô hạn số tự nhiên n mà không thể viết được thành tổng của hai số nguyên dương có tất cả các thừa số nguyên tố nhỏ hơn 1394. □

[1] Dựa theo lời giải của SCLT.

Ví dụ (IRN 2015 MO/N5)

[**unrated**] Cho $p > 30$ là một số nguyên tố. Chứng minh rằng tồn tại một số trong tập sau có dạng $x^2 + y^2$ với $x, y \in \mathbb{Z}$:

$$p+1,\ 2p+1,\ 3p+1,\ \ldots,\ (p-3)p+1$$

Lời giải. (Cách 1)[2]Thực ra, mệnh đề này đúng với mọi $p \geq 7$, không chỉ $p > 30$.

Ta xét các phần tử $x, y \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$ sao cho:

$$x \equiv \pm\frac{3}{5} \pmod p, \quad y \equiv \pm\frac{4}{5} \pmod p$$

Vì $\gcd(5, p) = 1$, nên $\frac{3}{5}, \frac{4}{5} \in \mathbb{F}_p$ tồn tại. Do đó ta có:

$$x^2 + y^2 \equiv \left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = \frac{9+16}{25} = 1 \pmod p$$

Tức là tồn tại x, y sao cho $x^2 + y^2 \equiv 1 \pmod p$. Mặt khác, ta đánh giá giá trị lớn nhất mà biểu thức $x^2 + y^2$ có thể nhận được trong miền xác định:

$$x^2 + y^2 \leq 2\left(\frac{p-1}{2}\right)^2 = \frac{(p-1)^2}{2} = \frac{p^2 - 2p + 1}{2}$$

Ta muốn tìm một số dạng $mp + 1$ (với $1 \leq m \leq p-3$) có dạng $x^2 + y^2$. Vì:

$$x^2 + y^2 \equiv 1 \pmod p \Rightarrow x^2 + y^2 = kp + 1 \quad \text{với } k \in \mathbb{N}$$

Và:

$$x^2 + y^2 \leq \frac{(p-1)^2}{2} = \frac{p^2 - 2p + 1}{2} < \frac{p(p-1)}{2} + 1$$

Nên $kp + 1 \leq \frac{p(p-1)}{2} + 1 \Rightarrow k \leq \frac{p-1}{2}$

Tức là tồn tại một giá trị $kp + 1$ với $k \leq \frac{p-1}{2}$, có dạng tổng hai bình phương.

Như vậy có ít nhất một số trong dãy $p+1, 2p+1, \ldots, (p-3)p+1$ là tổng của hai bình phương. □

[2]Dựa theo lời giải của math90.

Ví dụ (IRN 2015 TST/D1-P3)

[**unrated**] Gọi $b_1 < b_2 < b_3 < \dots$ là dãy tất cả các số tự nhiên có thể viết được dưới dạng tổng hai bình phương của hai số tự nhiên. Chứng minh rằng tồn tại vô hạn số tự nhiên m sao cho $b_{m+1} - b_m = 2015$.

Lời giải. (Cách 1)[3]

Khẳng định — *Với mỗi số nguyên $1 \le i \le 2014$, tồn tại vô hạn số nguyên tố $p \equiv 3 \pmod 8$ sao cho:*

$$\left(\frac{1007^2 + i}{p}\right) = -1$$

Chứng minh. Viết:

$$1007^2 + i = x^2 p_1 p_2 \dots p_k$$

trong đó $\mathcal{P} = \{p_1, \dots, p_k\}$ là tập các thừa số nguyên tố của $1007^2 + i$ có số mũ lẻ. Ta có $\mathcal{P} \neq \emptyset$ vì $1007^2 + i$ không thể là một số chính phương khi $i \in [1, 2014]$.

Trường hợp 1: Nếu $\mathcal{P} = \{2\}$, thì:

$$\left(\frac{1007^2 + i}{p}\right) = \left(\frac{2x^2}{p}\right) = \left(\frac{2}{p}\right) = -1 \quad \text{với } p \equiv 3 \pmod 8$$

Trường hợp 2: Nếu $2 \notin \mathcal{P}$, thì chọn p sao cho:

$$\left(\frac{\prod_{q \in \mathcal{P}} q}{p}\right) = -1$$

Trường hợp 3: Nếu $2 \in \mathcal{P}$, thì chọn p sao cho:

$$\left(\frac{\prod_{q \in \mathcal{P} \setminus \{2\}} q}{p}\right) = 1$$

Sử dụng định lý tương hỗ bậc hai, ta có thể dịch điều kiện trên thành điều kiện đồng dư của p modulo các số trong $\mathcal{P}$. Từ định lý Dirichlet và định lý đồng dư Trung Hoa (CRT), tồn tại vô hạn số nguyên tố $p \equiv 3 \pmod 8$ thỏa các điều kiện này. ■

Chọn các số nguyên tố phân biệt $p_1, p_2, \dots, p_{2014}$, sao cho:

- Mỗi $p_i > 1008^2$
- $p_i \equiv 3 \pmod 8$,
- $\left(\frac{1007^2+i}{p_i}\right) = -1$.

Nhờ bổ đề, ta có thể chọn được những p_i như vậy. Xét hệ congruence:

$$x + i \equiv p_i \pmod{p_i^2} \quad \text{với } 1 \le i \le 2014 \tag{*}$$

Theo định lý CRT, hệ này có nghiệm duy nhất modulo:

$$M = p_1^2 p_2^2 \cdots p_{2014}^2$$

Gọi nghiệm là $x \equiv k \pmod M$. Khi đó, với mọi $i \in [1, 2014]$, ta có:

$$x + i \equiv p_i \pmod{p_i^2} \implies x + i \not\equiv \text{tổng hai bình phương}$$

vì $p_i \equiv 3 \pmod 4$, nên một số chia hết cho p_i với lũy thừa lẻ thì không thể là tổng hai bình phương.

Bây giờ, ta chứng minh k là tổng hai bình phương:

$$\left(\frac{k-1007^2}{p_i}\right) = \left(\frac{-i-1007^2}{p_i}\right) = -\left(\frac{1007^2+i}{p_i}\right) = 1,$$

do đó, tồn tại x_i sao cho $x_i^2 \equiv k - 1007^2 \pmod{p_i}$, và $p_i \nmid x_i$.

Sử dụng phương pháp nâng nghiệm Hensel, ta có thể tìm $t_i \in \mathbb{Z}$:

$$t \equiv -\frac{x_i - (k-1007^2)}{p} \cdot (2x_i)^{-1} \pmod p \implies p_i^2 \mid (x_i + p_i t_i)^2 - (k - 1007^2)$$

Gọi $a \equiv x_i + p_i t_i \pmod{p_i^2}$ với mỗi i, và sử dụng CRT, tồn tại vô hạn $a \in \mathbb{N}$ thỏa:

$$a^2 = k - 1007^2 + \beta_a M \implies k = a^2 + 1007^2 + \beta_a M \implies k + 2015 = a^2 + 1008^2 + \beta_a M$$

Vì vậy, với:

$$n = k + \beta_a M = a^2 + 1007^2$$

thì n và $n + 2015$ đều là tổng hai bình phương, nhưng các số $n+1, n+2, \ldots, n+2014$ thì không. Do đó, ta tìm được hiệu $b_{m+1} - b_m = 2015$. Vì a có thể chọn tùy ý lớn, nên tồn tại vô hạn nhiều khoảng như vậy. □

[3] Dựa theo lời giải của Ariscrim.

Ví dụ (IRN 2015 TST/D2-P1)

[**unrated**] Cho trước số tự nhiên n. Tìm giá trị nhỏ nhất của k sao cho với mọi tập A gồm k số tự nhiên, luôn tồn tại một tập con của A có số phần tử chẵn và tổng các phần tử chia hết cho n.

Lời giải. (Cách 1)[4]

Khẳng định — Cho n là một số nguyên dương. Khi đó, trong mọi tập $X = \{x_1, x_2, \ldots, x_n\}$ gồm n số nguyên, tồn tại một tập con $A \subseteq X$ sao cho tổng các phần tử của A chia hết cho n.

Chứng minh. Xét các tổng sau:

$$A_1 = \{a_1\}, \quad A_2 = \{a_1 + a_2\}, \quad \ldots, \quad A_n = \{a_1 + a_2 + \cdots + a_n\}$$

Nếu tồn tại i sao cho $\overline{A_i} \equiv 0 \pmod n$ thì ta đã xong. Ngược lại, tồn tại hai tổng A_i, A_j với $j > i$ sao cho $\overline{A_i} \equiv \overline{A_j} \pmod n$, suy ra:

$$\overline{A_j - A_i} = a_{i+1} + \cdots + a_j \equiv 0 \pmod n$$

■

Xét ba trường hợp.

Trường hợp 1: $n = 2k$ là số chẵn và k là số lẻ.

Lấy $n + 1$ số tự nhiên bất kỳ. Chia chúng thành hai tập: $A = \{a_1, a_2, \ldots, a_t\}$: chứa các số lẻ. $B = \{b_1, b_2, \ldots, b_s\}$: chứa các số chẵn

Vì $t + s = n + 1$ là số lẻ, nên một trong hai số t, s là chẵn, số còn lại là lẻ. Giả sử t chẵn. Ta chia các phần tử trong A thành $\frac{t}{2}$ cặp:

$$A_1 = \{a_1, a_2\}, \quad A_2 = \{a_3, a_4\}, \quad \ldots, \quad A_{\frac{t}{2}} = \{a_{t-1}, a_t\}$$

Tương tự, bỏ b_s ra khỏi B, và chia phần còn lại thành $\frac{s-1}{2}$ cặp:

$$B_1 = \{b_1, b_2\}, \quad B_2 = \{b_3, b_4\}, \quad \ldots, \quad B_{\frac{s-1}{2}} = \{b_{s-2}, b_{s-1}\}$$

Gọi $\overline{X}$ là tổng các phần tử trong tập X. Ta thu được $\frac{t+s-1}{2} = \frac{n}{2} = k$ tổng. Theo bổ đề, tồn tại một tập con gồm các tổng trên sao cho tổng của chúng chia hết cho k. Vì mỗi tổng là tổng của hai số và k lẻ, nên tổng này cũng chia hết cho $2k = n$. Mỗi tổng được tạo bởi hai phần tử trong tập ban đầu, nên số phần tử trong tập con là chẵn.

Trường hợp t lẻ thì làm tương tự.

Trường hợp 2: $4 \mid n = 2k$. Gọi $A = \{a_1, a_2, \ldots, a_{n+1}\}$ là tập gồm $n + 1$ số bất kỳ.

Xét tập con $A_1 = \{a_1, a_2, \ldots, a_{k+1}\}$. Vì k chẵn, nên theo trường hợp (1), tồn tại tập con $X_1 \subseteq A_1$ gồm số phần tử chẵn sao cho tổng chia hết cho k, tức là $\overline{X_1} = kt$.

Do $|X_1| < n + 1$, phần còn lại $A \setminus X_1$ có ít nhất $k + 1$ phần tử. Áp dụng lại như trên, ta có tập con $X_2 \subseteq A \setminus X_1$ chẵn phần tử sao cho $\overline{X_2} = kl$.

Nếu t hoặc l chẵn, thì kt hoặc kl chia hết cho n. Nếu cả hai lẻ thì:

$$\overline{X_1 \cup X_2} = k(t + l) = 2ks = ns$$

Tập $X_1 \cup X_2$ có số phần tử chẵn. Vậy ta đã xong.

Trường hợp 3: n là số lẻ. Xét tập $A = \{a_1, a_2, \ldots, a_{2n}\}$

Chia thành hai nửa:

$$A_1 = \{a_1, a_2, \ldots, a_n\}, \quad A_2 = \{a_{n+1}, a_{n+2}, \ldots, a_{2n}\}$$

Áp dụng bổ đề cho A_1 và A_2, ta thu được hai tập con $X_1 \subseteq A_1$, $X_2 \subseteq A_2$ sao cho:

$$\overline{X_1} \equiv \overline{X_2} \equiv 0 \pmod{n}$$

Nếu X_1 hoặc X_2 có số phần tử chẵn, ta đã xong. Ngược lại, nếu cả hai có số phần tử lẻ, thì $|X_1 \cup X_2|$ chẵn và tổng chia hết cho n. Vậy $X_1 \cup X_2$ là tập con thỏa mãn yêu cầu. □

[4] Dựa theo lời giải của andria.

Ví dụ (RUS 2015 TST/D10/P2)

[**unrated**] Cho số nguyên tố $p \geq 5$. Chứng minh rằng tập $\{1, 2, \ldots, p-1\}$ 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.

Lời giải. (Cách 1)[5]Ta biết rằng:

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

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

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

Do đó, ta cần:

$$A \equiv \frac{-1}{B} \pmod p \iff AB \equiv -1 \pmod p.$$

Ta sẽ xây dựng S thỏa mãn điều này.

Trường hợp 1: Nếu $p \equiv 1 \pmod 4$. Khi đó $\exists a \in \mathbb{F}_p$ sao cho $a^2 \equiv -1 \pmod p$. Khi đó, lấy $S = \{a\}$ thì:

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

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

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

Do các phần tử đi thành cặp nghịch đảo, tích của S là 1 modulo p:

$$\prod_{i \in S} i \equiv 1 \pmod p.$$

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

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

vì đây là tổng cấp số nhân có công bội a bậc q.

Vậy:

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

□

[5]Dựa theo lời giải của IAmTheHazard.

Ví dụ (USA 2015 TSTST/P3)

[**40M**] Giả sử P là tập hợp tất cả các số nguyên tố, và M là một tập con không rỗng của P. Giả sử rằng với mọi tập con không rỗng $\{p_1, p_2, \ldots, p_k\}$ của M, tất cả các ước số nguyên tố của $p_1p_2 \ldots p_k + 1$ cũng thuộc M. Chứng minh rằng $M = P$.

Lời giải. (Cách 1)[6]Giả sử ngược lại rằng tồn tại số nguyên tố $p \notin M$. Do điều kiện đề bài, ta biết rằng nếu lấy tích các số nguyên tố trong M rồi cộng 1, thì các ước số nguyên tố của kết quả luôn thuộc M. Ta sẽ xây dựng một dãy số trong M để dẫn đến mâu thuẫn với giả thiết $p \notin M$.

Xét các lớp dư modulo p. Gọi X là tập các số nguyên tố trong M mà lớp dư modulo p của chúng xuất hiện vô hạn lần trong M, và $Y = M \setminus X$, tức là tập các số nguyên tố trong M mà lớp dư modulo p chỉ xuất hiện hữu hạn lần. Vì chỉ có hữu hạn lớp dư modulo p, nên Y là hữu hạn.

Đặt

$$t = \begin{cases} 1 & \text{nếu } Y = \emptyset, \\ \prod\limits_{y \in Y} y & \text{nếu } Y \neq \emptyset. \end{cases}$$

Rõ ràng $p \nmid t$, vì $p \notin M$ và t là tích các phần tử của M.

Bây giờ, ta xây dựng một dãy $\{a_n\}$ như sau:

- Đặt $a_0 = 1$.
- Với $n \geq 0$, xét $ta_n + 1$ và phân tích nó thành thừa số nguyên tố:

$$ta_n + 1 = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}.$$

  Vì $(t, ta_n + 1) = 1$, nên mọi p_i đều không chia hết t và do đó không thuộc Y, tức là $p_i \in X \subseteq M$.
- Với mỗi p_i, do $p_i \in X$ nên có vô hạn số nguyên tố trong M đồng dư với p_i modulo p. Do đó, ta có thể chọn α_i số nguyên tố phân biệt trong M, mỗi số đồng dư với $p_i \pmod p$, và tất cả các số này đều phân biệt. Gọi a_{n+1} là tích của các số nguyên tố được chọn.

Rõ ràng $a_{n+1} \equiv ta_n + 1 \pmod p$. Vì $a_0 = 1$, nên ta có:

$$a_1 \equiv t + 1 \pmod p, \quad a_2 \equiv t(t+1) + 1 = t^2 + t + 1 \pmod p, \quad \text{v.v.}$$

Suy ra:

$$a_n \equiv t^n + t^{n-1} + \ldots + 1 \pmod p.$$

Xét ba trường hợp:

- Nếu $t \equiv 0 \pmod p$ thì $p \mid t$, mâu thuẫn với $p \notin M$.
- Nếu $t \equiv 1 \pmod p$ thì $a_p \equiv p \equiv 0 \pmod p$.
- Nếu $t \not\equiv 0, 1 \pmod p$ thì theo công thức cấp số nhân:

$$a_{p-2} \equiv \frac{t^{p-1} - 1}{t - 1} \equiv 0 \pmod p.$$

Trong cả ba trường hợp, tồn tại n sao cho $a_n \equiv 0 \pmod p$. Nhưng điều này vô lý, vì mỗi a_n là tích của các số nguyên tố thuộc M, nên không thể chia hết cho $p \notin M$.

Vậy giả thiết ban đầu sai. Suy ra $M = P$. □

[6]Lời giải của Aiscrim do Evan Chen viết lại.

Ví dụ (USA 2015 TSTST/P5)

[**10M**] Cho $\varphi(n)$ là số các số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n. Chứng minh rằng tồn tại một số nguyên dương m sao cho phương trình

$$\varphi(n) = m$$

có ít nhất 2015 nghiệm nguyên dương n.

Lời giải. (Cách 1)[7]Xét tập các số nguyên tố:

$$S = \{11, 13, 17, 19, 29, 31, 37, 41, 43, 61, 71\},$$

với tính chất rằng với mọi $p \in S$, tất cả ước số nguyên tố của $p-1$ đều là số có một chữ số.

Gọi $N = 210^{\text{tỷ}}$, và đặt $M = \varphi(N)$. Với mỗi tập con $T \subseteq S$, định nghĩa:

$$n_T = \frac{N}{\prod_{p\in T}(p-1)} \cdot \prod_{p\in T} p.$$

Khi đó:

$$\varphi(n_T) = \varphi\left(\frac{N}{\prod_{p\in T}(p-1)} \cdot \prod_{p\in T} p\right) = \varphi(N) = M,$$

vì thay mỗi thừa số $p-1 \mid N$ bằng p không làm thay đổi giá trị Hàm Euler's Totient.

Do $|S| = 11$, ta có $2^{11} = 2048 > 2015$ tập con, nên ta thu được ít nhất 2015 số nguyên dương phân biệt có cùng giá trị φ. □

Nhận xét. Mẹo này bắt nguồn từ thực tế như: $\varphi(11 \cdot 1000) = \varphi(10 \cdot 1000)$, vì $\varphi(11) = 10 = \varphi(10)$.

Lời giải. (Cách 2)[8]Gọi $p_1 = 2 < p_2 < \cdots < p_{2015}$ là 2015 số nguyên tố nhỏ nhất. Xét 2015 số $n_1, \ldots, n_{2015}$ được định nghĩa như sau:

$$\begin{aligned} n_1 &= (p_1 - 1) \cdot p_2 \cdots p_{2015}, \\ n_2 &= p_1 \cdot (p_2 - 1) \cdot p_3 \cdots p_{2015}, \\ &\vdots \\ n_{2015} &= p_1 \cdots p_{2014} \cdot (p_{2015} - 1). \end{aligned}$$

Lưu ý rằng trong mỗi n_j, một số nguyên tố p_j được thay thế bằng $p_j - 1$.

Vì $\varphi(p_j - 1) = \varphi(p_j) = p_j - 1$ nếu p_j là nguyên tố, nên:

$$\varphi(n_j) = \prod_{i=1}^{2015} (p_i - 1) = \varphi(p_1 p_2 \cdots p_{2015}).$$

Do đó $n_1, \ldots, n_{2015}$ là 2015 số nguyên dương đôi một phân biệt có cùng giá trị Hàm Euler's Totient.

Các số này chỉ có ước số nguyên tố trong $\{p_1, \ldots, p_{2015}\}$. □

[7]Lời giải của Evan Chen.
[8]Lời giải của Yang Liu.

Lời giải. (Cách 3)[9]Ta chứng minh bài toán tổng quát.

Khẳng định — Cho $p_1 = 2 < p_2 < \cdots < p_k$ là k số nguyên tố đầu tiên. Khi đó tồn tại ít nhất k số nguyên dương phân biệt n sao cho:

$$\varphi(n) = \varphi(p_1 p_2 \cdots p_k)$$

và mọi ước số nguyên tố của n đều thuộc tập $\{p_1, p_2, \ldots, p_k\}$.

Chứng minh. Ta dùng phương pháp quy nạp theo k.

Bước cơ sở: Với $k = 1$, ta có $p_1 = 2$, nên $\varphi(2) = 1$. Số duy nhất n sao cho $\varphi(n) = 1$ là $n = 2$, thỏa mãn điều kiện. Mệnh đề đúng với $k = 1$.

Bước quy nạp: Giả sử với một số $k \geq 1$, tồn tại ít nhất k số nguyên dương phân biệt $n_1, n_2, \ldots, n_k$ sao cho:

$$\varphi(n_j) = \varphi(P_k), \quad \text{với } P_k = \prod_{i=1}^{k} p_i,$$

và mọi ước số nguyên tố của n_j đều thuộc $\{p_1, \ldots, p_k\}$.

Ta chứng minh mệnh đề đúng với $k+1$. Xét $P_{k+1} = P_k \cdot p_{k+1}$. Khi đó:

$$\varphi(P_{k+1}) = \varphi(P_k) \cdot (p_{k+1} - 1).$$

Với mỗi $j = 1, \ldots, k$, xét số $m_j = n_j \cdot p_{k+1}$. Vì $\gcd(n_j, p_{k+1}) = 1$, ta có:

$$\varphi(m_j) = \varphi(n_j) \cdot \varphi(p_{k+1}) = \varphi(P_k) \cdot (p_{k+1} - 1) = \varphi(P_{k+1}).$$

Các m_j đều có ước số nguyên tố thuộc $\{p_1, \ldots, p_{k+1}\}$, và phân biệt vì n_j phân biệt. Như vậy ta đã có k số thỏa mãn. Ta cần thêm một số nữa.

Vì $p_{k+1} - 1$ là số chẵn và nhỏ hơn p_{k+1}, nên mọi ước số nguyên tố của nó đều thuộc $\{p_1, \ldots, p_k\}$. Viết:

$$p_{k+1} - 1 = \prod_{i=1}^{k} p_i^{e_i}.$$

Đặt:

$$m_{k+1} = \left(\prod_{i=1}^{k} p_i^{e_i + 1} \right).$$

Vì $\gcd(p_i, p_j) = 1$ khi $i \neq j$, ta có:

$$\varphi(m_{k+1}) = \prod_{i=1}^{k} p_i^{e_i}(p_i - 1) = (p_{k+1} - 1) \cdot \varphi(P_k) = \varphi(P_{k+1}).$$

Hơn nữa, m_{k+1} có dạng mũ khác với các số m_j trước đó (vì chúng đều chỉ có mũ ≤ 1), nên m_{k+1} là số thứ $(k+1)$ phân biệt. Do đó, tồn tại ít nhất $k+1$ số nguyên dương phân biệt thỏa mãn yêu cầu với $k+1$. ■

□

[9]Dựa theo lời giải của mathocean97.

Ví dụ (USA 2015 TST/P2)

[**25M**] Chứng minh rằng với mọi $n \in \mathbb{N}$, tồn tại một tập S gồm n số nguyên dương sao cho với mọi hai phần tử phân biệt $a, b \in S$, hiệu $a-b$ chia hết cả a và b, nhưng không chia hết bất kỳ phần tử nào khác trong S.

Lời giải. (Cách 1)[10]Chúng ta xây dựng một dãy các hiệu $d_1, d_2, \ldots, d_{n-1}$ sao cho dãy số được tạo thành từ:

$$s_1 = 0, \quad s_2 = d_1, \quad s_3 = d_1 + d_2, \quad \ldots, \quad s_n = d_1 + \cdots + d_{n-1}$$

và đặt $S = \{a + s_1, a + s_2, \ldots, a + s_n\}$ với một số $a \in \mathbb{Z}_{>0}$ được chọn sao cho các tính chất sau được đảm bảo:

(i) Với mọi cặp chỉ số $1 \le i < j \le n$, đặt $t_{i,j} = s_j - s_i = d_i + d_{i+1} + \cdots + d_{j-1}$. Ta yêu cầu rằng các số $t_{i,j}$ không chia hết nhau, tức là không tồn tại $(i,j) \neq (k,\ell)$ sao cho $t_{i,j} \mid t_{k,\ell}$.

(ii) Có tồn tại một số $a \in \mathbb{Z}_{>0}$ sao cho:

$$a \equiv -s_i \pmod{t_{i,j}} \quad \text{với mọi } 1 \le i < j \le n.$$

Với những điều kiện này, nếu đặt $S = \{a + s_1, a + s_2, \ldots, a + s_n\}$ thì với mọi $a', b' \in S$, ta có:

$$|a' - b'| = t_{i,j} \mid a', b', \quad \text{nhưng không chia bất kỳ phần tử nào khác trong } S.$$

Bước cơ sở: $n = 3$. Chọn $d_1 = 2$, $d_2 = 3$. Khi đó $s_1 = 0, s_2 = 2, s_3 = 5$, và:

$$t_{1,2} = 2, \quad t_{2,3} = 3, \quad t_{1,3} = 5.$$

Rõ ràng $2, 3, 5$ là các số nguyên tố phân biệt nên không chia hết nhau. Giải hệ:

$$\left.\begin{aligned} a &\equiv 0 \pmod 2, \\ a &\equiv -2 \pmod 3, \\ a &\equiv 0 \pmod 5. \end{aligned}\right\} \implies a \equiv 10 \pmod{30}.$$

Chọn $a = 10$, ta được $S = \{10, 12, 15\}$. Dễ thấy:

$$|12 - 10| = 2 \mid 10, 12, \ |15 - 12| = 3 \mid 12, 15, \ |15 - 10| = 5 \mid 10, 15$$

nhưng các hiệu đó không chia hết phần tử còn lại.

Bước quy nạp: Giả sử đã xây dựng được $d_1, \ldots, d_{n-1}$ và a thỏa mãn (i) và (ii) cho n phần tử. Ta sẽ mở rộng thành $n+1$ phần tử như sau:

(i) Chọn một số nguyên tố p sao cho $p \nmid t_{i,j}$ với mọi $1 \le i < j \le n$. Điều này đảm bảo p không chia hết bất kỳ hiệu nào có sẵn.

(ii) Đặt $M = \operatorname{LCM}(t_{i,j} \mid 1 \le i < j \le n)$.

(iii) Thay mỗi d_i bởi $d_i' = M \cdot d_i$, và đặt thêm hiệu mới $d_n' = p$.

Từ đó xây dựng các $s_1', \ldots, s_{n+1}'$, và giữ nguyên a ban đầu. Do M chia hết tất cả $t_{i,j}$, ta có:

$$t_{i,j}' = M \cdot t_{i,j}, \quad \text{và } t_{i,n+1}' = M \cdot t_{i,n} + p.$$

Các hiệu mới đều nguyên tố cùng nhau, nên điều kiện (i) vẫn giữ nguyên.

Về (ii): Vì các mô-đun $t_{i,j}'$ vẫn nguyên tố cùng nhau, và $t_{i,n+1}' \equiv p \pmod M$, ta có thể mở rộng hệ đồng dư cũ để thêm điều kiện cho phần tử thứ $n+1$, sử dụng Định lý phần dư Trung Hoa.

Kết luận: Bằng quy nạp, tồn tại một dãy hiệu $d_1, \ldots, d_{n-1}$ và một số a sao cho tập $S = \{a + s_1, \ldots, a + s_n\}$ thỏa mãn yêu cầu đề bài. □

[10]Dựa theo lời giải của Evan Chen.

12.3 Bài tập

Bài tập (KOR 2015 FR/P1)**.** [**unrated**] Cho số nguyên dương cố định k. Xét hai dãy số A_n và B_n được định nghĩa như sau:

$$A_1 = k, \quad A_2 = k, \quad A_{n+2} = A_n A_{n+1},$$
$$B_1 = 1, \quad B_2 = k, \quad B_{n+2} = \frac{B_{n+1}^3 + 1}{B_n}.$$

Chứng minh rằng với mọi số nguyên dương n, biểu thức $A_{2n}B_{n+3}$ là một số nguyên.

Bài tập (RUS 2015 TST/D10/P1)**.** [**unrated**] Chứng minh rằng tồn tại hai số nguyên dương a, b sao cho với mọi cặp số nguyên dương m, n nguyên tố cùng nhau, ta có:

$$|a - m| + |b - n| > 1000.$$

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 $\frac{a_1}{a_2} + \dots + \frac{a_n}{a_1} \in \mathbb{Z}$

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).

Từ điển chú giải

CHN 2015 MO China National Olympiad 2015 50

CHN 2015 TST China Team Selection Test 2015 12–14, 39, 51, 59

IMO 2015 International Mathematical Olympiad 2015 29, 30, 40, 52

IMO 2023 International Mathematical Olympiad 2023 15, 53

IND 2015 MO India National Olympiad 2015 17, 18

IND 2015 TST India Team Selection Test 2015 19, 32, 33

IRN 2015 MO Iran National Olympiad 2015 21, 34, 60, 64, 65

IRN 2015 TST Iran Team Selection Test 2015 22, 66, 68

JPN 2015 MO Japan National Olympiad 2015 27, 36

KOR 2015 FR Korea Final Round 2015 75

KOR 2015 MO Korea National Olympiad 2015 23, 43

RUS 2015 MO All-Russia Olympiad 2015 54

RUS 2015 TST Russia Team Selection Test 2015 25, 35, 46, 70, 75

USA 2015 MO USA National Olympiad 2015 44, 45

USA 2015 TST USA Team Selection Test 2015 74

USA 2015 TSTST USA Team Selection Test Selection Test 2015 71, 72